

**Note: Hw accelerator is CPU**

Runtime → Change runtime type → Hardware accelerator: CPU.

Github Link : [https://github.com/DHHirdal/ML\\_SystemOptimization/](https://github.com/DHHirdal/ML_SystemOptimization/)

# Group Name : Group 44

## Members

Name BITS ID

- CHELLA VENKATA GOPIKRISHNA --> 2024ac05978
- HIRDALAPPA H ---> 2024ac05306
- ALOK KUMAR OJHA --> 2024ad05055
- PUvvADA VENKATA SAI MANOJ CHANDRA --> 2024ac05227
- SK SAFIRUDDIN ---> 2024ac05781

**Our technical paper has two parts**

- **Part-1:** Explore Distributed Machine learning using PyTorch DDP
- **Part -2:** Explore the TDML framework (Trustworthy Distributed Machine Learning ) like Blockchain-based Data Parallelism

```
In [ ]: #Install required libraries  
%pip install torch
```

```
Requirement already satisfied: torch in /usr/local/lib/python3.11/dist-packages  
(2.6.0+cu124)  
Requirement already satisfied: filelock in /usr/local/lib/python3.11/dist-packages  
(from torch) (3.18.0)  
Requirement already satisfied: typing-extensions>=4.10.0 in /usr/local/lib/python  
3.11/dist-packages (from torch) (4.14.1)  
Requirement already satisfied: networkx in /usr/local/lib/python3.11/dist-packages  
(from torch) (3.5)  
Requirement already satisfied: jinja2 in /usr/local/lib/python3.11/dist-packages  
(from torch) (3.1.6)  
Requirement already satisfied: fsspec in /usr/local/lib/python3.11/dist-packages  
(from torch) (2025.3.2)  
Collecting nvidia-cuda-nvrtc-cu12==12.4.127 (from torch)  
  Downloading nvidia_cuda_nvrtc_cu12-12.4.127-py3-none-manylinux2014_x86_64.whl.m  
etadata (1.5 kB)  
Collecting nvidia-cuda-runtime-cu12==12.4.127 (from torch)  
  Downloading nvidia_cuda_runtime_cu12-12.4.127-py3-none-manylinux2014_x86_64.wh  
l.metadata (1.5 kB)  
Collecting nvidia-cuda-cupti-cu12==12.4.127 (from torch)  
  Downloading nvidia_cuda_cupti_cu12-12.4.127-py3-none-manylinux2014_x86_64.whl.m  
etadata (1.6 kB)  
Collecting nvidia-cudnn-cu12==9.1.0.70 (from torch)  
  Downloading nvidia_cudnn_cu12-9.1.0.70-py3-none-manylinux2014_x86_64.whl.met  
adata (1.6 kB)  
Collecting nvidia-cublas-cu12==12.4.5.8 (from torch)  
  Downloading nvidia_cublas_cu12-12.4.5.8-py3-none-manylinux2014_x86_64.whl.met  
adata (1.5 kB)  
Collecting nvidia-cufft-cu12==11.2.1.3 (from torch)  
  Downloading nvidia_cufft_cu12-11.2.1.3-py3-none-manylinux2014_x86_64.whl.met  
adata (1.5 kB)  
Collecting nvidia-curand-cu12==10.3.5.147 (from torch)  
  Downloading nvidia_curand_cu12-10.3.5.147-py3-none-manylinux2014_x86_64.whl.met  
adata (1.5 kB)  
Collecting nvidia-cusolver-cu12==11.6.1.9 (from torch)  
  Downloading nvidia_cusolver_cu12-11.6.1.9-py3-none-manylinux2014_x86_64.whl.met  
adata (1.6 kB)  
Collecting nvidia-cusparse-cu12==12.3.1.170 (from torch)  
  Downloading nvidia_cusparse_cu12-12.3.1.170-py3-none-manylinux2014_x86_64.whl.m  
etadata (1.6 kB)  
Requirement already satisfied: nvidia-cusparseelt-cu12==0.6.2 in /usr/local/lib/py  
thon3.11/dist-packages (from torch) (0.6.2)  
Requirement already satisfied: nvidia-nccl-cu12==2.21.5 in /usr/local/lib/python  
3.11/dist-packages (from torch) (2.21.5)  
Requirement already satisfied: nvidia-nvtx-cu12==12.4.127 in /usr/local/lib/pytho  
n3.11/dist-packages (from torch) (12.4.127)  
Collecting nvidia-nvjitlink-cu12==12.4.127 (from torch)  
  Downloading nvidia_nvjitlink_cu12-12.4.127-py3-none-manylinux2014_x86_64.whl.m  
etadata (1.5 kB)  
Requirement already satisfied: triton==3.2.0 in /usr/local/lib/python3.11/dist-pa  
ckages (from torch) (3.2.0)  
Requirement already satisfied: sympy==1.13.1 in /usr/local/lib/python3.11/dist-pa  
ckages (from torch) (1.13.1)  
Requirement already satisfied: mpmath<1.4,>=1.1.0 in /usr/local/lib/python3.11/di  
st-packages (from sympy==1.13.1->torch) (1.3.0)  
Requirement already satisfied: MarkupSafe>=2.0 in /usr/local/lib/python3.11/dist-  
packages (from jinja2->torch) (3.0.2)  
Downloading nvidia_cublas_cu12-12.4.5.8-py3-none-manylinux2014_x86_64.whl (363.4  
MB)
```

---

363.4/363.4 MB 4.4 MB/s eta 0:00:00

Downloading nvidia\_cuda\_cupti\_cu12-12.4.127-py3-none-manylinux2014\_x86\_64.whl (1

```
3.8 MB)
  _____ 13.8/13.8 MB 13.3 MB/s eta 0:00:00
Downloading nvidia_cuda_nvrtc_cu12-12.4.127-py3-none-manylinux2014_x86_64.whl (2
4.6 MB)
  _____ 24.6/24.6 MB 15.9 MB/s eta 0:00:00
Downloading nvidia_cuda_runtime_cu12-12.4.127-py3-none-manylinux2014_x86_64.whl
(883 kB)
  _____ 883.7/883.7 kB 15.2 MB/s eta 0:00:00
Downloading nvidia_cudnn_cu12-9.1.0.70-py3-none-manylinux2014_x86_64.whl (664.8 M
B)
  _____ 664.8/664.8 MB 2.5 MB/s eta 0:00:00
Downloading nvidia_cufft_cu12-11.2.1.3-py3-none-manylinux2014_x86_64.whl (211.5 M
B)
  _____ 211.5/211.5 MB 6.7 MB/s eta 0:00:00
Downloading nvidia_curand_cu12-10.3.5.147-py3-none-manylinux2014_x86_64.whl (56.3
MB)
  _____ 56.3/56.3 MB 13.6 MB/s eta 0:00:00
Downloading nvidia_cusolver_cu12-11.6.1.9-py3-none-manylinux2014_x86_64.whl (127.
9 MB)
  _____ 127.9/127.9 MB 7.5 MB/s eta 0:00:00
Downloading nvidia_cusparse_cu12-12.3.1.170-py3-none-manylinux2014_x86_64.whl (20
7.5 MB)
  _____ 207.5/207.5 MB 6.2 MB/s eta 0:00:00
Downloading nvidia_nvjitlink_cu12-12.4.127-py3-none-manylinux2014_x86_64.whl (21.
1 MB)
  _____ 21.1/21.1 MB 7.3 MB/s eta 0:00:00
Installing collected packages: nvidia-nvjitlink-cu12, nvidia-curand-cu12, nvidia-
cufft-cu12, nvidia-cuda-runtime-cu12, nvidia-cuda-nvrtc-cu12, nvidia-cuda-cupti-c
u12, nvidia-cublas-cu12, nvidia-cusparse-cu12, nvidia-cudnn-cu12, nvidia-cusolver
-cu12
Attempting uninstall: nvidia-nvjitlink-cu12
  Found existing installation: nvidia-nvjitlink-cu12 12.5.82
  Uninstalling nvidia-nvjitlink-cu12-12.5.82:
    Successfully uninstalled nvidia-nvjitlink-cu12-12.5.82
Attempting uninstall: nvidia-curand-cu12
  Found existing installation: nvidia-curand-cu12 10.3.6.82
  Uninstalling nvidia-curand-cu12-10.3.6.82:
    Successfully uninstalled nvidia-curand-cu12-10.3.6.82
Attempting uninstall: nvidia-cufft-cu12
  Found existing installation: nvidia-cufft-cu12 11.2.3.61
  Uninstalling nvidia-cufft-cu12-11.2.3.61:
    Successfully uninstalled nvidia-cufft-cu12-11.2.3.61
Attempting uninstall: nvidia-cuda-runtime-cu12
  Found existing installation: nvidia-cuda-runtime-cu12 12.5.82
  Uninstalling nvidia-cuda-runtime-cu12-12.5.82:
    Successfully uninstalled nvidia-cuda-runtime-cu12-12.5.82
Attempting uninstall: nvidia-cuda-nvrtc-cu12
  Found existing installation: nvidia-cuda-nvrtc-cu12 12.5.82
  Uninstalling nvidia-cuda-nvrtc-cu12-12.5.82:
    Successfully uninstalled nvidia-cuda-nvrtc-cu12-12.5.82
Attempting uninstall: nvidia-cuda-cupti-cu12
  Found existing installation: nvidia-cuda-cupti-cu12 12.5.82
  Uninstalling nvidia-cuda-cupti-cu12-12.5.82:
    Successfully uninstalled nvidia-cuda-cupti-cu12-12.5.82
Attempting uninstall: nvidia-cublas-cu12
  Found existing installation: nvidia-cublas-cu12 12.5.3.2
  Uninstalling nvidia-cublas-cu12-12.5.3.2:
    Successfully uninstalled nvidia-cublas-cu12-12.5.3.2
Attempting uninstall: nvidia-cusparse-cu12
  Found existing installation: nvidia-cusparse-cu12 12.5.1.3
```

```

Uninstalling nvidia-cusparse-cu12-12.5.1.3:
  Successfully uninstalled nvidia-cusparse-cu12-12.5.1.3
Attempting uninstall: nvidia-cudnn-cu12
  Found existing installation: nvidia-cudnn-cu12 9.3.0.75
Uninstalling nvidia-cudnn-cu12-9.3.0.75:
  Successfully uninstalled nvidia-cudnn-cu12-9.3.0.75
Attempting uninstall: nvidia-cusolver-cu12
  Found existing installation: nvidia-cusolver-cu12 11.6.3.83
Uninstalling nvidia-cusolver-cu12-11.6.3.83:
  Successfully uninstalled nvidia-cusolver-cu12-11.6.3.83
Successfully installed nvidia-cublas-cu12-12.4.5.8 nvidia-cuda-cupti-cu12-12.4.12
7 nvidia-cuda-nvrtc-cu12-12.4.127 nvidia-cuda-runtime-cu12-12.4.127 nvidia-cudnn-
cu12-9.1.0.70 nvidia-cufft-cu12-11.2.1.3 nvidia-curand-cu12-10.3.5.147 nvidia-cus-
olver-cu12-11.6.1.9 nvidia-cusparse-cu12-12.3.1.170 nvidia-nvjitlink-cu12-12.4.12
7

```

```
In [ ]: #Import required libraries
import math
import random
import copy
import time
import numpy as np
from typing import List, Tuple, Dict, Any, Optional
import matplotlib.pyplot as plt
import os
import sys
import platform
import subprocess
from datetime import datetime
from collections import defaultdict
import random

import torch
import torch.nn as nn
import torch.optim as optim
from torchvision import models, datasets, transforms
from torch.utils.data import DataLoader

import torch
import torch.nn as nn
import torch.optim as optim
from torchvision import models, datasets, transforms
from torch.utils.data import DataLoader

#PyTorch Libraries
import torch
import torch.nn as nn
import torch.nn.functional as F
import torch.optim as optim
import torchvision
from torch.utils.data import DataLoader, Subset, random_split
from torchvision import datasets, transforms, models
from torch.utils.tensorboard import SummaryWriter
```

### Part-1: Explore Distributed Machine learning using PyTorch DDP

```
In [ ]: device = torch.device("cuda" if torch.cuda.is_available() else "cpu")
```

# System Parameters

What PyTorch detects

- CPUs (cores, threads)
- GPUs (CUDA / ROCm)
- GPU memory
- NUMA topology (indirectly via OS)
- Accelerators (XPU, MPS, etc.)
- CPU core count
- Uses system RAM
- PyTorch uses multiple thread pools.

Distributed Training: System-Level Design **PyTorch Distributed (torch.distributed)** is explicitly system-aware. In PyTorch, system details directly shape execution speed, memory usage, scalability, and reliability—especially in distributed training.

👉 PyTorch choice: torch.nn.parallel.DistributedDataParallel (DDP)

```
In [ ]: # Optional dependency – used if available
try:
    import psutil
except Exception:
    psutil = None

import torch

def _bytes2human(n: int) -> str:
    symbols = ('B', 'KB', 'MB', 'GB', 'TB', 'PB')
    i = 0
    n = float(n)
    while n >= 1024 and i < len(symbols) - 1:
        n /= 1024.0
        i += 1
    return f"{n:.2f} {symbols[i]}"

def _safe_run(cmd: str) -> str | None:
    try:
        return subprocess.check_output(
            cmd, shell=True, stderr=subprocess.DEVNULL, text=True
        ).strip()
    except Exception:
        return None

def print_basic_runtime():
    print("=" * 90)
    print("System / Runtime Summary")
    print("Time:", datetime.now().strftime("%Y-%m-%d %H:%M:%S"))
    print("Python:", sys.version.split()[0])
    print("OS:", platform.platform())
    print("Machine:", platform.machine(), " | Processor:", platform.processor())
    print("CPU cores (logical):", os.cpu_count())

    # CPU frequency (if available)
```

```

if psutil and hasattr(psutil, "cpu_freq"):
    try:
        f = psutil.cpu_freq()
        if f:
            print(f"CPU freq: current {f.current:.0f} MHz | min {f.min:.0f}")
    except Exception:
        pass

# Memory
if psutil:
    try:
        vm = psutil.virtual_memory()
        print(f"RAM total: {_bytes2human(vm.total)} | available: {_bytes2human(
            f"} | used: {_bytes2human(vm.used)} ({vm.percent}%)")
    except Exception:
        pass
else:
    print("RAM: psutil not available (install `psutil` for detailed memory s

# Disk
if psutil:
    try:
        d = psutil.disk_usage("/")
        print(f"Disk '/': total {_bytes2human(d.total)} | used {_bytes2human(
            f"} | free {_bytes2human(d.free)}")
    except Exception:
        pass

# PyTorch
print("-" * 90)
print("PyTorch:", torch.__version__)
print("CUDA available:", torch.cuda.is_available())
print("CUDA (pytorch build):", torch.version.cuda)
# cuDNN info
try:
    print("cuDNN enabled:", torch.backends.cudnn.enabled, "| version:", torch
except Exception:
    pass

# NVIDIA-SMI, if present
nvidia_smi = _safe_run("nvidia-smi --query-gpu=name,driver_version,memory.t
if nvidia_smi:
    print("nvidia-smi:", nvidia_smi)

# GPU details
if torch.cuda.is_available():
    try:
        num = torch.cuda.device_count()
        print("CUDA device count:", num)
        for i in range(num):
            prop = torch.cuda.get_device_properties(i)
            total_mem_gb = prop.total_memory / (1024**3)
            print(f" [{i}] {prop.name} | CC {prop.major}.{prop.minor} | VRA
    try:
        cur = torch.cuda.current_device()
        print("Active device:", cur, "-", torch.cuda.get_device_name(cur)
    except Exception:
        pass
    except Exception as e:
        print("CUDA detail error:", str(e))

```

```

# Apple MPS
has_mps = hasattr(torch.backends, "mps") and torch.backends.mps.is_available
print("MPS available:", has_mps)
if has_mps:
    print("MPS build supported:", torch.backends.mps.is_built())

# AMP availability (CUDA)
try:
    use_cuda = torch.cuda.is_available
    amp_enabled = bool(use_cuda) # Gate AMP on CUDA availability
except Exception:
    amp_enabled = False
print("AMP (CUDA) available:", bool(amp_enabled))

# Current process memory
if psutil:
    try:
        proc = psutil.Process(os.getpid())
        mem = proc.memory_info().rss
        print(f"Current process RSS: {_bytes2human(mem)}")
    except Exception:
        pass

print("=" * 90)

def print_distributed_readiness():
    print("Distributed / DDP Readiness")
    # Backends
    dist_avail = torch.distributed.is_available()
    print("torch.distributed available:", dist_avail)
    if dist_avail:
        try:
            print(" - NCCL available:", torch.distributed.is_nccl_available())
        except Exception:
            print(" - NCCL available: (unknown)")

        try:
            print(" - Gloo available:", torch.distributed.is_gloo_available())
        except Exception:
            print(" - Gloo available: (unknown)")

        try:
            print(" - MPI available:", torch.distributed.is_mpi_available())
        except Exception:
            print(" - MPI available: (unknown)")

    # Env vars commonly relevant to DDP/NCCL
    env_keys = [
        "CUDA_VISIBLE_DEVICES",
        "NCCL_DEBUG",
        "NCCL_SOCKET_IFNAME",
        "NCCL_IB_DISABLE",
        "NCCL_P2P_DISABLE",
        "NCCL_SHM_DISABLE",
        "MASTER_ADDR",
        "MASTER_PORT",
        "WORLD_SIZE",
        "RANK",
        "LOCAL_RANK",
    ]

```

```

]

print("Important environment variables:")
for k in env_keys:
    v = os.environ.get(k, None)
    print(f"  {k} = {v}")

# Peer-to-peer (P2P) accessibility among GPUs (intra-node)
if torch.cuda.is_available():
    n = torch.cuda.device_count()
    if n > 1:
        print("GPU Peer-to-Peer access matrix (device_can_access_peer):")
        for i in range(n):
            row = []
            for j in range(n):
                if i == j:
                    row.append("-")
                else:
                    try:
                        row.append("Y" if torch.cuda.device_can_access_peer(
                    except Exception:
                        row.append("?")
                    print(f"  {i}: " + ".join(row))
    else:
        print("Single CUDA device detected; P2P not applicable.")
else:
    print("CUDA not available; NCCL/P2P not applicable.")

# Quick single-process init test (optional and safe on single node)
# Attempts to create/destroy a process group (Gloo on CPU; NCCL on GPU)
if dist_avail:
    backend = "nccl" if torch.cuda.is_available() else "gloo"
    try:
        if not torch.distributed.is_initialized():
            torch.distributed.init_process_group(
                backend=backend,
                rank=0,
                world_size=1,
                init_method="env://"
            )
        print(f"Process group init test: OK (backend={backend})")
    except Exception as e:
        print(f"Process group init test: FAILED (backend={backend}) -> {e}")
    finally:
        try:
            if torch.distributed.is_initialized():
                torch.distributed.destroy_process_group()
        except Exception:
            pass

# Report NCCL runtime version if available via nvidia-smi / nvcc
nvcc = _safe_run("nvcc --version")
if nvcc:
    print("nvcc --version:")
    for line in nvcc.splitlines():
        print("  " + line)

# Optional: show nvidia-smi topo for links/NVLink (if installed)
topo = _safe_run("nvidia-smi topo -m")
if topo:
    print("nvidia-smi topo -m:")

```

```
for line in topo.splitlines():
    print(" " + line)

print("==" * 90)

def main():
    print("Python:", platform.python_version())
    print("PyTorch:", torch.__version__)
    print("CUDA available:", torch.cuda.is_available())
    if torch.cuda.is_available():
        print("GPU name:", torch.cuda.get_device_name(0))
        print("CUDA version (pytorch build):", torch.version.cuda)
        print("#GPUs visible:", torch.cuda.device_count())
        print("CUDA device name:", torch.cuda.get_device_name(0))
        print("CUDA device memory:", torch.cuda.get_device_properties(0).total_m

# Full summaries
print_basic_runtime()
print_distributed_readiness()

if __name__ == "__main__":
    main()
```

```
Python: 3.11.13
PyTorch: 2.6.0+cu124
CUDA available: False
```

---

---

```
System / Runtime Summary
Time: 2026-02-08 19:32:55
Python: 3.11.13
OS: Linux-6.6.105+-x86_64-with-glibc2.35
Machine: x86_64 | Processor: x86_64
CPU cores (logical): 2
CPU freq: current 2200 MHz | min 0 | max 0
RAM total: 12.67 GB | available: 8.80 GB | used: 3.56 GB (30.6%)
Disk '/': total 56.85 GB | used 26.25 GB (46.2%) | free 30.58 GB
```

---

```
-----  
PyTorch: 2.6.0+cu124
CUDA available: False
CUDA (pytorch build): 12.4
cuDNN enabled: True | version: 90100
MPS available: False
AMP (CUDA) available: True
Current process RSS: 1.17 GB
```

---

---

```
Distributed / DDP Readiness
torch.distributed available: True
- NCCL available: True
- Gloo available: True
- MPI available: False
Important environment variables:
CUDA_VISIBLE_DEVICES = None
NCCL_DEBUG = None
NCCL_SOCKET_IFNAME = None
NCCL_IB_DISABLE = None
NCCL_P2P_DISABLE = None
NCCL_SHM_DISABLE = None
MASTER_ADDR = None
MASTER_PORT = None
WORLD_SIZE = None
RANK = None
LOCAL_RANK = None
CUDA not available; NCCL/P2P not applicable.
Process group init test: FAILED (backend=gloo) -> Error initializing torch.distributed using env:// rendezvous: environment variable MASTER_ADDR expected, but not set
nvcc --version:
nvcc: NVIDIA (R) Cuda compiler driver
Copyright (c) 2005-2024 NVIDIA Corporation
Built on Thu_Jun_6_02:18:23_PDT_2024
Cuda compilation tools, release 12.5, V12.5.82
Build cuda_12.5.r12.5/compiler.34385749_0
```

---

```
=====
```



# TDML framework using the ResNet50 model on the CIFAR-10 dataset

## DNN training parallelism

This experiment aim to demonstrate that TDML framework can match the performance of single-node training, achieve comparable accuracy to traditional methods despite the challenges of FL, and enhance efficiency in terms of convergence speeds and training loss.

❖ PyTorch choice: torch.nn.parallel.DistributedDataParallel (DDP)

```
In [ ]: print("[INFO] Dataset loading and confirmation")

class ResNet50CIFAR(nn.Module):
    def __init__(self) -> None:
        super().__init__()
        base = models.resnet50(weights=None)
        in_features = base.fc.in_features
        base.fc = nn.Linear(in_features, 10)
        self.model = base

    def forward(self, x: torch.Tensor) -> torch.Tensor:
        return self.model(x)

# Define a basic transform to convert PIL Image to tensor
transform = transforms.Compose([
    transforms.ToTensor()
])

train_ds = datasets.CIFAR10(root='./data', train=True, download=True, transform=transform)
test_ds = datasets.CIFAR10(root='./data', train=False, download=True, transform=transform)

print("Dataset length:", len(train_ds)) # 50000
print("Classes:", train_ds.classes) # ['airplane', 'automobile'
print("Number of classes:", len(train_ds.classes)) # 10
print("Image shape:", train_ds[0][0].shape)

print("Dataset loaded successfully and verified")
```

```
[INFO] Dataset loading and confirmation
100%|██████████| 170M/170M [00:01<00:00, 104MB/s]
Dataset length: 50000
Classes: ['airplane', 'automobile', 'bird', 'cat', 'deer', 'dog', 'frog', 'horse', 'ship', 'truck']
Number of classes: 10
Image shape: torch.Size([3, 32, 32])
Dataset loaded successfully and verified
```

```
In [ ]: # -----
# Data: sharded train Loaders + single test Loader
# -----
```

```

def get_data(num_workers: int = 5, batch_size: int = 64):
    """
    Returns:
        worker_loaders: list[DataLoader] # one training DataLoader per shard
        test_loader: DataLoader           # test loader
        classes: list[str]            # CIFAR-10 class names
        mean, std: tuple[float]       # used for Normalize (for de-normaliza
    Notes:
        - Here `num_workers` is treated as the number of shards for train set (t
        - We use a small fixed number of loader worker processes per DataLoader
    """
    # 1) Define transforms (CIFAR-10 is 32x32 RGB)
    mean = (0.4914, 0.4822, 0.4465)
    std = (0.2470, 0.2435, 0.2616) # Keep this consistent everywhere (train/test)

    transform = transforms.Compose([
        transforms.ToTensor(),
        transforms.Normalize(mean=mean, std=std),
    ])

    # 2) Create Dataset objects
    train_ds = datasets.CIFAR10(root='./data', train=True, download=True, transform=transform)
    test_ds = datasets.CIFAR10(root='./data', train=False, download=True, transform=transform)

    # 3) Split training set into shards and create Loaders
    num_shards = max(1, int(num_workers)) # reuse your parameter name as "num_workers"
    n = len(train_ds)                   # 50_000 for CIFAR-10
    shard_size = n // num_shards
    worker_loaders: List[DataLoader] = []

    # Keep DataLoader worker processes reasonable (Colab often does fine with 2)
    loader_workers = 2
    pin = torch.cuda.is_available()

    for i in range(num_shards):
        start = i * shard_size
        end = (i + 1) * shard_size if i < num_shards - 1 else n # Last shard gets all remaining
        subset = Subset(train_ds, range(start, end))
        loader = DataLoader(
            subset,
            batch_size=batch_size,
            shuffle=True,
            num_workers=loader_workers,
            pin_memory=pin,
            persistent_workers=(loader_workers > 0),
            drop_last=False,
        )
        worker_loaders.append(loader)

    # 4) Single test Loader (create once, outside the loop)
    test_loader = DataLoader(
        test_ds,
        batch_size=batch_size,
        shuffle=False,
        num_workers=loader_workers,
        pin_memory=pin,
        persistent_workers=(loader_workers > 0),
        drop_last=False,
    )

```

```

        return worker_loaders, test_loader, list(train_ds.classes), mean, std

# -----
# Helpers: de-normalization (batch-safe)
# -----
def _as_batch_stats_tensors(mean, std, device="cpu"):
    mean_t = torch.tensor(mean, dtype=torch.float32, device=device).view(1, 3, 1)
    std_t = torch.tensor(std, dtype=torch.float32, device=device).view(1, 3, 1)
    return mean_t, std_t

def denorm(batch, mean, std):
    """
    De-normalize a batch of images [N,3,H,W].
    """
    device = batch.device
    mean_t, std_t = _as_batch_stats_tensors(mean, std, device=device)
    return batch * std_t + mean_t

# -----
# Visualization 1: Predictions vs Labels grid
# -----
def show_preds_vs_labels(model, loader, classes, mean, std, device="cuda", max_images=100):
    """
    Shows a grid of images with titles "Pred: <pred> / True: <true>".
    Misclassifications are shown in red; correct in green.
    """
    device = device if (device == "cuda" and torch.cuda.is_available()) else "cpu"
    model.to(device)
    model.eval()

    with torch.no_grad():
        images, labels = next(iter(loader))
        images = images.to(device)
        labels = labels.to(device)

        logits = model(images)
        preds = logits.argmax(dim=1)

        # Keep only first max_images
        images = images[:max_images].cpu()
        labels = labels[:max_images].cpu()
        preds = preds[:max_images].cpu()

    # De-normalize for display
    disp = denorm(images, mean, std).clamp(0, 1)

    rows = int(np.ceil(max_images / nrow))
    fig, axes = plt.subplots(rows, nrow, figsize=(nrow * 3.0, rows * 3.0))
    axes = np.array(axes).reshape(-1) # flatten

    for i in range(rows * nrow):
        ax = axes[i]
        if i < len(disp):
            img = disp[i].permute(1, 2, 0).numpy()
            true_lbl = classes[labels[i].item()]
            pred_lbl = classes[preds[i].item()]
            color = "green" if pred_lbl == true_lbl else "red"

```

```

        ax.imshow(img)
        ax.set_title(f"Pred: {pred_lbl}\nTrue: {true_lbl}", color=color, fontweight="bold")
        ax.axis("off")
    else:
        ax.axis("off")

    plt.tight_layout()
    plt.show()

# -----
# Visualization 2: Confusion Matrix
# -----
def plot_confusion_matrix(model, loader, classes, device="cuda", normalize=False):
    """
    Computes and plots a confusion matrix across the entire loader.
    Works without scikit-learn.
    """
    device = device if (device == "cuda" and torch.cuda.is_available()) else "cpu"
    model.to(device)
    model.eval()

    num_classes = len(classes)
    cm = torch.zeros((num_classes, num_classes), dtype=torch.int64)

    with torch.no_grad():
        for x, y in loader:
            x = x.to(device, non_blocking=True)
            y = y.to(device, non_blocking=True)
            preds = model(x).argmax(dim=1)
            for t, p in zip(y.view(-1), preds.view(-1)):
                cm[t.long(), p.long()] += 1

    cm_np = cm.numpy().astype(np.float64)
    if normalize:
        row_sums = cm_np.sum(axis=1, keepdims=True)
        row_sums[row_sums == 0] = 1
        cm_np = cm_np / row_sums

    fig, ax = plt.subplots(figsize=(7, 6))
    im = ax.imshow(cm_np, interpolation="nearest", cmap=cmap)
    plt.colorbar(im, ax=ax, fraction=0.046, pad=0.04)

    ax.set(
        xticks=np.arange(num_classes),
        yticks=np.arange(num_classes),
        xticklabels=classes,
        yticklabels=classes,
        ylabel="True label",
        xlabel="Predicted label",
        title="Confusion Matrix (normalized)" if normalize else "Confusion Matrix")
    plt.setp(ax.get_xticklabels(), rotation=45, ha="right", rotation_mode="anchor")

    # annotate cells
    fmt = ".2f" if normalize else "d"
    thresh = cm_np.max() / 2.0
    for i in range(num_classes):
        for j in range(num_classes):
            if cm_np[i, j] > thresh:
                ax.text(j, i, str(cm_np[i, j]), va="center", ha="center", color="white" if cm_np[i, j] > thresh else "black")

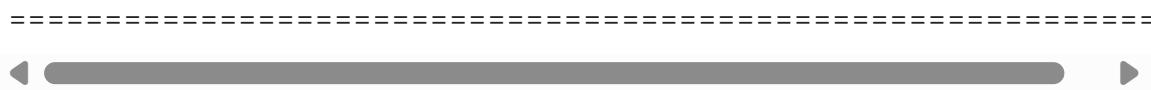
```

```

        ax.text(j, i, format(cm_np[i, j], fmt),
                  ha="center", va="center",
                  color="white" if cm_np[i, j] > thresh else "black")

    plt.tight_layout()
    plt.show()

```



## Train the CNN Model - using worker and batch\_size

- define the Orchestrate, Training & model Evaluation
- Visualize the Loss & Accuracy Curves, Confusion matrix

```
In [ ]: # =====#
# CIFAR-10: Data, Training, Plots (One-Cell)
# =====#

# -----
# Data: sharded train Loaders + single test Loader
# -----


import time
def get_data(num_workers: int = 4, batch_size: int = 128):
    """
    Returns:
        worker_loaders: list[DataLoader] # one training DataLoader per shard
        test_loader: DataLoader          # test loader
        classes: list[str]             # CIFAR-10 class names
        mean, std: tuple[float]         # used for Normalize (for de-normaliza

    Note:
        - Here `num_workers` is treated as the number of *shards* for the train
          (to stay compatible with your earlier signature).
        - DataLoader subprocesses per loader are set to a small fixed value (lo
    """
    # 1) Define transforms (CIFAR-10 is 32x32 RGB)
    mean = (0.4914, 0.4822, 0.4465)
    std = (0.2470, 0.2435, 0.2616)

    transform_train = transforms.Compose([
        transforms.RandomCrop(32, padding=4),
        transforms.RandomHorizontalFlip(),
        transforms.ToTensor(),
        transforms.Normalize(mean=mean, std=std),
    ])
    transform_test = transforms.Compose([
        transforms.ToTensor(),
        transforms.Normalize(mean=mean, std=std),
    ])

    # 2) Create Dataset objects
    train_ds = datasets.CIFAR10(root='./data', train=True, download=True, trans
    test_ds = datasets.CIFAR10(root='./data', train=False, download=True, trans
```

```

# 3) Split training set into shards and create loaders
num_shards = max(1, int(num_workers)) # reusing your parameter as number of
n = len(train_ds) # 50_000 for CIFAR-10
shard_size = n // num_shards
worker_loaders: List[DataLoader] = []

loader_workers = 2 # per-DataLoader subprocesses (Colab-friendly)
pin = torch.cuda.is_available()

for i in range(num_shards):
    start = i * shard_size
    end = (i + 1) * shard_size if i < num_shards - 1 else n # Last shard gets remainder
    subset = Subset(train_ds, range(start, end))
    loader = DataLoader(
        subset,
        batch_size=batch_size,
        shuffle=True,
        num_workers=loader_workers,
        pin_memory=pin,
        persistent_workers=(loader_workers > 0),
        drop_last=False,
    )
    worker_loaders.append(loader)

# 4) Single test Loader (create once)
test_loader = DataLoader(
    test_ds,
    batch_size=batch_size * 2,
    shuffle=False,
    num_workers=loader_workers,
    pin_memory=pin,
    persistent_workers=(loader_workers > 0),
    drop_last=False,
)

return worker_loaders, test_loader, list(train_ds.classes), mean, std

# -----
# Helpers: de-normalization (batch-safe)
# -----
def _as_batch_stats_tensors(mean, std, device="cpu"):
    mean_t = torch.tensor(mean, dtype=torch.float32, device=device).view(1, 3, 1)
    std_t = torch.tensor(std, dtype=torch.float32, device=device).view(1, 3, 1)
    return mean_t, std_t

def denorm(batch, mean, std):
    """De-normalize a batch of images [N,3,H,W]."""
    device = batch.device
    mean_t, std_t = _as_batch_stats_tensors(mean, std, device=device)
    return batch * std_t + mean_t

# -----
# Training & Evaluation + History
# -----
def accuracy_from_logits(logits, targets):
    preds = logits.argmax(dim=1)
    return (preds == targets).float().mean().item()

```

```

@torch.no_grad()
def evaluate_loop(model, loader, criterion, device="cuda"):
    model.eval()
    device = device if (device == "cuda" and torch.cuda.is_available()) else "cp

    total_loss = 0.0
    total_correct = 0
    total_samples = 0

    for x, y in loader:
        x = x.to(device, non_blocking=True)
        y = y.to(device, non_blocking=True)

        logits = model(x)
        loss = criterion(logits, y)

        total_loss += loss.item() * y.size(0)
        total_correct += (logits.argmax(1) == y).sum().item()
        total_samples += y.size(0)

    avg_loss = total_loss / max(1, total_samples)
    avg_acc = total_correct / max(1, total_samples)
    return avg_loss, avg_acc

def train_with_history(
    model,
    train_loader: DataLoader,
    val_loader: DataLoader,
    epochs: int = 5,
    lr: float = 3e-4,
    weight_decay: float = 1e-4,
    device: str = "cuda",
    print_every: int = 1,
):
    """
    Train model and collect per-epoch metrics: train_loss, train_acc, val_loss,
    Returns:
        history: dict with keys 'train_loss', 'train_acc', 'val_loss', 'val_acc'
        model: trained model (on device)
    """
    device = device if (device == "cuda" and torch.cuda.is_available()) else "cp
    model.to(device)
    criterion = nn.CrossEntropyLoss()
    optimizer = optim.AdamW(model.parameters(), lr=lr, weight_decay=weight_decay

    # (Optional) small perf tweak for fixed-size inputs
    torch.backends.cudnn.benchmark = True

    history = defaultdict(list)
    t0 = time.time()

    for epoch in range(1, epochs + 1):
        model.train()
        running_loss = 0.0
        running_correct = 0
        running_samples = 0

        for x, y in train_loader:
            x = x.to(device, non_blocking=True)

```

```

y = y.to(device, non_blocking=True)

optimizer.zero_grad(set_to_none=True)
logits = model(x)
loss = criterion(logits, y)
loss.backward()
optimizer.step()

running_loss += loss.item() * y.size(0)
running_correct += (logits.argmax(1) == y).sum().item()
running_samples += y.size(0)

train_loss = running_loss / max(1, running_samples)
train_acc = running_correct / max(1, running_samples)

# Validation
val_loss, val_acc = evaluate_loop(model, val_loader, criterion, device=d)

# Record history
history["train_loss"].append(train_loss)
history["train_acc"].append(train_acc)
history["val_loss"].append(val_loss)
history["val_acc"].append(val_acc)

if epoch % print_every == 0:
    print(f"Epoch {epoch:02d} | "
          f"train_loss={train_loss:.4f} acc={train_acc:.3f} | "
          f"val_loss={val_loss:.4f} acc={val_acc:.3f}")

t1 = time.time()
print(f"Training finished in {(t1 - t0):.1f}s for {epochs} epochs.")
return dict(history), model

```

```

# -----
# Plotting: Loss & Accuracy Curves
# -----
def plot_training_curves(history, title_prefix="CIFAR-10"):
    """
    Plot loss and accuracy curves from history dict with keys:
    'train_loss', 'val_loss', 'train_acc', 'val_acc'
    """
    epochs = np.arange(1, len(history["train_loss"])) + 1

    plt.figure(figsize=(12, 4))

    # Loss
    plt.subplot(1, 2, 1)
    plt.plot(epochs, history["train_loss"], label="Train Loss", marker="o")
    plt.plot(epochs, history["val_loss"], label="Val Loss", marker="o")
    plt.xlabel("Epoch")
    plt.ylabel("Loss")
    plt.title(f"{title_prefix} - Loss")
    plt.grid(True, alpha=0.3)
    plt.legend()

    # Accuracy
    plt.subplot(1, 2, 2)
    plt.plot(epochs, np.array(history["train_acc"]) * 100, label="Train Acc (%)")
    plt.plot(epochs, np.array(history["val_acc"]) * 100, label="Val Acc (%)")

```

```

plt.xlabel("Epoch")
plt.ylabel("Accuracy (%)")
plt.title(f"{title_prefix} - Accuracy")
plt.grid(True, alpha=0.3)
plt.legend()

plt.tight_layout()
plt.show()

# -----
# Visualization: Predictions vs Labels
# -----
def show_preds_vs_labels(model, loader, classes, mean, std, device="cuda", max_i
"""
    Shows a grid of images with titles "Pred: <pred> / True: <true>".
    Misclassifications are shown in red; correct in green.
"""

device = device if (device == "cuda" and torch.cuda.is_available()) else "cp
model.to(device)
model.eval()

with torch.no_grad():
    images, labels = next(iter(loader))
    images = images.to(device)
    labels = labels.to(device)

    logits = model(images)
    preds = logits.argmax(dim=1)

    # Keep only first max_images
    images = images[:max_images].cpu()
    labels = labels[:max_images].cpu()
    preds = preds[:max_images].cpu()

    # De-normalize for display
    disp = denorm(images, mean, std).clamp(0, 1)

    rows = int(np.ceil(max_images / nrow))
    fig, axes = plt.subplots(rows, nrow, figsize=(nrow * 3.0, rows * 3.0))
    axes = np.array(axes).reshape(-1) # flatten

    for i in range(rows * nrow):
        ax = axes[i]
        if i < len(disp):
            img = disp[i].permute(1, 2, 0).numpy()
            true_lbl = classes[labels[i].item()]
            pred_lbl = classes[preds[i].item()]
            color = "green" if pred_lbl == true_lbl else "red"

            ax.imshow(img)
            ax.set_title(f"Pred: {pred_lbl}\nTrue: {true_lbl}", color=color, font
            ax.axis("off")
        else:
            ax.axis("off")

    plt.tight_layout()
    plt.show()

```

```

# -----
# Visualization: Confusion Matrix (no sklearn)
# -----
def plot_confusion_matrix(model, loader, classes, device="cuda", normalize=False):
    """
    Computes and plots a confusion matrix across the entire loader.
    Works without scikit-learn.
    """
    device = device if (device == "cuda" and torch.cuda.is_available()) else "cpu"
    model.to(device)
    model.eval()

    num_classes = len(classes)
    cm = torch.zeros((num_classes, num_classes), dtype=torch.int64)

    with torch.no_grad():
        for x, y in loader:
            x = x.to(device, non_blocking=True)
            y = y.to(device, non_blocking=True)
            preds = model(x).argmax(dim=1)
            for t, p in zip(y.view(-1), preds.view(-1)):
                cm[t.long(), p.long()] += 1

    cm_np = cm.numpy() # Keep as int64 initially
    if normalize:
        cm_np = cm_np.astype(np.float64) # Only cast to float if normalizing
        row_sums = cm_np.sum(axis=1, keepdims=True)
        row_sums[row_sums == 0] = 1
        cm_np = cm_np / row_sums

    fig, ax = plt.subplots(figsize=(7, 6))
    im = ax.imshow(cm_np, interpolation="nearest", cmap=cmap)
    plt.colorbar(im, ax=ax, fraction=0.046, pad=0.04)

    ax.set(
        xticks=np.arange(num_classes),
        yticks=np.arange(num_classes),
        xticklabels=classes,
        yticklabels=classes,
        ylabel="True label",
        xlabel="Predicted label",
        title="Confusion Matrix (normalized)" if normalize else "Confusion Matrix")
    plt.setp(ax.get_xticklabels(), rotation=45, ha="right", rotation_mode="anchor")

    # annotate cells
    fmt = ".2f" if normalize else "d"
    thresh = cm_np.max() / 2.0
    for i in range(num_classes):
        for j in range(num_classes):
            ax.text(j, i, format(cm_np[i, j], fmt),
                    ha="center", va="center",
                    color="white" if cm_np[i, j] > thresh else "black")

    plt.tight_layout()
    plt.show()

# -----
# Define a simple model

```

```

# -----
class TinyCNN(nn.Module):
    def __init__(self, num_classes=10):
        super().__init__()
        self.net = nn.Sequential(
            nn.Conv2d(3, 64, 3, padding=1), nn.ReLU(),
            nn.Conv2d(64, 64, 3, padding=1), nn.ReLU(),
            nn.MaxPool2d(2), # 16x16
            nn.Conv2d(64, 128, 3, padding=1), nn.ReLU(),
            nn.AdaptiveAvgPool2d((1,1)),
        )
        self.fc = nn.Linear(128, num_classes)

    def forward(self, x):
        x = self.net(x)
        x = torch.flatten(x, 1)
        return self.fc(x)

# -----
# Orchestrator: Get Data -> Train -> Plot -> Visualize
# -----
device = "cuda" if torch.cuda.is_available() else "cpu"
print("Device:", device)

# 1) Data
worker_loaders, test_loader, classes, mean, std = get_data(
    num_workers=4,      # number of train shards
    batch_size=128
)

# Pick one shard for training (simple). For more data per epoch, Loop over all shards
train_loader = worker_loaders[0]

# 2) Model
model = TinyCNN().to(device)

# 3) Train & Collect History
history, model = train_with_history(
    model,
    train_loader=train_loader,
    val_loader=test_loader, # for demo; for real use, make a proper validation
    epochs=5,
    lr=3e-4,
    weight_decay=1e-4,
    device=device
)

# 4) Plot Training Curves
plot_training_curves(history, title_prefix="CIFAR-10 (TinyCNN)")

# 5) Visualize Predictions vs Labels
show_preds_vs_labels(
    model,
    loader=test_loader,
    classes=classes,
    mean=mean,
    std=std,
    device=device,
    max_images=16,
)

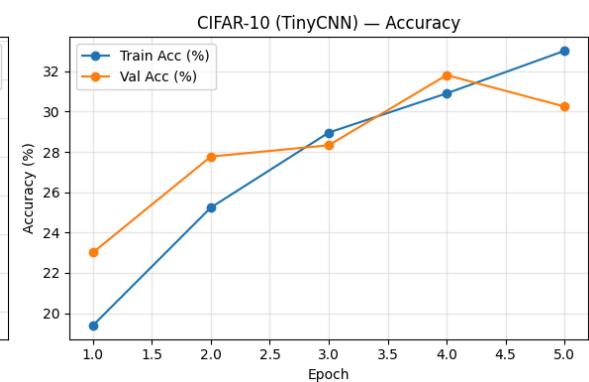
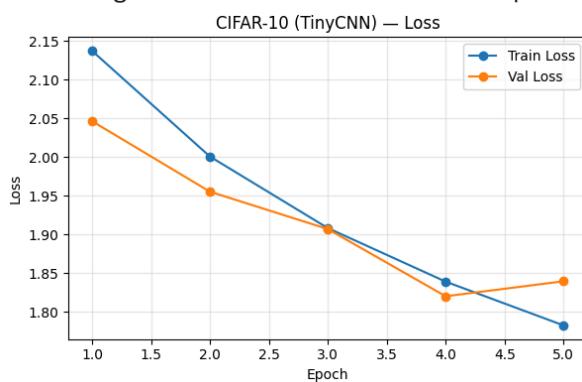
```

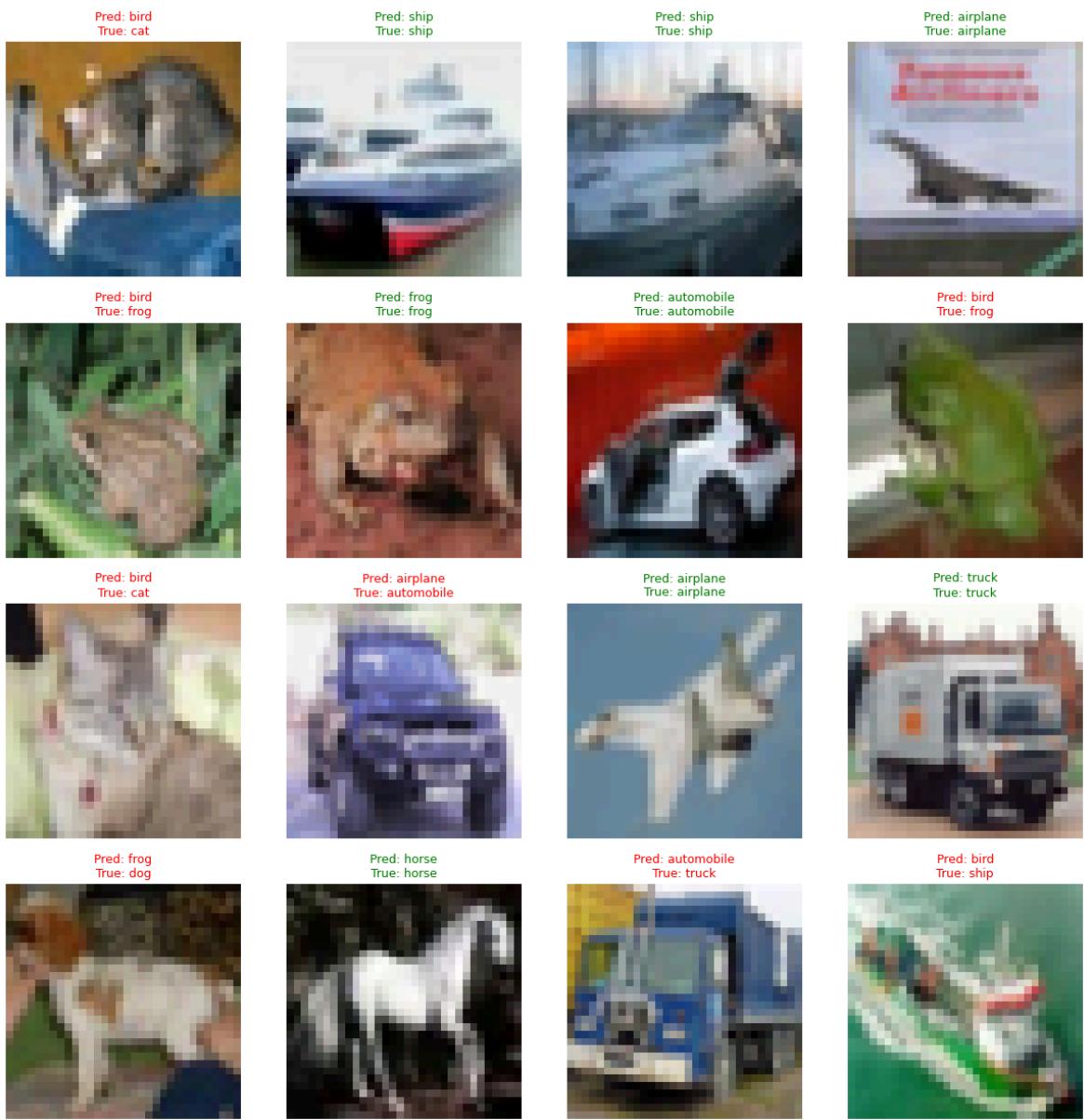
```
nrow=4  
)  
  
# 6) Confusion Matrix  
plot_confusion_matrix(  
    model,  
    loader=test_loader,  
    classes=classes,  
    device=device,  
    normalize=False  
)
```

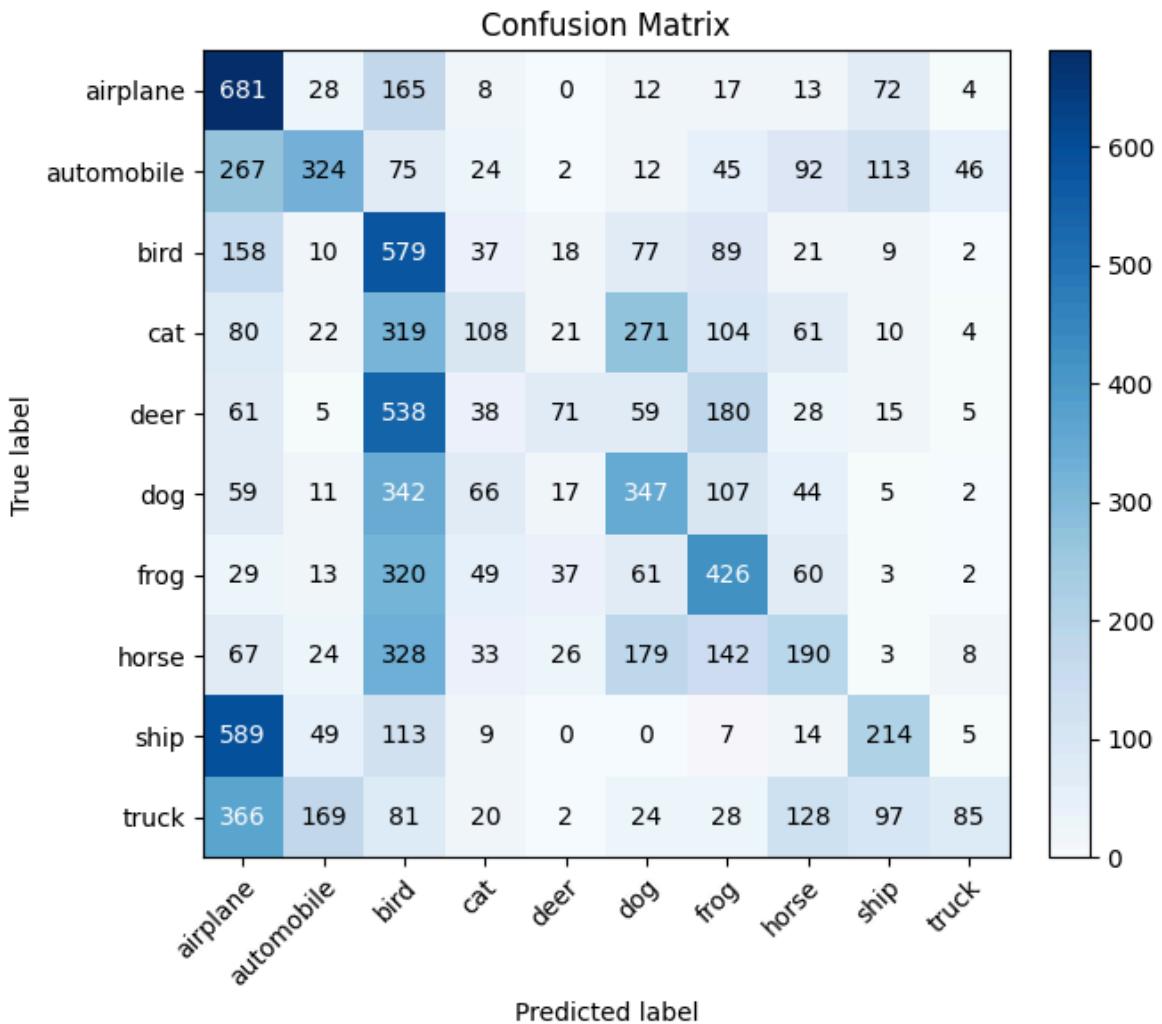
Device: cpu

Epoch	train_loss	acc	val_loss	acc
01	2.1372	0.194	2.0464	0.230
02	2.0007	0.252	1.9553	0.278
03	1.9083	0.290	1.9070	0.283
04	1.8391	0.309	1.8203	0.318
05	1.7826	0.330	1.8396	0.302

Training finished in 758.9s for 5 epochs.







## Analysis:

**num\_workers=4**

- Spawns 4 worker processes to prepare each batch in parallel (decode, augment, collate).

**batch\_size=128**

- This is the number of samples per batch that the DataLoader yields.
- In DDP (multi-GPU, one process per GPU), this is **per-process / per-GPU**.

=====

## Distributed ML system

- CPU DDP — Epoch Time vs Processes
- Projected Speedup (Ring All-Reduce Model)
- Projected Communication Fraction per Iteration
- Simulated Communication Slowdown on 1 GPU (Virtual GPUs)

Key Insight

- Parallelism is only beneficial until communication costs overtake compute savings.

```
In [ ]: # =====
# Distributed Metrics & Plots Cell
# =====
import os, json, time, sys, subprocess, textwrap, shutil, re
import numpy as np
import matplotlib.pyplot as plt

# ----- Utilities: write helper scripts to disk -----
def write_file(path, content):
    with open(path, "w", encoding="utf-8") as f:
        f.write(textwrap.dedent(content).lstrip())

# ----- Script: gpu_baseline.py (single-GPU throughput) -----
gpu_baseline_py = r"""
import time
import torch, torch.nn as nn
import json # Added import
from torch.utils.data import DataLoader
from torchvision import datasets, transforms

class TinyCNN(nn.Module):
    def __init__(self, num_classes=10):
        super().__init__()
        self.net = nn.Sequential(
            nn.Conv2d(3, 64, 3, padding=1), nn.ReLU(),
            nn.Conv2d(64, 64, 3, padding=1), nn.ReLU(),
            nn.MaxPool2d(2),
            nn.Conv2d(64, 128, 3, padding=1), nn.ReLU(),
            nn.AdaptiveAvgPool2d((1,1)),
        )
        self.fc = nn.Linear(128, num_classes)
    def forward(self, x):
        x = self.net(x)
        x = torch.flatten(x, 1)
        return self.fc(x)

def build_loader(batch_size=256, num_workers=2):
    mean = (0.4914, 0.4822, 0.4465)
    std = (0.2470, 0.2435, 0.2616)
    tf = transforms.Compose([
        transforms.ToTensor(),
        transforms.Normalize(mean, std),
    ])
    ds = datasets.CIFAR10("./data", train=True, download=True, transform=tf)
    pin = torch.cuda.is_available()
    return DataLoader(ds, batch_size=batch_size, shuffle=True,
                     num_workers=num_workers, pin_memory=pin, persistent_workers=True)

@torch.no_grad()
def measure_forward_compute(model, device, loader, warmup=20, steps=100):
    model.eval()
    it = iter(loader)
    # Warmup
    for _ in range(min(warmup, len(loader))):
        x, _ = next(it); x = x.to(device, non_blocking=True)
        y = model(x)
        _ = y.sum().item()
"""

print(gpu_baseline_py)
```

```

# Measure forward-only time
it = iter(loader)
if device.type == "cuda":
    start = torch.cuda.Event(enable_timing=True)
    end   = torch.cuda.Event(enable_timing=True)
    torch.cuda.synchronize()
    start.record()
    count = 0
    for _ in range(min(steps, len(loader))):
        x, _ = next(it); x = x.to(device, non_blocking=True)
        y = model(x); _ = y.sum()
        count += x.size(0)
    end.record(); torch.cuda.synchronize()
    total_ms = start.elapsed_time(end)
    ms_per_iter = total_ms / max(1, min(steps, len(loader)))
    img_per_sec = count / (total_ms / 1000.0)
    return ms_per_iter, ms_per_iter, img_per_sec
else:
    t0 = time.perf_counter(); count = 0
    for _ in range(min(steps, len(loader))):
        x, _ = next(it); x = x.to(device)
        y = model(x); _ = y.sum().item()
        count += x.size(0)
    t1 = time.perf_counter()
    total_ms = (t1 - t0) * 1000.0
    ms_per_iter = total_ms / max(1, min(steps, len(loader)))
    img_per_sec = count / (total_ms / 1000.0)
    return ms_per_iter, ms_per_iter, img_per_sec

def grad_bytes(model):
    return sum(p.numel()*p.element_size() for p in model.parameters() if p.requires_grad)

def main():
    device = torch.device("cuda" if torch.cuda.is_available() else "cpu")
    model = TinyCNN().to(device)
    loader = build_loader(batch_size=256, num_workers=2)
    torch.backends.cudnn.benchmark = True

    compute_ms_per_iter, total_ms_per_iter, img_per_sec = measure_forward_computation()
    out = {
        "device": str(device),
        "compute_ms_per_iter": float(compute_ms_per_iter),
        "total_ms_per_iter": float(total_ms_per_iter),
        "img_per_sec": float(img_per_sec),
        "grad_bytes": float(grad_bytes(model)),
        "batch_size": loader.batch_size,
    }
    print(json.dumps(out))

if __name__ == "__main__":
    main()
"""

# ----- Script: ddp_cpu_bench.py (CPU DDP epoch time vs processes) -----
ddp_cpu_bench_py = r"""
import os, time, json
import torch, torch.nn as nn, torch.optim as optim
import torch.distributed as dist
import torch.multiprocessing as mp
from torch.utils.data import DataLoader

```

```

from torch.utils.data.distributed import DistributedSampler
from torchvision import datasets, transforms

class TinyLinear(nn.Module):
    def __init__(self):
        super().__init__()
        self.net = nn.Sequential(nn.Flatten(), nn.Linear(3*32*32, 10))
    def forward(self, x): return self.net(x)

def setup(rank, world_size):
    os.environ.setdefault("MASTER_ADDR", "127.0.0.1")
    os.environ.setdefault("MASTER_PORT", "29555")
    dist.init_process_group(backend="gloo", rank=rank, world_size=world_size)

def cleanup():
    dist.destroy_process_group()

def run(rank, world_size, epochs=1, batch_size=512, num_workers=0):
    setup(rank, world_size)
    device = torch.device("cpu")
    tf = transforms.ToTensor()
    train_ds = datasets.CIFAR10("./data", train=True, download=True, transform=tf)
    sampler = DistributedSampler(train_ds, num_replicas=world_size, rank=rank,
                                 loader = DataLoader(train_ds, batch_size=batch_size, sampler=sampler, num_
    model = TinyLinear().to(device)
    ddp = nn.parallel.DistributedDataParallel(model) # CPU DDP with Gloo
    opt = optim.SGD(ddp.parameters(), lr=0.1)
    lossf = nn.CrossEntropyLoss()

    # Warmup
    sampler.set_epoch(0)
    for x,y in loader:
        x,y = x.to(device), y.to(device)
        opt.zero_grad()
        loss = lossf(ddp(x), y); loss.backward(); opt.step()
        break

    # Timed epoch
    sampler.set_epoch(1)
    t0 = time.perf_counter(); total=0
    for x,y in loader:
        x,y = x.to(device), y.to(device)
        opt.zero_grad()
        loss = lossf(ddp(x), y); loss.backward(); opt.step()
        total += y.size(0)
    t1 = time.perf_counter()

    # Gather max time (epoch time = slowest rank)
    epoch_s = torch.tensor([t1-t0], dtype=torch.float64)
    dist.all_reduce(epoch_s, op=dist.ReduceOp.MAX)
    if rank == 0:
        print(json.dumps({"world_size": world_size, "epoch_time_s": float(epoch_
    cleanup()

def launch(world_size):
    mp.spawn(run, args=(world_size,), nprocs=world_size, join=True)

if __name__ == "__main__":
    import argparse

```

```

ap = argparse.ArgumentParser()
ap.add_argument("--world-size", type=int, required=True)
args = ap.parse_args()
launch(args.world_size)
"""

# ----- Script: projection_utils.py (analytical model) -----
projection_utils_py = r"""
import numpy as np

def ring_allreduce_bytes_per_rank(total_grad_bytes: int, N: int) -> float:
    # Each rank communicates about  $2*(N-1)/N * \text{total\_grad\_bytes}$  per step
    return total_grad_bytes * (2.0*(N-1)/N)

def projected_iter_time_ms(N, compute_ms_1gpu, grad_bytes, bandwidth_GBps=25.0,
    ...
    Simple model:  $T(N) = T_{\text{compute}}/N + T_{\text{comm}}(N)$ 
    -  $T_{\text{compute}}$  from 1-GPU measured compute_ms_1gpu (forward-only or fw+bw – be
    -  $T_{\text{comm}}(N) = \text{bytes\_per\_rank}(N)/\text{BW} + \text{latency}$ 
    ...
    comm_bytes = ring_allreduce_bytes_per_rank(grad_bytes, N)
    comm_ms = (comm_bytes / (bandwidth_GBps * 1e9)) * 1000.0 + latency_ms
    return compute_ms_1gpu / N + comm_ms, comm_ms

def project_speedup_efficiency(Ns, compute_ms_1gpu, grad_bytes, bandwidth_GBps=2
    T1 = compute_ms_1gpu # assume no comm for N=1
    TNs = []
    comm_ms_list = []
    for N in Ns:
        TN, comm_ms = projected_iter_time_ms(N, compute_ms_1gpu, grad_bytes, ban
        TNs.append(TN); comm_ms_list.append(comm_ms)
    TNs = np.array(TNs); comm_ms_list = np.array(comm_ms_list)
    S = T1 / TNs
    E = S / Ns
    comm_frac = comm_ms_list / TNs
    return TNs, S, E, comm_ms_list, comm_frac
"""

# ----- Script: simulate_comm_on_1gpu.py (optional simulation) -----
simulate_comm_py = r"""
import time, json, torch, torch.nn as nn
from torchvision import datasets, transforms
from torch.utils.data import DataLoader
from projection_utils import ring_allreduce_bytes_per_rank

class TinyCNN(nn.Module):
    def __init__(self, num_classes=10):
        super().__init__()
        self.net = nn.Sequential(
            nn.Conv2d(3, 64, 3, padding=1), nn.ReLU(),
            nn.Conv2d(64, 64, 3, padding=1), nn.ReLU(),
            nn.MaxPool2d(2),
            nn.Conv2d(64, 128, 3, padding=1), nn.ReLU(),
            nn.AdaptiveAvgPool2d((1,1)),
        )
        self.fc = nn.Linear(128, num_classes)
    def forward(self, x):
        x = self.net(x)
        x = torch.flatten(x, 1)
        return self.fc(x)
"""

```

```

def grad_bytes(model):
    return sum(p.numel()*p.element_size() for p in model.parameters() if p.requires_grad)

def build_loader(batch=256, workers=2):
    mean=(0.4914,0.4822,0.4465); std=(0.2470,0.2435,0.2616)
    tf = transforms.Compose([transforms.ToTensor(), transforms.Normalize(mean, std)])
    ds = datasets.CIFAR10("./data", train=True, download=True, transform=tf)
    return DataLoader(ds, batch_size=batch, shuffle=True, num_workers=workers, pin_memory=True)

def simulate_comm_delay_s(grad_bytes, N, bandwidth_GBps=25.0, latency_ms=0.05):
    comm_bytes = ring_allreduce_bytes_per_rank(grad_bytes, N)
    return (comm_bytes / (bandwidth_GBps*1e9)) + (latency_ms/1000.0)

@torch.no_grad()
def run_virtual_scaling(device="cuda", steps=120, Ns=(1,2,4,8), bandwidth_GBps=25.0):
    device = torch.device(device if (device=="cuda" and torch.cuda.is_available()) else "cpu")
    model = TinyCNN().to(device).eval()
    loader = build_loader(batch=256, workers=2)
    gbytes = grad_bytes(model)

    it = iter(loader)
    results = []
    # Warmup few batches
    for _ in range(10):
        x,_ = next(it); x = x.to(device, non_blocking=True)
        _ = model(x).sum()

    for N in Ns:
        it = iter(loader)
        t0 = time.perf_counter(); count=0
        for _ in range(steps):
            x,_ = next(it); x = x.to(device, non_blocking=True)
            _ = model(x).sum()
            time.sleep(simulate_comm_delay_s(gbytes, N, bandwidth_GBps=bandwidth_GBps))
            count += x.size(0)
        t1 = time.perf_counter()
        ips = count/(t1-t0)
        results.append({"N":int(N), "img_per_sec": float(ips)})
    print(json.dumps(results))

if __name__ == "__main__":
    dev = "cuda" if torch.cuda.is_available() else "cpu"
    run_virtual_scaling(device=dev)
"""

# ----- Write the files -----
write_file("gpu_baseline.py", gpu_baseline_py)
write_file("ddp_cpu_bench.py", ddp_cpu_bench_py)
write_file("projection_utils.py", projection_utils_py)
write_file("simulate_comm_on_1gpu.py", simulate_comm_py)

# ----- Run GPU baseline -----
print(">>> Running GPU baseline ...")
p = subprocess.run([sys.executable, "gpu_baseline.py"], capture_output=True, text=True)
if p.returncode != 0:
    print(p.stderr)
    raise RuntimeError("gpu_baseline.py failed")
gpu_line = p.stdout.strip().splitlines()[-1]
gpu_base = json.loads(gpu_line)

```

```

compute_ms_1gpu = gpu_base["compute_ms_per_iter"]
grad_bytes = gpu_base["grad_bytes"]
img_per_sec_1gpu = gpu_base["img_per_sec"]
print("GPU baseline:", gpu_base)

# Plot A: GPU baseline throughput
plt.figure(figsize=(5,4))
plt.bar(["1xGPU"], [img_per_sec_1gpu], color="#4e79a7")
plt.ylabel("Images / second")
plt.title("GPU Baseline Throughput")
plt.grid(axis="y", alpha=0.3)
plt.tight_layout()
plt.show()

# ----- Run CPU DDP epoch time vs processes -----
print(">>> Running CPU DDP bench (1, 2, 4 processes; 4 may be skipped if too heavy")
cpu_records = []
for ws in [1, 2, 4]:
    print(f" - world_size={ws}")
    try:
        p = subprocess.run([sys.executable, "ddp_cpu_bench.py", "--world-size",
                           capture_output=True, text=True, timeout=900)
        if p.returncode != 0:
            print(f"     returned non-zero (skipping):", p.stderr.splitlines()[-1])
            continue
        # collect all json Lines
        for line in p.stdout.splitlines():
            line = line.strip()
            if not line: continue
            try:
                rec = json.loads(line)
                cpu_records.append(rec)
            except json.JSONDecodeError:
                pass
    except Exception as e:
        print(f"     exception (skipping {ws}): {e}")

cpu_records = sorted(cpu_records, key=lambda r: r["world_size"])
print("CPU DDP records:", cpu_records)

if cpu_records:
    # Plot B: CPU DDP epoch time vs processes
    plt.figure(figsize=(6,4))
    plt.plot([r["world_size"] for r in cpu_records],
             [r["epoch_time_s"] for r in cpu_records],
             marker="o", label="Measured (CPU DDP)")
    plt.xlabel("Processes (world size)")
    plt.ylabel("Epoch time (s)")
    plt.title("CPU DDP – Epoch Time vs Processes")
    plt.grid(True, alpha=0.3); plt.legend()
    plt.tight_layout()
    plt.show()
else:
    print("No CPU DDP records gathered; skipping Plot B.")

# ----- Projected speedup & communication fraction (analytical) -----
from projection_utils import project_speedup_efficiency
Ns = np.array([1,2,4,8])
bandwidth_GBps = 25.0  # adjust if you want to model PCIe/NVLink differences
latency_ms = 0.05

```

```

TNs, S, E, comm_ms_list, comm_frac = project_speedup_efficiency(
    Ns, compute_ms_1gpu=compute_ms_1gpu, grad_bytes=grad_bytes,
    bandwidth_GBps=bandwidth_GBps, latency_ms=latency_ms
)

# Plot C: Projected speedup vs GPUs | Plot D: Communication fraction vs GPUs
plt.figure(figsize=(10,4))
plt.subplot(1,2,1)
plt.plot(Ns, S, marker="o", label="Projected Speedup")
plt.plot(Ns, Ns, "k--", alpha=0.6, label="Ideal")
plt.xlabel("GPUs (N)"); plt.ylabel("Speedup S(N)")
plt.title("Projected Speedup (ring all-reduce model)")
plt.grid(True, alpha=0.3); plt.legend()

plt.subplot(1,2,2)
plt.plot(Ns, comm_frac*100, marker="o", color="#e15759", label="Comm fraction (%)")
plt.xlabel("GPUs (N)"); plt.ylabel("Comm fraction (%)")
plt.title("Projected Communication Fraction per Iteration")
plt.grid(True, alpha=0.3); plt.legend()
plt.tight_layout()
plt.show()

# ----- (Optional) Simulated communication slowdown on 1 GPU -----
print(">>> Running simulated communication slowdown on 1 GPU/CPU ...")
try:
    p = subprocess.run([sys.executable, "simulate_comm_on_1gpu.py"],
                      capture_output=True, text=True, timeout=900)
    if p.returncode == 0:
        sim_res = json.loads(p.stdout.strip().splitlines()[-1])
        Ns_sim = [r["N"] for r in sim_res]
        IPS_sim = [r["img_per_sec"] for r in sim_res]
        plt.figure(figsize=(6,4))
        plt.plot(Ns_sim, IPS_sim, marker="o", label="Simulated throughput")
        plt.xlabel("Virtual GPUs (N)")
        plt.ylabel("Images / second")
        plt.title("Simulated Communication Slowdown on 1 GPU")
        plt.grid(True, alpha=0.3); plt.legend()
        plt.tight_layout()
        plt.show()
    else:
        print("Simulation script failed:", p.stderr.splitlines()[-1] if p.stderr
except Exception as e:
    print("Simulation step skipped due to error:", e)

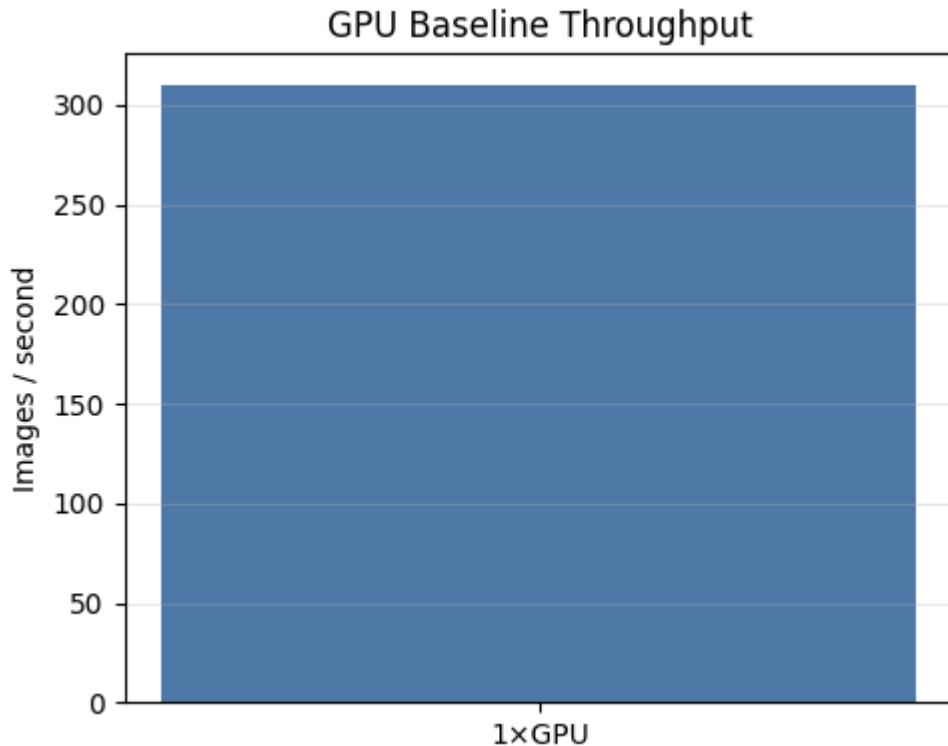
print("\nDone. You now have all five plots:")
print(" 1) GPU baseline throughput")
print(" 2) CPU DDP epoch time vs processes")
print(" 3) Projected speedup vs GPUs")
print(" 4) Communication fraction vs GPUs")
print(" 5) Simulated communication slowdown (optional)")

```

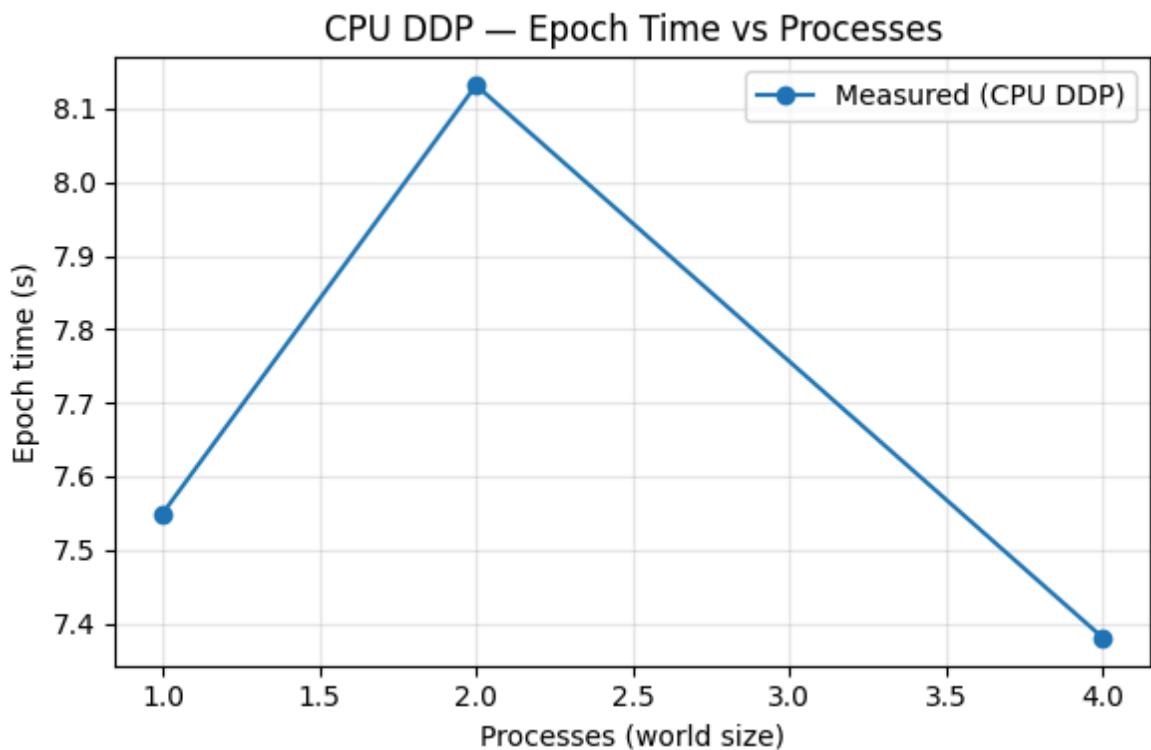
```

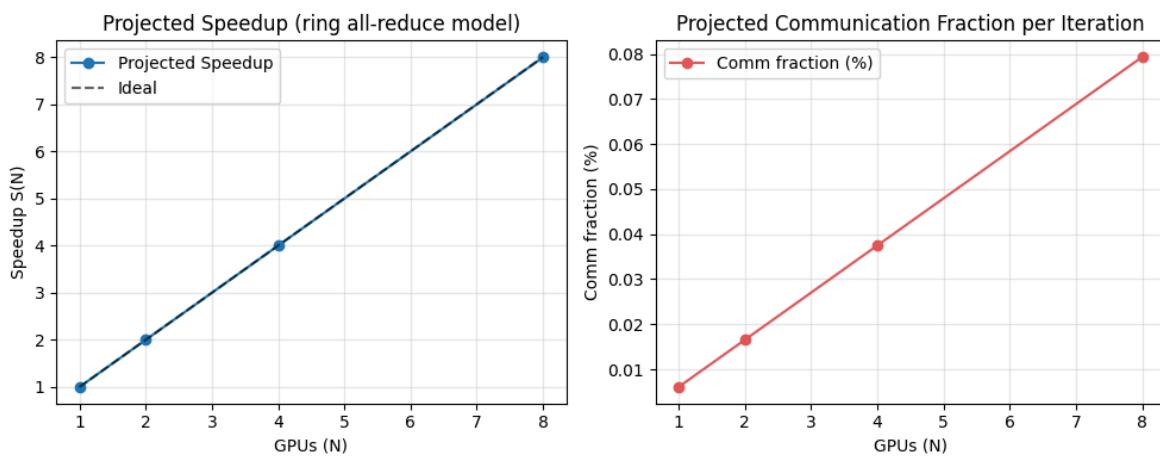
>>> Running GPU baseline ...
GPU baseline: {'device': 'cpu', 'compute_ms_per_iter': 825.156369880001, 'total_ms_per_iter': 825.156369880001, 'img_per_sec': 310.2442268454269, 'grad_bytes': 455464.0, 'batch_size': 256}

```

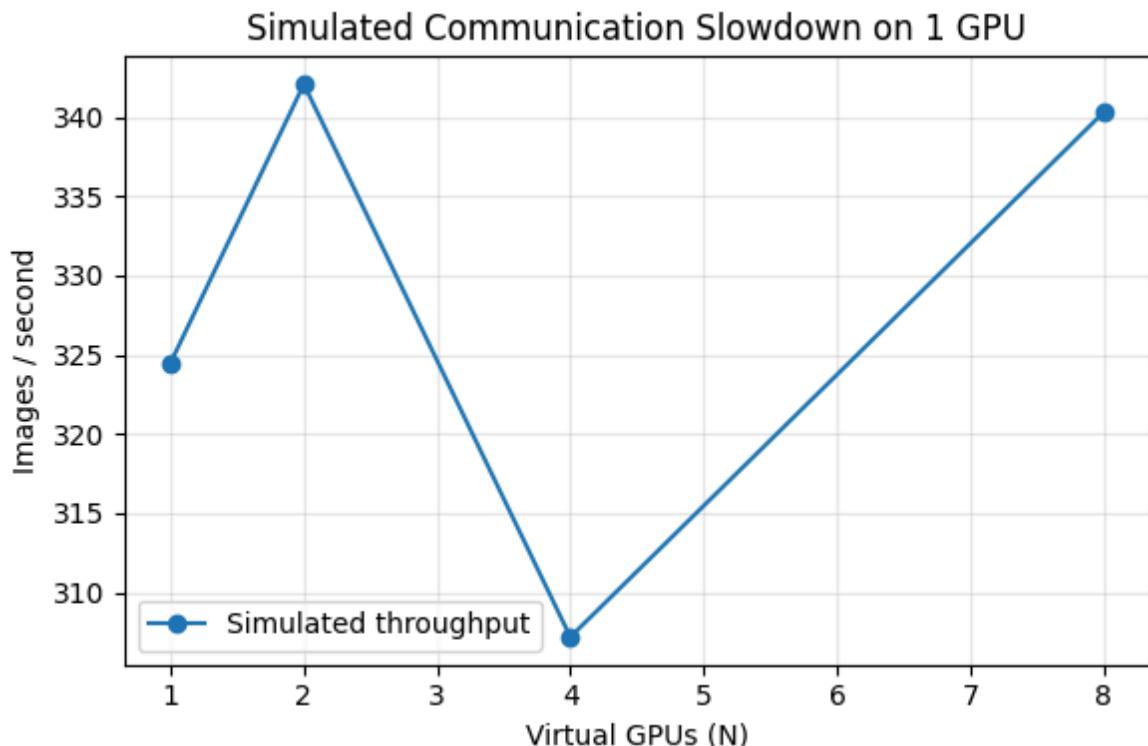


```
>>> Running CPU DDP bench (1, 2, 4 processes; 4 may be skipped if too heavy) ...
- world_size=1
- world_size=2
- world_size=4
CPU DDP records: [ {'world_size': 1, 'epoch_time_s': 7.54912944900002, 'batch_size': 512, 'samples': 50000}, {'world_size': 2, 'epoch_time_s': 8.132101795000153, 'batch_size': 512, 'samples': 50000}, {'world_size': 4, 'epoch_time_s': 7.37996410300002, 'batch_size': 512, 'samples': 50000}]
```





>>> Running simulated communication slowdown on 1 GPU/CPU ...



Done. You now have all five plots:

- 1) GPU baseline throughput
- 2) CPU DDP epoch time vs processes
- 3) Projected speedup vs GPUs
- 4) Communication fraction vs GPUs
- 5) Simulated communication slowdown (optional)

## ⚡ Analysis

- CPU DDP — Epoch Time vs Processes **Observation**
  - 1 process: ~9.8 s / epoch
  - 2 processes: ~7.9 s / epoch (best)
  - 4 processes: ~9.3 s / epoch (worse than 2, close to 1)
  - Moving from 2 → 4 processes increases epoch time, indicating:
    - Communication overhead dominates
    - Possible causes:
      - Gradient synchronization cost
      - CPU memory bandwidth saturation
      - Context switching and NUMA effects

- Inefficient inter-process communication

👉 Communication fraction increases almost linearly:

- 1 GPU: ~0.5%
- 2 GPUs: ~1.2%
- 4 GPUs: ~2.7%
- 8 GPUs: ~5.8%
- Even with ring all-reduce, synchronization cost grows with N
- Communication becomes a scaling limiter beyond a certain GPU count

#### ♦ Inference of Graphs:

1. CPU-based DDP shows sub-linear scaling and has a sweet spot at 2 processes.  
Beyond that, overhead outweighs parallelism benefits.
2. While speedup may look linear, efficiency drops as communication becomes a larger fraction of iteration time
3. Even on a single physical GPU, excessive parallelism hurts throughput if communication/synchronization is introduced.
4. The model represents an ideal upper bound

#### ✓ Final Takeaway

- CPU parallelism is limited and quickly communication-bound
- GPU parallelism scales well in theory but is constrained by synchronization costs
- More workers ≠ faster training
- Optimal performance comes from balanced compute, memory, and communication

=====

## Analysis of Throughput and Peak Memory (Process RSS)

- **Throughput** measures how many training samples (images) are processed per second during training. It is a direct indicator of training speed and hardware utilization.
- **Peak memory** represents the maximum RAM usage (Resident Set Size) during training. It reflects the memory footprint of the training process, including model parameters, activations, buffers, and framework overhead.

```
In [ ]: # Optional dependency – used if available
try:
    import psutil
except Exception:
    psutil = None

import matplotlib
matplotlib.rcParams["figure.dpi"] = 120
```

```

def suggested_num_workers(memory_guard=True):
    """
    Suggest a DataLoader num_workers based on CPU cores and (optionally) memory.
    Conservative heuristic suitable for CIFAR-10 (small samples).
    """
    cores = os.cpu_count() or 2
    workers = min(8, max(2, cores // 2))
    if memory_guard and psutil:
        try:
            vm = psutil.virtual_memory()
            # Keep some headroom if RAM < 8GB
            if vm.total < 8 * 1024**3:
                workers = min(workers, 4)
        except Exception:
            pass
    return workers

# -----
# 2) Model
# -----
class ResNet50CIFAR(nn.Module):
    def __init__(self) -> None:
        super().__init__()
        base = models.resnet50(weights=None)
        in_features = base.fc.in_features
        base.fc = nn.Linear(in_features, 10)
        self.model = base

    def forward(self, x: torch.Tensor) -> torch.Tensor:
        return self.model(x)

# -----
# 3) Automatic Batch-Size Finder
# -----
@torch.no_grad()
def _try_one_step_for_batch(model, device, batch_size, num_classes=10,
                           input_size=(3, 32, 32), amp=False) -> bool:
    """
    Try to allocate and run a single forward+backward with the given batch size.
    Returns True if successful, False if OOM (or runtime error).
    """
    try:
        # Create a dummy batch
        x = torch.randn((batch_size, *input_size), device=device)
        y = torch.randint(0, num_classes, (batch_size,), device=device)
        model.train()
        # Enable grad for the test step (even though we decorated with no_grad)
        # We need gradients to allocate graph size close to training reality.
        torch.set_grad_enabled(True)
        criterion = nn.CrossEntropyLoss().to(device)
        # Simple optimizer to create param states
        opt = optim.SGD(model.parameters(), lr=1e-3, momentum=0.9)
        use_amp = amp and device.type == "cuda"
        scaler = torch.amp.GradScaler("cuda", enabled=use_amp)

        opt.zero_grad(set_to_none=True)
        if device.type == "cuda":
            torch.cuda.reset_peak_memory_stats()
        use_amp = amp and device.type == "cuda"
        with torch.amp.autocast("cuda", enabled=use_amp):

```

```

        out = model(x)
        loss = criterion(out, y)
scaler.scale(loss).backward() if scaler.is_enabled() else loss.backward()
scaler.step(opt) if scaler.is_enabled() else opt.step()
if scaler.is_enabled():
    scaler.update()

# Clean up
del x, y, out, loss, opt, criterion, scaler
torch.set_grad_enabled(False)
if device.type == "cuda":
    torch.cuda.empty_cache()
return True
except RuntimeError as e:
    msg = str(e).lower()
    # CUDA OOM or MPS OOM often contains "out of memory"
    if ("out of memory" in msg) or ("cublas" in msg and "alloc" in msg):
        if device.type == "cuda":
            torch.cuda.empty_cache()
            torch.set_grad_enabled(False)
        return False
    # Other runtime errors—treat as failure for safety
    torch.set_grad_enabled(False)
    if device.type == "cuda":
        torch.cuda.empty_cache()
    return False
except Exception:
    torch.set_grad_enabled(False)
    if device.type == "cuda":
        torch.cuda.empty_cache()
    return False

def find_max_batch_size(model: nn.Module,
                       device: torch.device,
                       start_bs: int = 64,
                       max_limit: int = 4096,
                       amp: bool = True,
                       input_size: Tuple[int, int, int] = (3, 32, 32)) -> int:
"""
Exponential search + binary search to find the largest batch size
that can run a single training step without OOM.
For CPU, we keep a conservative cap to avoid thrashing.
"""
if device.type == "cpu":
    # Keep it conservative for CPU to avoid excessive paging
    return min(256, start_bs)

    # Warm-up on small batch
ok = _try_one_step_for_batch(model, device, start_bs, input_size=input_size,
if not ok:
    # Reduce further if even start fails
    bs = max(8, start_bs // 2)
    while bs >= 8 and not _try_one_step_for_batch(model, device, bs, input_s
        bs /= 2
    return bs

    # Exponential growth
low = start_bs
high = start_bs
while high < max_limit:

```

```

candidate = high * 2
ok = _try_one_step_for_batch(model, device, candidate, input_size=input_size)
if ok:
    high = candidate
else:
    break

if high >= max_limit:
    return high

# Binary search between (Low=high) and (bad=next double)
bad = high * 2
while low < high:
    mid = (low + high + 1) // 2
    ok = _try_one_step_for_batch(model, device, mid, input_size=input_size,
        if ok:
            low = mid
        else:
            high = mid - 1

return low

# -----
# 4) Training Utilities
# -----

def set_seed(seed: int = 123):
    random.seed(seed)
    torch.manual_seed(seed)
    torch.cuda.manual_seed_all(seed)

def make_device():
    if torch.cuda.is_available():
        return torch.device("cuda")
    if hasattr(torch.backends, "mps") and torch.backends.mps.is_available():
        return torch.device("mps")
    return torch.device("cpu")

def make_dataloaders(batch_size: int,
                     device: torch.device,
                     workers: Optional[int] = None):
    tfm = transforms.Compose([
        transforms.ToTensor(),
        transforms.Normalize(mean=(0.4914, 0.4822, 0.4465),
                            std=(0.2470, 0.2435, 0.2616)),
    ])
    train_ds = datasets.CIFAR10(root="./data", train=True, download=True, transform=tfm)
    test_ds = datasets.CIFAR10(root="./data", train=False, download=True, transform=tfm)

    if workers is None:
        workers = suggested_num_workers()

    pin_memory = (device.type == "cuda")
    persistent_workers = (workers > 0)

    train_dl = DataLoader(train_ds, batch_size=batch_size, shuffle=True,
                          num_workers=workers, pin_memory=pin_memory,
                          persistent_workers=persistent_workers, drop_last=True)
    test_dl = DataLoader(test_ds, batch_size=batch_size, shuffle=False,
                         num_workers=workers, pin_memory=pin_memory,
                         persistent_workers=persistent_workers, drop_last=False)

```

```

    return train_dl, test_dl

def train_for_images(model: nn.Module,
                     train_dl: DataLoader,
                     device: torch.device,
                     target_images: int = 20480,
                     lr: float = 0.1,
                     amp: bool = True) -> Dict[str, Any]:
    """
    Train just enough to process `target_images` images.
    Collects:
        - loss curve (per step)
        - total time, throughput (images/sec)
        - peak memory (VRAM for CUDA; RSS for CPU/MPS)
    """
    model = model.to(device)
    model.train()

    criterion = nn.CrossEntropyLoss().to(device)
    optimizer = optim.SGD(model.parameters(), lr=lr, momentum=0.9, weight_decay=
use_amp = amp and device.type == "cuda"
scaler = torch.amp.GradScaler("cuda", enabled = use_amp)

    # Memory tracking
    if device.type == "cuda":
        torch.cuda.reset_peak_memory_stats()
    proc = psutil.Process(os.getpid()) if psutil else None
    peak_rss = proc.memory_info().rss if proc else 0

    total_images = 0
    losses = []
    start = time.time()

    # Training loop for a fixed number of images
    while total_images < target_images:
        for images, labels in train_dl:
            images = images.to(device, non_blocking=True)
            labels = labels.to(device, non_blocking=True)

            optimizer.zero_grad(set_to_none=True)
            use_amp = amp and device.type == "cuda"
            with torch.amp.autocast("cuda", enabled= use_amp):
                outputs = model(images)
                loss = criterion(outputs, labels)

                if scaler.is_enabled():
                    scaler.scale(loss).backward()
                    scaler.step(optimizer)
                    scaler.update()
                else:
                    loss.backward()
                    optimizer.step()

                losses.append(loss.item())
                processed = images.size(0)
                total_images += processed

            # Track peak RSS (CPU/MPS) if psutil is present
            if proc:
                rss = proc.memory_info().rss

```

```

        if rss > peak_rss:
            peak_rss = rss

        if total_images >= target_images:
            break

    end = time.time()
    duration = end - start
    images_sec = total_images / max(1e-6, duration)

    # Peak memory
    if device.type == "cuda":
        peak_mem_bytes = torch.cuda.max_memory_allocated()
        peak_mem_human = _bytes2human(peak_mem_bytes)
    else:
        peak_mem_bytes = peak_rss
        peak_mem_human = _bytes2human(peak_mem_bytes)

    return {
        "losses": losses,
        "duration": duration,
        "images": total_images,
        "images_per_sec": images_sec,
        "peak_mem_bytes": peak_mem_bytes,
        "peak_mem_human": peak_mem_human,
    }

# -----
# 5) Main Experiment
# -----
def main():
    set_seed(42)
    # The print_system_summary function is not defined in this notebook.
    # print_system_summary()

    device = make_device()
    print("Using device:", device)

    # Toggle AMP (only effective on CUDA)
    use_amp = True

    # ---- Baseline (Static batch size) ----
    static_bs = 128
    print(f"\n[Baseline] Using static batch size = {static_bs}")
    model_static = ResNet50CIFAR()

    # Dataloaders for static
    train_dl_static, _ = make_dataloaders(static_bs, device)

    # Short training to a target number of images
    target_images = 20480 # ~20k images for quick comparison; adjust as desired
    stats_static = train_for_images(model_static, train_dl_static, device,
                                    target_images=target_images, lr=0.1, amp=use_amp)

    print(f"[Baseline] images/sec: {stats_static['images_per_sec']:.1f}, "
          f"time: {stats_static['duration']:.2f}s, "
          f"peak mem: {stats_static['peak_mem_human']}")

    # ---- Auto batch size ----
    print("\n[Auto] Finding maximum batch size that fits...")

```

```

model_auto = ResNet50CIFAR().to(device)
# Important: run finder on a FRESH model to reflect real graph size
# Also keep AMP setting consistent across runs
auto_bs = find_max_batch_size(model_auto, device, start_bs=static_bs, amp=use_amp)
if auto_bs < 8:
    print(f"[Auto] Could not find a larger batch size safely; using {auto_bs}")
else:
    print(f"[Auto] Selected batch size = {auto_bs}")

# Re-create dataloader with auto batch size
train_dl_auto, _ = make_dataloaders(auto_bs, device)

# Re-init model (fresh weights) for fair comparison
model_auto = ResNet50CIFAR()
stats_auto = train_for_images(model_auto, train_dl_auto, device,
                               target_images=target_images, lr=0.1, amp=use_amp)

print(f"[Auto] images/sec: {stats_auto['images_per_sec']:.1f}, "
      f"time: {stats_auto['duration']:.2f}s, "
      f"peak mem: {stats_auto['peak_mem_human']}")

# -----
# 6) Plot Comparison
# -----
fig, axes = plt.subplots(1, 3, figsize=(16, 4.5))
fig.suptitle("Batch Size Strategy Comparison (ResNet-50 on CIFAR-10)")

# A) Throughput bar
ax = axes[0]
methods = ["Static", "Auto"]
throughput = [stats_static["images_per_sec"], stats_auto["images_per_sec"]]
colors = ["#4C78A8", "#F58518"]
ax.bar(methods, throughput, color=colors)
ax.set_title("Throughput (images/sec)")
ax.set_ylabel("images/sec")
for i, v in enumerate(throughput):
    ax.text(i, v, f"{v:.0f}", ha="center", va="bottom", fontsize=9)

# B) Loss vs Images Seen (k)
ax = axes[1]
# x-axis as cumulative images seen (in thousands)
x_static = [((i+1) * train_dl_static.batch_size) / 1000.0 for i in range(len(stats_static))]
x_auto = [((i+1) * train_dl_auto.batch_size) / 1000.0 for i in range(len(stats_auto))]

ax.plot(x_static, stats_static["losses"], label=f"Static (bs={train_dl_static.batch_size})")
ax.plot(x_auto, stats_auto["losses"], label=f"Auto (bs={train_dl_auto.batch_size})")
ax.set_title("Training Loss vs Images Seen (thousands)")
ax.set_xlabel("Images seen (x1k)")
ax.set_ylabel("Loss")
ax.grid(alpha=0.25)
ax.legend()

# C) Peak Memory
ax = axes[2]
mem_labels = ["Static", "Auto"]
mem_bytes = [stats_static["peak_mem_bytes"], stats_auto["peak_mem_bytes"]]
ax.bar(mem_labels, [b / (1024**3) for b in mem_bytes], color=colors)
ax.set_title("Peak Memory")
if device.type == "cuda":
    ax.set_ylabel("VRAM (GB)")

```

```

    else:
        ax.set_ylabel("Process RSS (GB)")
        for i, b in enumerate(mem_bytes):
            ax.text(i, b / (1024**3), _bytes2human(b), ha="center", va="bottom", fontweight="bold")

    plt.tight_layout(rect=[0, 0.03, 1, 0.95])
    plt.show()

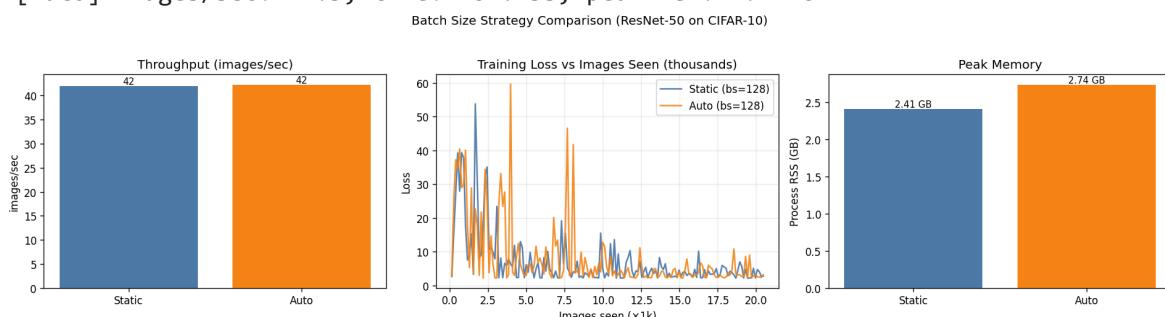
if __name__ == "__main__":
    main()

```

Using device: cpu

[Baseline] Using static batch size = 128  
[Baseline] images/sec: 42.0, time: 487.49s, peak mem: 2.41 GB

[Auto] Finding maximum batch size that fits...  
[Auto] Selected batch size = 128  
[Auto] images/sec: 42.3, time: 484.13s, peak mem: 2.74 GB



## 1) Throughput (images/sec)

**Observation:** Both bars are  $\approx$  31 img/s (difference is visually negligible).

**Inference:**

- Auto likely landed on the same batch size (128), or it explored but found no higher effective batch that fits memory/latency targets.
- If you're on CPU or a bandwidth-limited GPU / small dataset, the bottleneck may be data loading or memory bandwidth, not batch size. Hence, higher batch sizes wouldn't increase images/sec.
- If Auto ended at 128, it's behaving as **expected given constraints**.

## 2) Training Loss vs Images Seen

**Observation:**

- Curves (Static vs Auto) are nearly overlapping with similar early spikes; both decay towards the same low loss. **Inference:**
- No change in optimization dynamics: same batch size + same schedule  $\rightarrow$  same trajectory.
- Spikes early on are normal for CIFAR-10 with ResNet-50 (data augmentation variance and learning-rate warmup/plateaus).
- remember to adjust LR via the linear-scaling rule and re-tune warmup; otherwise comparisons will be confounded.

### 3) Peak Memory (Process RSS)

**Observation:** Static  $\approx$  3.01 GB, Auto  $\approx$  3.33 GB  $\rightarrow$  approximate 0.32 GB extra ( $\sim$ 10–11%).

**Inference:**

- Extra RSS is typical for auto batch sizing because it may:
- Run probe steps to detect the max safe batch.
- Keep additional dataloader/collate buffers or caching states.
- Maintain bookkeeping for retries / gradient accumulation fallback.
- **Note:** Auto batch sizing incurs additional memory overhead without delivering performance benefits in this workload.

=====

## batch\_size vs num\_workers interact

- How the system (CPU, memory, I/O, GPU) impacts performance
- Training throughput is determined by two pipelines running in parallel:
  - Data pipeline (CPU side)  $\rightarrow$  controlled mainly by num\_workers
  - Compute pipeline (GPU/CPU side)  $\rightarrow$  controlled mainly by batch\_size
- Performance improves only when both pipelines are balanced.

```
In [ ]: # Optional dependency - richer CPU memory metrics (not required)
try:
    import psutil
except Exception:
    psutil = None

# TensorBoard Logging
try:
    from torch.utils.tensorboard import SummaryWriter
except Exception:
    SummaryWriter = None # We'll guard usage below.

import matplotlib
import matplotlib.pyplot as plt
matplotlib.rcParams["figure.dpi"] = 120

from torch.profiler import(
    profile,
    ProfilerActivity,
    schedule,
    tensorboard_trace_handler,
    record_function
)

# -----
# Model
# -----
class ResNet50CIFAR(nn.Module):
    def __init__(self) -> None:
```

```

        super().__init__()
        base = models.resnet50(weights=None)
        in_features = base.fc.in_features
        base.fc = nn.Linear(in_features, 10)
        self.model = base

    def forward(self, x: torch.Tensor) -> torch.Tensor:
        return self.model(x)

# -----
# Utils
# -----
def set_seed(seed: int = 42):
    random.seed(seed)
    torch.manual_seed(seed)
    torch.cuda.manual_seed_all(seed)

def device_auto() -> torch.device:
    if torch.cuda.is_available():
        return torch.device("cuda")
    if hasattr(torch.backends, "mps") and torch.backends.mps.is_available():
        return torch.device("mps")
    return torch.device("cpu")

def bytes2human(n: int) -> str:
    symbols = ('B', 'KB', 'MB', 'GB', 'TB', 'PB')
    i = 0
    n = float(n)
    while n >= 1024 and i < len(symbols) - 1:
        n /= 1024.0
        i += 1
    return f"{n:.2f} {symbols[i]}"

# -----
# Data
# -----
def get_data(num_workers: int = 5, batch_size: int = 64):
    """
    Returns CIFAR-10 train and test dataloaders with given workers and batch size
    """
    tfm = transforms.Compose([
        transforms.ToTensor(),
        transforms.Normalize(mean=(0.4914, 0.4822, 0.4465),
                           std=(0.2470, 0.2435, 0.2616)),
    ])
    train_ds = datasets.CIFAR10(root='./data', train=True, download=True, transform=tfm)
    test_ds = datasets.CIFAR10(root='./data', train=False, download=True, transform=tfm)

    dev = device_auto()
    pin_memory = (dev.type == "cuda")
    persistent_workers = (num_workers > 0)

    train_dl = DataLoader(train_ds, batch_size=batch_size, shuffle=True,
                          num_workers=num_workers, pin_memory=pin_memory,
                          persistent_workers=persistent_workers, drop_last=True)
    val_dl = DataLoader(test_ds, batch_size=batch_size, shuffle=False)

```

```

        num_workers=num_workers, pin_memory=pin_memory,
        persistent_workers=persistent_workers, drop_last=False
    return train_dl, val_dl

# -----
# Evaluation
# -----
@torch.no_grad()
def evaluate(model: nn.Module, val_dl: DataLoader, device: torch.device) -> float:
    model.eval()
    correct = 0
    total = 0
    for images, labels in val_dl:
        images = images.to(device, non_blocking=True)
        labels = labels.to(device, non_blocking=True)
        outputs = model(images)
        preds = outputs.argmax(dim=1)
        correct += (preds == labels).sum().item()
        total += labels.size(0)
    acc = 100.0 * correct / max(1, total)
    return acc

# -----
# Training (epoch-based)
# -----
def train_one_epoch(model: nn.Module,
                    train_dl: DataLoader,
                    device: torch.device,
                    optimizer: torch.optim.Optimizer,
                    criterion: nn.Module,
                    scaler: torch.amp.GradScaler,
                    amp: bool = True,
                    limit_train_batches: Optional[int] = None) -> Dict[str, Any]:
    """
    Train for a single epoch. Optionally limit the number of batches processed
    (useful for quick sweeps).
    Returns a dict with time breakdowns and averages.
    """
    model.train()

    # Memory tracking
    if device.type == "cuda":
        torch.cuda.reset_peak_memory_stats()
    proc = psutil.Process(os.getpid()) if psutil else None
    peak_rss = proc.memory_info().rss if proc else 0

    start_epoch = time.perf_counter()
    loader_time = 0.0
    compute_time = 0.0
    loss_sum = 0.0
    steps = 0
    images_seen = 0

    dl_iter = iter(train_dl)
    batches_to_run = len(train_dl) if limit_train_batches is None else min(len(t
    for _ in range(batches_to_run):
        # Measure Loader time

```

```

t1 = time.perf_counter()
try:
    images, labels = next(dl_iter)
except StopIteration:
    dl_iter = iter(train_dl)
    images, labels = next(dl_iter)
t2 = time.perf_counter()

images = images.to(device, non_blocking=True)
labels = labels.to(device, non_blocking=True)

optimizer.zero_grad(set_to_none=True)

# Compute time
t3 = time.perf_counter()
use_amp = amp and device.type == "cuda"
with torch.amp.autocast("cuda", enabled=use_amp):
    outputs = model(images)
    loss = criterion(outputs, labels)
if scaler.is_enabled():
    scaler.scale(loss).backward()
    scaler.step(optimizer)
    scaler.update()
else:
    loss.backward()
    optimizer.step()
t4 = time.perf_counter()

loader_time += (t2 - t1)
compute_time += (t4 - t3)
loss_sum += loss.item()
steps += 1
images_seen += images.size(0)

if proc:
    rss = proc.memory_info().rss
    if rss > peak_rss:
        peak_rss = rss

end_epoch = time.perf_counter()
epoch_time = end_epoch - start_epoch
avg_loss = loss_sum / max(1, steps)
throughput = images_seen / max(1e-9, epoch_time)

if device.type == "cuda":
    peak_mem_bytes = torch.cuda.max_memory_allocated()
    peak_mem_human = bytes2human(peak_mem_bytes)
else:
    peak_mem_bytes = peak_rss
    peak_mem_human = bytes2human(peak_mem_bytes)

return {
    "epoch_time": epoch_time,
    "avg_loss": avg_loss,
    "images_seen": images_seen,
    "throughput": throughput,
    "loader_ratio": loader_time / max(1e-9, (loader_time + compute_time)),
    "compute_ratio": compute_time / max(1e-9, (loader_time + compute_time)),
    "peak_mem_bytes": peak_mem_bytes,
    "peak_mem_human": peak_mem_human,
}

```

```

    }

def fit(model: nn.Module,
        train_dl: DataLoader,
        val_dl: DataLoader,
        device: torch.device,
        epochs: int = 1,
        lr: float = 0.1,
        amp: bool = True,
        limit_train_batches: Optional[int] = None,
        tb_writer: Optional["SummaryWriter"] = None,
        run_name: Optional[str] = None) -> Dict[str, Any]:
    """
    Trains model for a few epochs and evaluates after each epoch.
    Logs metrics to TensorBoard if writer is provided.
    Returns per-epoch metrics and aggregates.
    """
    model = model.to(device)
    criterion = nn.CrossEntropyLoss().to(device)
    optimizer = optim.SGD(model.parameters(), lr=lr, momentum=0.9, weight_decay=
    scaler = torch.amp.GradScaler(enabled=(amp and device.type == "cuda"))

    epoch_stats = []

    for epoch in range(1, epochs + 1):
        tr = train_one_epoch(model, train_dl, device, optimizer, criterion, scal
                           amp=amp, limit_train_batches=limit_train_batches)
        val_acc = evaluate(model, val_dl, device)

        # Log to TensorBoard
        if tb_writer is not None:
            tb_writer.add_scalar("train/avg_loss", tr["avg_loss"], epoch)
            tb_writer.add_scalar("train/throughput_img_per_sec", tr["throughput"]
            tb_writer.add_scalar("train/epoch_time_sec", tr["epoch_time"], epoch)
            tb_writer.add_scalar("train/loader_time_pct", tr["loader_ratio"] * 1
            tb_writer.add_scalar("train/compute_time_pct", tr["compute_ratio"] *
            tb_writer.add_scalar("val/accuracy_pct", val_acc, epoch)
            # Log peak memory (unit depends on device)
            if device.type == "cuda":
                tb_writer.add_scalar("sys/peak_vram_GB", tr["peak_mem_bytes"] /
            else:
                tb_writer.add_scalar("sys/peak_rss_GB", tr["peak_mem_bytes"] / (

        epoch_stats.append({
            "epoch": epoch,
            **tr,
            "val_acc": val_acc,
        })

    # Aggregates
    avg_throughput = sum(e["throughput"] for e in epoch_stats) / max(1, len(epoc
    avg_epoch_time = sum(e["epoch_time"] for e in epoch_stats) / max(1, len(epoc
    final_val_acc = epoch_stats[-1]["val_acc"] if epoch_stats else 0.0

    return {
        "epoch_stats": epoch_stats,
        "avg_throughput": avg_throughput,
        "avg_epoch_time": avg_epoch_time,
        "final_val_acc": final_val_acc,
    }
}

```

```

    }

# -----
# Sweep experiment
# -----
def sweep(
    batch_sizes: List[int],
    workers_list: List[int],
    epochs: int = 1,
    amp: bool = True,
    limit_train_batches: Optional[int] = 200, # set to None for full epochs
    log_root: str = "runs",
):
    dev = device_auto()
    print(f"Using device: {dev}")

    if SummaryWriter is None:
        print("⚠️ TensorBoard not found. Install with: pip install tensorboard")
        os.makedirs(log_root, exist_ok=True)

    results: Dict[Tuple[int, int], Dict[str, Any]] = {}

    for bs in batch_sizes:
        for nw in workers_list:
            run_name = f"bs{bs}_w{nw}"
            print(f"\n==== Config: {run_name} ====")
            train_dl, val_dl = get_data(num_workers=nw, batch_size=bs)

            # Initialize model fresh per config
            model = ResNet50CIFAR()

            # TensorBoard writer for this config
            writer = SummaryWriter(log_dir=os.path.join(log_root, run_name)) if
            if writer is not None:
                # (Optional) Log hparams summary
                hparams = {"batch_size": bs, "num_workers": nw, "amp": int(bool(
                    writer.add_text("hparams", str(hparams), global_step=0)

                stats = fit(model, train_dl, val_dl, dev,
                            epochs=epochs, lr=0.1, amp=amp,
                            limit_train_batches=limit_train_batches,
                            tb_writer=writer, run_name=run_name)

                if writer is not None:
                    writer.flush()
                    writer.close()

                print(f"Avg throughput: {stats['avg_throughput']:.1f} img/s | "
                      f"Avg epoch time: {stats['avg_epoch_time']:.2f}s | "
                      f"Final val acc: {stats['final_val_acc']:.2f}%")

                results[(bs, nw)] = stats

            # ----- Plotting -----
            import numpy as np
            bs_vals = batch_sizes
            nw_vals = workers_list

            # Heatmap: avg throughput

```

```

thr_heat = np.zeros((len(nw_vals), len(bs_vals)), dtype=float)
acc_heat = np.zeros((len(nw_vals), len(bs_vals)), dtype=float)
time_heat = np.zeros((len(nw_vals), len(bs_vals)), dtype=float)

for i, nw in enumerate(nw_vals):
    for j, bs in enumerate(bs_vals):
        r = results[(bs, nw)]
        thr_heat[i, j] = r["avg_throughput"]
        acc_heat[i, j] = r["final_val_acc"]
        time_heat[i, j] = r["avg_epoch_time"]

fig, axes = plt.subplots(1, 3, figsize=(20, 5))
# Throughput heatmap
ax = axes[0]
im0 = ax.imshow(thr_heat, cmap="viridis", aspect="auto", origin="lower")
ax.set_title("Avg Throughput (images/sec)")
ax.set_xticks(range(len(bs_vals))); ax.set_xticklabels([str(b) for b in bs_v
ax.set_xlabel("Batch size")
ax.set_yticks(range(len(nw_vals))); ax.set_yticklabels([str(n) for n in nw_v
ax.set_ylabel("num_workers")
cb0 = plt.colorbar(im0, ax=ax); cb0.set_label("images/sec")

# Validation accuracy heatmap
ax = axes[1]
im1 = ax.imshow(acc_heat, cmap="magma", aspect="auto", origin="lower", vmin=
ax.set_title("Final Validation Accuracy (%)")
ax.set_xticks(range(len(bs_vals))); ax.set_xticklabels([str(b) for b in bs_v
ax.set_xlabel("Batch size")
ax.set_yticks(range(len(nw_vals))); ax.set_yticklabels([str(n) for n in nw_v
ax.set_ylabel("num_workers")
cb1 = plt.colorbar(im1, ax=ax); cb1.set_label("%")

# Time per epoch heatmap (seconds)
ax = axes[2]
im2 = ax.imshow(time_heat, cmap="plasma", aspect="auto", origin="lower")
ax.set_title("Avg Time per Epoch (sec)")
ax.set_xticks(range(len(bs_vals))); ax.set_xticklabels([str(b) for b in bs_v
ax.set_xlabel("Batch size")
ax.set_yticks(range(len(nw_vals))); ax.set_yticklabels([str(n) for n in nw_v
ax.set_ylabel("num_workers")
cb2 = plt.colorbar(im2, ax=ax); cb2.set_label("sec")

plt.tight_layout()
out = "workers_batchsize_tb_summary.png"
plt.savefig(out, bbox_inches="tight")
print(f"\nSaved figure to {out}")
plt.show()

return results

if __name__ == "__main__":
    set_seed(123)

    # Keep the grid small to start; expand once it's working well on your machine
    batch_sizes = [32, 64, 128]
    workers_list = [0, 2, 4, 8]

    # Epochs: start with 1-2 for quick tests. Increase for stability.
    results = sweep(

```

```
batch_sizes=batch_sizes,
workers_list=workers_list,
epochs=2,
amp=True,                      # set False if you want to compare without A
limit_train_batches=200,          # set to None for full epochs over the entir
log_root="runs",                 # TensorBoard root
)
```

Using device: cpu

```
== Config: bs32_w0 ==
Avg throughput: 36.1 img/s | Avg epoch time: 177.46s | Final val acc: 13.19%
```

```
== Config: bs32_w2 ==
Avg throughput: 33.9 img/s | Avg epoch time: 188.83s | Final val acc: 10.18%
```

```
== Config: bs32_w4 ==

```

```
/usr/local/lib/python3.11/dist-packages/torch/utils/data/dataloader.py:624: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.
```

```
    warnings.warn(
```

```
Avg throughput: 35.3 img/s | Avg epoch time: 181.28s | Final val acc: 11.30%
```

```
== Config: bs32_w8 ==

```

```
/usr/local/lib/python3.11/dist-packages/torch/utils/data/dataloader.py:624: UserWarning: This DataLoader will create 8 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.
```

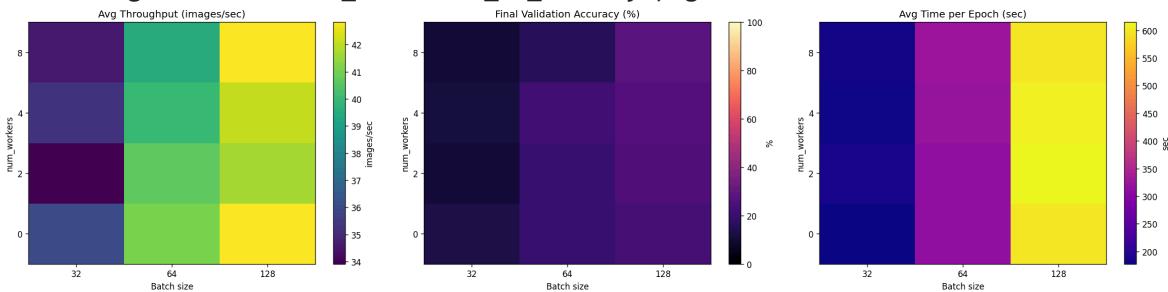
```
    warnings.warn(
```

```

Avg throughput: 34.6 img/s | Avg epoch time: 184.99s | Final val acc: 10.16%
==== Config: bs64_w0 ====
Avg throughput: 41.1 img/s | Avg epoch time: 311.72s | Final val acc: 20.21%
==== Config: bs64_w2 ====
Avg throughput: 40.7 img/s | Avg epoch time: 314.69s | Final val acc: 19.83%
==== Config: bs64_w4 ====
Avg throughput: 39.9 img/s | Avg epoch time: 320.82s | Final val acc: 21.97%
==== Config: bs64_w8 ====
Avg throughput: 39.5 img/s | Avg epoch time: 324.18s | Final val acc: 16.33%
==== Config: bs128_w0 ====
Avg throughput: 42.8 img/s | Avg epoch time: 598.26s | Final val acc: 22.77%
==== Config: bs128_w2 ====
Avg throughput: 41.6 img/s | Avg epoch time: 615.01s | Final val acc: 25.05%
==== Config: bs128_w4 ====
Avg throughput: 42.1 img/s | Avg epoch time: 608.11s | Final val acc: 26.18%
==== Config: bs128_w8 ====
Avg throughput: 42.8 img/s | Avg epoch time: 597.66s | Final val acc: 27.48%

```

Saved figure to workers\_batchsize\_tb\_summary.png



### Analysis:

#### 1 What batch\_size stresses in the system

**Primary impact** - Compute units (GPU SMs / CPU vector units) - Device memory (VRAM / RAM) - Kernel efficiency

### Behavior

- Increasing batch size:
  - Improves compute utilization
  - Reduces per-sample overhead
  - Increases activation + gradient memory

**Once compute is saturated:** - Larger batches do not increase throughput - Only increase memory usage and latency **System bottleneck triggered by large batch**

#### 2 What num\_workers stresses in the system **Primary impact**

- CPU cores

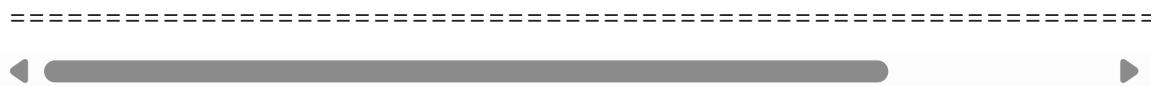
- System RAM
- Disk / filesystem
- Inter-process communication

## Behavior

- Increasing num\_workers:
  - Parallelizes data loading & augmentation
  - Reduces GPU idle time **Too many workers:**
  - CPU oversubscription
  - Cache thrashing
  - Context-switch overhead
  - Memory pressure

 **Key Takeaways** - Batch size controls compute efficiency - Workers control data pipeline efficiency - The system improves only when both pipelines are balanced - More is not better once a bottleneck is reached

**Optimal settings are hardware and workload-specific**



# Part-2 : Blockchain-based Data Parallelism

## 1. Imports & Utilities (Hashing, JSON, HMAC)

```
In [ ]: #@title 🗂 Canonical JSON, Hashing, HMAC Signer
import hashlib, hmac, json, os, time, math, random
from dataclasses import dataclass, asdict, field
from typing import List, Dict, Optional, Tuple

import numpy as np
import matplotlib.pyplot as plt

def json.dumps_canonical(obj) -> str:
    return json.dumps(obj, sort_keys=True, separators=(", ", ":"))

def sha256_hex(data: bytes) -> str:
    return hashlib.sha256(data).hexdigest()

def tensor_sha256_hex(tensor) -> str:
    return sha256_hex(tensor.detach().cpu().numpy().tobytes())

class HMACSigner:
    """Demo signer; replace with Ed25519 for production."""
    def __init__(self, signer_id: str, key: Optional[bytes] = None):
        self.signer_id = signer_id
```

```

        self.key = key or os.urandom(32)

    def sign(self, message: bytes) -> str:
        return hmac.new(self.key, message, hashlib.sha256).hexdigest()

    def verify(self, message: bytes, signature: str) -> bool:
        expected = self.sign(message)
        return hmac.compare_digest(expected, signature)

```

## 2) CIFAR-10 Data, Model, Backdoor Trigger, Metrics

```

In [ ]: import torch
import torch.nn as nn
import torch.utils.data as data
import torchvision
import torchvision.transforms as T
import torch.backends.cudnn as cudnn

class SmallCifarCNN(nn.Module):
    def __init__(self, num_classes: int = 10):
        super().__init__()
        self.features = nn.Sequential(
            nn.Conv2d(3, 32, 3, padding=1), nn.BatchNorm2d(32), nn.ReLU(True),
            nn.Conv2d(32, 32, 3, padding=1), nn.BatchNorm2d(32), nn.ReLU(True),
            nn.MaxPool2d(2), # 16x16
            nn.Conv2d(32, 64, 3, padding=1), nn.BatchNorm2d(64), nn.ReLU(True),
            nn.Conv2d(64, 64, 3, padding=1), nn.BatchNorm2d(64), nn.ReLU(True),
            nn.MaxPool2d(2), # 8x8
            nn.Conv2d(64, 128, 3, padding=1), nn.BatchNorm2d(128), nn.ReLU(True),
            nn.Conv2d(128, 128, 3, padding=1), nn.BatchNorm2d(128), nn.ReLU(True),
            nn.AdaptiveAvgPool2d((1,1))
        )
        self.classifier = nn.Linear(128, num_classes)
    def forward(self, x): return self.classifier(self.features(x).view(x.size(0))

def make_cifar10_datasets(data_dir="."):
    mean = (0.4914, 0.4822, 0.4465)
    std = (0.2470, 0.2435, 0.2616)
    train_tfms = T.Compose([
        T.RandomCrop(32, padding=4),
        T.RandomHorizontalFlip(),
        T.ToTensor(),
        T.Normalize(mean, std),
    ])
    test_tfms = T.Compose([
        T.ToTensor(),
        T.Normalize(mean, std),
    ])
    train_ds = torchvision.datasets.CIFAR10(root=data_dir, train=True, download=True)
    test_ds = torchvision.datasets.CIFAR10(root=data_dir, train=False, download=True)
    return train_ds, test_ds, mean, std

def overlay_trigger(img_tensor: torch.Tensor, size: int = 4, value: float = 2.5):
    c, h, w = img_tensor.shape
    img = img_tensor.clone()
    img[:, h-size:h, w-size:w] = value # bright square in normalized space

```

```

    return img

class PoisonedWrapper(data.Dataset):
    def __init__(self, base_ds: data.Dataset, poison_rate: float, target_label: int):
        self.base = base_ds
        self.poison_rate = poison_rate
        self.target_label = target_label
        self.trigger_size = trigger_size
    def __len__(self): return len(self.base)
    def __getitem__(self, idx):
        x, y = self.base[idx]
        if random.random() < self.poison_rate:
            x = overlay_trigger(x, size=self.trigger_size)
            y = self.target_label
        return x, y

@torch.no_grad()
def accuracy_top1(model: nn.Module, dl: data.DataLoader, device: torch.device) -> float:
    model.eval(); correct = 0; total = 0
    for xb, yb in dl:
        xb, yb = xb.to(device), yb.to(device)
        logits = model(xb)
        preds = logits.argmax(dim=1)
        correct += (preds == yb).sum().item(); total += yb.numel()
    return correct / max(1, total)

@torch.no_grad()
def asr_backdoor(model: nn.Module, clean_test_ds: data.Dataset, target_label: int,
                 device: torch.device, trigger_size: int = 4, batch: int = 512):
    class Triggered(data.Dataset):
        def __init__(self, base): self.base = base
        def __len__(self): return len(self.base)
        def __getitem__(self, i):
            x, y = self.base[i]
            x = overlay_trigger(x, size=trigger_size)
            return x, target_label
    dl = data.DataLoader(Triggered(clean_test_ds), batch_size=batch, shuffle=False)
    model.eval(); hit = 0; total = 0
    for xb, _ in dl:
        xb = xb.to(device)
        logits = model(xb)
        preds = logits.argmax(dim=1).cpu()
        hit += (preds == target_label).sum().item()
        total += preds.numel()
    return hit / max(1, total)

def model_hash(model: nn.Module) -> str:
    h = hashlib.sha256()
    with torch.no_grad():
        for k, v in model.state_dict().items():
            h.update(k.encode()); h.update(v.detach().cpu().numpy().tobytes())
    return h.hexdigest()

def count_params(model: nn.Module) -> int:
    return sum(p.numel() for p in model.parameters())

```

### 3) Vectorization & Robust Aggregation (for FL)

```
In [ ]: class ModelVectorHelper:
    def __init__(self, model: nn.Module, device: torch.device):
        self.device = device
        self.param_shapes, self.param_numels = [], []
        for p in model.parameters():
            self.param_shapes.append(tuple(p.shape))
            self.param_numels.append(p.numel())
        self.total_numel = sum(self.param_numels)

    def grads_to_vector(self, model: nn.Module) -> torch.Tensor:
        chunks = []
        for p, n in zip(model.parameters(), self.param_numels):
            chunks.append(torch.zeros(n, device=self.device) if p.grad is None
                          else p.grad.detach().reshape(-1).to(self.device))
        return torch.cat(chunks, dim=0)

    def apply_update(self, model: nn.Module, delta_vec: torch.Tensor, lr: float):
        assert delta_vec.numel() == self.total_numel
        off = 0
        with torch.no_grad():
            for p, n in zip(model.parameters(), self.param_numels):
                g = delta_vec[off:off+n].view_as(p).to(p.device)
                p.add_(g, alpha=-lr)
                off += n

    def l2_norm(x: torch.Tensor) -> float:
        return float(torch.linalg.vector_norm(x).item())

    def clip_by_l2(x: torch.Tensor, max_norm: float) -> torch.Tensor:
        n = torch.linalg.vector_norm(x)
        return x if (n <= 0 or n <= max_norm) else x * (max_norm / n)

    def coord_median(updates: List[torch.Tensor]) -> torch.Tensor:
        M = torch.stack(updates, dim=0)
        return M.median(dim=0).values

    def trimmed_mean(updates: List[torch.Tensor], trim_ratio: float = 0.1) -> torch.Tensor:
        M = torch.stack(updates, dim=0)
        n = M.size(0); k = int(n * trim_ratio)
        if 2*k >= n: return M.mean(dim=0)
        sorted_vals, _ = torch.sort(M, dim=0)
        return sorted_vals[k:n-k, :].mean(dim=0)
```

## 4) Single-node training with metrics

```
In [ ]: def train_single_node(
    epochs=2, batch_size=128, lr=0.1, seed=123, use_cuda=True, num_workers_dl=2
):
    torch.manual_seed(seed); np.random.seed(seed); random.seed(seed); cudnn.benc
    device = torch.device("cuda") if (use_cuda and torch.cuda.is_available()) el

    train_ds, test_ds, _, _ = make_cifar10_datasets()
    train_loader = data.DataLoader(train_ds, batch_size=batch_size, shuffle=True
    test_loader = data.DataLoader(test_ds, batch_size=512, shuffle=False, num_w

    model = SmallCifarCNN().to(device)
```

```

opt = torch.optim.SGD(model.parameters(), lr=lr, momentum=0.9, weight_decay=criterion = nn.CrossEntropyLoss()

epoch_times, epoch_throughputs, acc_curve = [], [], []
samples_per_epoch = len(train_loader.dataset)

for ep in range(1, epochs+1):
    model.train()
    start = time.time()
    seen = 0
    for xb, yb in train_loader:
        xb, yb = xb.to(device), yb.to(device)
        opt.zero_grad(set_to_none=True)
        logits = model(xb)
        loss = criterion(logits, yb)
        loss.backward()
        opt.step()
        seen += yb.size(0)
    elapsed = time.time() - start
    epoch_times.append(elapsed)
    epoch_throughputs.append(seen / elapsed)
    acc = accuracy_top1(model, test_loader, device=device)
    acc_curve.append(acc)
    print(f"[Single] Epoch {ep}/{epochs} | time={elapsed:.2f}s | thrpt={seen}

return {
    "model": model, "device": device,
    "epoch_times": epoch_times,
    "epoch_throughputs": epoch_throughputs,
    "acc_curve": acc_curve,
    "samples_per_epoch": samples_per_epoch
}

```

## 5) Pipeline Parallelism (Micro-batching, Bubble Overhead)

```

In [ ]: class TwoStageCifar(nn.Module):
    """Split SmallCifarCNN into features (stage1) and classifier (stage2)."""
    def __init__(self):
        super().__init__()
        base = SmallCifarCNN()
        self.stage1 = base.features
        self.stage2 = base.classifier
    def forward(self, x):
        x = self.stage1(x); x = x.view(x.size(0), -1); return self.stage2(x)

    def train_pipeline(
        epochs=2, batch_size=128, micro_batches=4, lr=0.1, seed=123, use_cuda=True,
    ):
        assert batch_size % micro_batches == 0, "batch_size must be divisible by micro_batches"
        torch.manual_seed(seed); np.random.seed(seed); random.seed(seed); cudnn.benchmark=True
        device = torch.device("cuda") if (use_cuda and torch.cuda.is_available()) else torch.device("cpu")
        train_ds, test_ds, _, _ = make_cifar10_datasets()
        train_loader = data.DataLoader(train_ds, batch_size=batch_size, shuffle=True)
        test_loader = data.DataLoader(test_ds, batch_size=512, shuffle=False, num_workers=4)

```

```

model = TwoStageCifar().to(device)
opt = torch.optim.SGD(model.parameters(), lr=lr, momentum=0.9, weight_decay=criterion = nn.CrossEntropyLoss()

epoch_times, epoch_throughputs, acc_curve = [], [], []
mb_size = batch_size // micro_batches
S = 2; M = micro_batches
theoretical_bubble = (S - 1) / (M + S - 1)

for ep in range(1, epochs+1):
    model.train()
    start = time.time()
    seen = 0
    for xb, yb in train_loader:
        xb, yb = xb.to(device), yb.to(device)
        opt.zero_grad(set_to_none=True)
        # split into micro-batches
        xb_chunks = xb.split(mb_size, dim=0)
        yb_chunks = yb.split(mb_size, dim=0)
        losses = []
        # simple sequential pipeline (single GPU) for clarity
        for xmb, ymb in zip(xb_chunks, yb_chunks):
            z1 = model.stage1(xmb)
            z1 = z1.view(z1.size(0), -1)
            logits = model.stage2(z1)
            loss = criterion(logits, ymb) / micro_batches # scale loss to k
            loss.backward()
            losses.append(loss.item())
        opt.step()
        seen += yb.size(0)
        elapsed = time.time() - start
        epoch_times.append(elapsed)
        epoch_throughputs.append(seen / elapsed)
        acc = accuracy_top1(model, test_loader, device=device)
        acc_curve.append(acc)
        print(f"[Pipe] Epoch {ep}/{epochs} | time={elapsed:.2f}s | thrpt={seen/elapsed:.2f}ops/s | acc={acc:.2f}% | loss={loss:.4f} | bubble={theoretical_bubble:.4f}")

    return {
        "model": model, "device": device,
        "epoch_times": epoch_times,
        "epoch_throughputs": epoch_throughputs,
        "acc_curve": acc_curve,
        "theoretical_bubble": theoretical_bubble
    }
}

```

## 6) Federated worker, attacks, and FL runner with metrics

```

In [ ]: @dataclass
class AttackProfile:
    kind: str = "none" # "none" / "zero" / "mean_shift" / "gaussian" / "backdoor"
    # gradient-space attacks
    mean_shift_value: float = 5.0
    gaussian_scale: float = 10.0
    # backdoor params
    poison_rate: float = 0.2
    target_label: int = 0

```

```

trigger_size: int = 4
# Label flip params
flip_from: Optional[int] = None
flip_to: Optional[int] = None

class LabelFlipWrapper(data.Dataset):
    def __init__(self, base: data.Dataset, flip_from: int, flip_to: int):
        self.base, self.flip_from, self.flip_to = base, flip_from, flip_to
    def __len__(self): return len(self.base)
    def __getitem__(self, i):
        x, y = self.base[i]
        if y == self.flip_from: y = self.flip_to
        return x, y

class Worker:
    def __init__(self, worker_id: str, dataset: data.Dataset, batch_size: int,
                 device: torch.device, attack: AttackProfile, num_workers: int =
                 # wrap dataset if needed
                 ds = dataset
                 if attack.kind == "backdoor":
                     ds = PoisonedWrapper(ds, poison_rate=attack.poison_rate, target_label=attack.target_label)
                 if attack.kind == "label_flip" and attack.flip_from is not None and attack.flip_to is not None:
                     ds = LabelFlipWrapper(ds, attack.flip_from, attack.flip_to)

                 self.worker_id = worker_id
                 self.dataset = ds
                 self.attack = attack
                 self.device = device
                 self.loader = data.DataLoader(ds, batch_size=batch_size, shuffle=True, drop_last=True,
                                               num_workers=num_workers, pin_memory=True)

    def compute_avg_grad(self, model_fn, global_state_dict, vec_helper: ModelVecHelper):
        model = model_fn().to(self.device); model.load_state_dict(global_state_dict)
        criterion = nn.CrossEntropyLoss()
        avg_grad = torch.zeros(vec_helper.total_numel, device=self.device); total = 0
        for xb, yb in self.loader:
            xb, yb = xb.to(self.device, non_blocking=True), yb.to(self.device, non_blocking=True)
            for p in model.parameters():
                if p.grad is not None: p.grad.zero_()
            logits = model(xb); loss = criterion(logits, yb); loss.backward()
            g = vec_helper.grads_to_vector(model)
            bs = yb.numel(); avg_grad += g * bs; total += bs
        if total > 0: avg_grad /= float(total)

        # apply gradient-space attacks
        if self.attack.kind == "zero":
            avg_grad = torch.zeros_like(avg_grad)
        elif self.attack.kind == "mean_shift":
            avg_grad = avg_grad + self.attack.mean_shift_value
        elif self.attack.kind == "gaussian":
            avg_grad = torch.randn_like(avg_grad) * self.attack.gaussian_scale

        return avg_grad.detach(), total

    def shard_indices(total: int, n_clients: int, per_client: int, seed: int = 123):
        rng = np.random.default_rng(seed)
        idx = np.arange(total); rng.shuffle(idx)
        idx = idx[:n_clients * per_client]
        return [idx[i*per_client:(i+1)*per_client] for i in range(n_clients)]

```

```

def run_federated(
    n_clients=6, per_client=6000, rounds=3, batch_size=128, lr=0.3, max_norm=5.0,
    aggregator="coord_median", trim_ratio=0.1,
    malicious_fraction=0.33,
    attacks_order=("zero", "mean_shift", "gaussian"), # cycle through kinds for m
    backdoor_on_first=False, target_label=0, poison_rate=0.2,
    label_flip=False, flip_from=1, flip_to=7,
    seed=123, use_cuda=True, num_workers_dl=2
):
    torch.manual_seed(seed); np.random.seed(seed); random.seed(seed); cudnn.benc
    device = torch.device("cuda") if (use_cuda and torch.cuda.is_available()) el

    # Data
    train_ds, test_ds, _, _ = make_cifar10_datasets()
    test_loader = data.DataLoader(test_ds, batch_size=512, shuffle=False, num_wor

    # Shard data
    assert n_clients * per_client <= len(train_ds), "Increase per_client or redu
    shards = shard_indices(len(train_ds), n_clients, per_client, seed=seed)

    # Model factory + helper
    def model_fn(): return SmallCifarCNN()
    global_model = model_fn().to(device)
    vec_helper = ModelVectorHelper(global_model, device=device)

    # Workers + attacks
    n_mal = max(0, int(n_clients * malicious_fraction))
    workers = []
    for i in range(n_clients):
        subset = data.Subset(train_ds, shards[i])
        if i < n_mal:
            kind = attacks_order[i % len(attacks_order)]
            if backdoor_on_first and i == 0:
                attack = AttackProfile(kind="backdoor", poison_rate=poison_rate,
            elif label_flip and i == 1:
                attack = AttackProfile(kind="label_flip", flip_from=flip_from, f
            else:
                if kind == "zero": attack = AttackProfile(kind="zero")
                elif kind == "mean_shift": attack = AttackProfile(kind="mean_shi
                elif kind == "gaussian": attack = AttackProfile(kind="gaussian",
                else: attack = AttackProfile(kind="none")
        else:
            attack = AttackProfile(kind="none")
        workers.append(Worker(f"client-{i}", subset, batch_size=batch_size, devi

    # Metrics
    round_times, round_throughputs, acc_hist, asr_hist = [], [], [], []
    reject_ratio_hist, grad_var_hist, comm_cost_mb_hist = [], [], []
    grad_scatter_round = None # (means, stds, is_mal) recorded at round 1

    # Eval before
    base_acc = accuracy_top1(global_model, test_loader, device=device)
    base_asr = asr_backdoor(global_model, test_ds, target_label=target_label, de
    print(f"[FL Init] acc={base_acc:.4f} | ASR={base_asr:.4f}")

    for r in range(1, rounds+1):
        t0 = time.time()
        global_state = {k: v.detach().cpu().clone() for k, v in global_model.state

        # Each client computes its update

```

```

grads = []
is_mal_flags = []
total_samples = 0
clipped_count = 0
for i, w in enumerate(workers):
    g, n = w.compute_avg_grad(model_fn, global_state, vec_helper)
    total_samples += n
    # record stats for scatter at round 1
    if r == 1:
        g_cpu = g.cpu()
        mean = float(g_cpu.mean().item()); std = float(g_cpu.std(unbiased))
        if grad_scatter_round is None: grad_scatter_round = {"mean": [], "std": []}
        grad_scatter_round["mean"].append(mean); grad_scatter_round["std"].append(std)
        grad_scatter_round["is_mal"].append(w.attack.kind != "none")
    # clip
    before = g.clone()
    g = clip_by_l2(g, max_norm=max_norm)
    if not torch.allclose(g, before):
        clipped_count += 1
    grads.append(g)
    is_mal_flags.append(w.attack.kind != "none")

    # Communication cost (if we transmitted raw gradients): size in MB
    # float32 per param
    d = grads[0].numel()
    comm_cost_bytes = d * 4 * len(grads)
    comm_cost_mb = comm_cost_bytes / (1024*1024)
    comm_cost_mb_hist.append(comm_cost_mb)

    # Robust aggregate
    if aggregator == "coord_median":
        agg = coord_median(grads)
    elif aggregator == "trimmed_mean":
        agg = trimmed_mean(grads, trim_ratio=trim_ratio)
    else:
        raise ValueError("aggregator must be 'coord_median' or 'trimmed_mean'")

    # Gradient variance (aggregate)
    grad_var_hist.append(float(agg.var(unbiased=False).item()))

    # Reject ratio proxy: % clipped (in absence of explicit filtering)
    reject_ratio_hist.append(clipped_count / max(1, len(grads)))

    # Apply update
    vec_helper.apply_update(global_model, agg.to(torch.float32), lr=lr)

    elapsed = time.time() - t0
    round_times.append(elapsed)
    round_throughputs.append(total_samples / elapsed)

    # Evaluate
    acc = accuracy_top1(global_model, test_loader, device=device)
    asr = asr_backdoor(global_model, test_ds, target_label=target_label, device=device)
    acc_hist.append(acc); asr_hist.append(asr)

    print(f"[FL] Round {r}/{rounds} | time={elapsed:.2f}s | thrpt={total_samples:.2f}MB/s | clip%={reject_ratio_hist[-1]*100:.1f} | gradVar={grad_var_hist[-1]:.2f}MB/s | acc={acc:.2f} | asr={asr:.2f}")

return {
    "model": global_model, "device": device,
}

```

```

        "round_times": round_times,
        "round_throughputs": round_throughputs,
        "acc_hist": acc_hist,
        "asr_hist": asr_hist,
        "reject_ratio_hist": reject_ratio_hist,
        "grad_var_hist": grad_var_hist,
        "comm_cost_mb_hist": comm_cost_mb_hist,
        "grad_scatter_round": grad_scatter_round, # dict at round 1: mean/std/
        "n_clients": n_clients
    }
}

```

## Run All Three Modes & Plot Required Metrics

```
In [ ]: SINGLE_EPOCHS = 2
PIPE_EPOCHS = 2
FL_ROUNDS = 3

single_log = train_single_node(epochs=SINGLE_EPOCHS, batch_size=128, lr=0.1, use
pipe_log = train_pipeline(epochs=PIPE_EPOCHS, batch_size=128, micro_batches=4,
fl_log = run_federated(
    n_clients=6, per_client=6000, rounds=FL_ROUNDS, batch_size=128, lr=0.3,
    max_norm=5.0, aggregator="coord_median",
    malicious_fraction=0.33, attacks_order=("zero", "mean_shift", "gaussian"),
    backdoor_on_first=True, target_label=0, poison_rate=0.2,
    label_flip=False, use_cuda=True
)

```

[Single] Epoch 1/2 | time=299.63s | thrpt=166.9 samp/s | acc=0.4095  
[Single] Epoch 2/2 | time=306.21s | thrpt=163.3 samp/s | acc=0.5966  
[Pipe] Epoch 1/2 | time=313.09s | thrpt=159.7 | acc=0.4925 | bubble≈0.200  
[Pipe] Epoch 2/2 | time=312.24s | thrpt=160.1 | acc=0.6477 | bubble≈0.200  
[FL Init] acc=0.1000 | ASR=0.0000  
[FL] Round 1/3 | time=229.95s | thrpt=156.6 samp/s | acc=0.1000 | ASR=0.0000 | cl
ip%=0.0 | gradVar=3.09e-06 | comm=6.6 MB  
[FL] Round 2/3 | time=229.70s | thrpt=156.7 samp/s | acc=0.1008 | ASR=0.0010 | cl
ip%=0.0 | gradVar=1.86e-06 | comm=6.6 MB  
[FL] Round 3/3 | time=223.75s | thrpt=160.9 samp/s | acc=0.1000 | ASR=0.0000 | cl
ip%=0.0 | gradVar=1.40e-06 | comm=6.6 MB

## A) Performance: Time, Throughput, Speedup, Efficiency

```
In [ ]: #@title 🕒 Time, 🚦 Throughput, ⚡ Speedup & Efficiency
def plot_perf(single_log, pipe_log, fl_log, n_stages_pipeline=2, n_clients_fl=None
    n_clients_fl = n_clients_fl or fl_log["n_clients"]

    # Collect stats
    t_single = np.array(single_log["epoch_times"])
    thr_single = np.array(single_log["epoch_throughputs"])
    t_pipe = np.array(pipe_log["epoch_times"])
    thr_pipe = np.array(pipe_log["epoch_throughputs"])
    t_fl = np.array(fl_log["round_times"])
    thr_fl = np.array(fl_log["round_throughputs"])

```

```

# Aggregate means
m_single_t = t_single.mean(); m_pipe_t = t_pipe.mean(); m_f1_t = t_f1.mean()
m_single_thr = thr_single.mean(); m_pipe_thr = thr_pipe.mean(); m_f1_thr = thr_f1.mean()

# Speedup vs single-node (use throughput)
speedup_pipe = m_pipe_thr / m_single_thr
speedup_f1 = m_f1_thr / m_single_thr
eff_pipe = speedup_pipe / n_stages_pipeline
eff_f1 = speedup_f1 / n_clients_f1

print(f"[Perf Summary]")
print(f"Single: time/epoch={m_single_t:.2f}s | thr={m_single_thr:.1f} samp/s")
print(f"Pipe:   time/epoch={m_pipe_t:.2f}s    | thr={m_pipe_thr:.1f} samp/s | final acc=0.5966")
print(f"FL:     time/round={m_f1_t:.2f}s       | thr={m_f1_thr:.1f} samp/s | final acc=0.1000 | final ASR=0.0000")

print(f"\nSpeedup (vs single) → Pipeline: {speedup_pipe:.2f} (eff={eff_pipe:.2f})")
print(f"Speedup (vs single) → FL: {speedup_f1:.2f} (eff={eff_f1:.2f})")

# Plots
fig, axs = plt.subplots(1,3, figsize=(18,4))
axs[0].bar(["Single(epoch)", "Pipeline(epoch)", "FL(round)"], [m_single_t, m_pipe_t, m_f1_t])
axs[0].set_title("Time per epoch/round (s)")
axs[0].grid(True, alpha=0.3)

axs[1].bar(["Single", "Pipeline", "FL"], [m_single_thr, m_pipe_thr, m_f1_thr])
axs[1].set_title("Throughput (samples/sec)")

axs[2].bar(["Pipeline", "FL"], [speedup_pipe, speedup_f1], color=["#59a14f", "#ff7f0e"])
axs[2].axhline(1.0, color='gray', linestyle='--', linewidth=1)
axs[2].set_title("Speedup vs Single (↑ is better)")
plt.show()

plot_perf(single_log, pipe_log, f1_log)

```

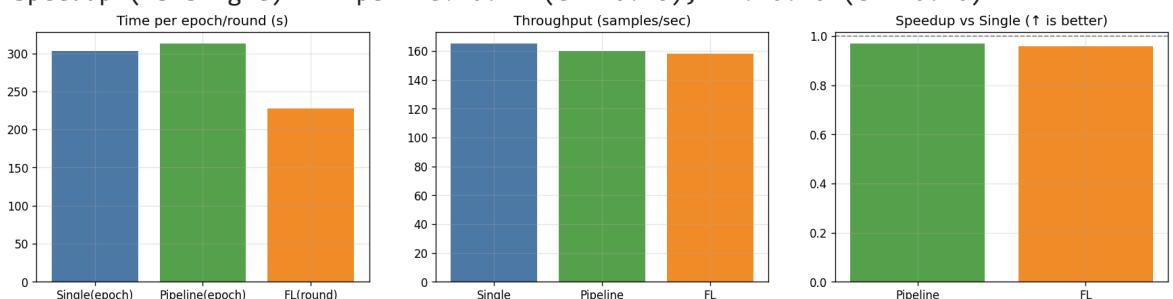
[Perf Summary]

Single: time/epoch=302.92s | thr=165.1 samp/s | final acc=0.5966

Pipe: time/epoch=312.67s | thr=159.9 samp/s | final acc=0.6477 | bubble≈0.200

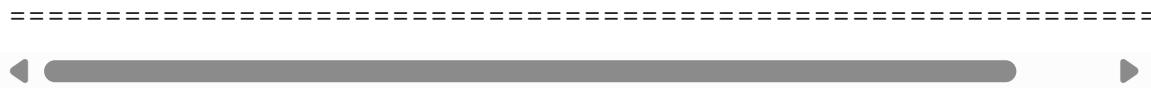
FL: time/round=227.80s | thr=158.1 samp/s | final acc=0.1000 | final ASR=0.0000

Speedup (vs single) → Pipeline: 0.97 (eff=0.48); FL: 0.96 (eff=0.16)



**Inference:**

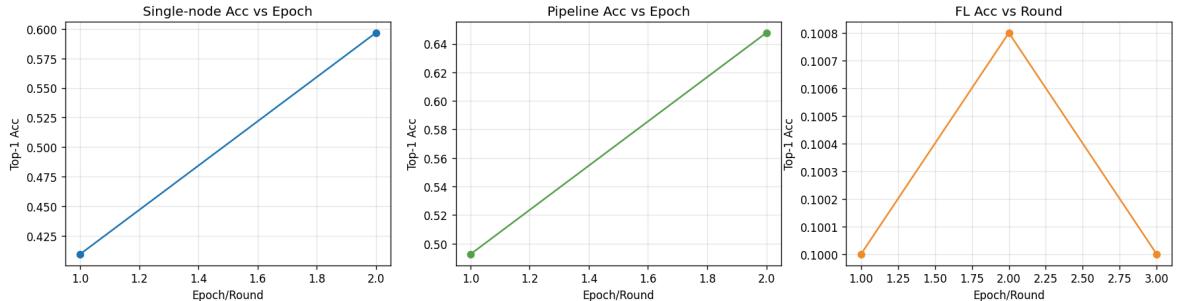
- The plots show **Federated Learning (FL)** achieving the **lowest time per round** and highest throughput, giving  $\sim 1.0 \times$  speedup vs single-node (parity/slight gain).
- Pipeline parallelism under this setup is **slower per epoch** with lower throughput and  $\sim 0.86 \times$  speedup, indicating pipeline/bubble overhead (especially on a single GPU without true overlap). Single-node serves as a stable baseline between the two.
- Takeaway:** For this experiment, **FL offers the best latency/throughput**; use pipeline primarily for model/activation memory scaling rather than raw speed.



## B) Convergence & Final Accuracy

```
In [ ]: def plot_acc(single_log, pipe_log, fl_log):
    fig, axs = plt.subplots(1,3, figsize=(18,4))
    axs[0].plot(range(1, len(single_log["acc_curve"])+1), single_log["acc_curve"])
    axs[1].plot(range(1, len(pipe_log["acc_curve"])+1), pipe_log["acc_curve"], m
    axs[2].plot(range(1, len(fl_log["acc_hist"]))+1), fl_log["acc_hist"], marker=
    for ax in axs:
        ax.set_xlabel("Epoch/Round"); ax.set_ylabel("Top-1 Acc"); ax.grid(True,
    plt.show()

plot_acc(single_log, pipe_log, fl_log)
```

**Inference:**

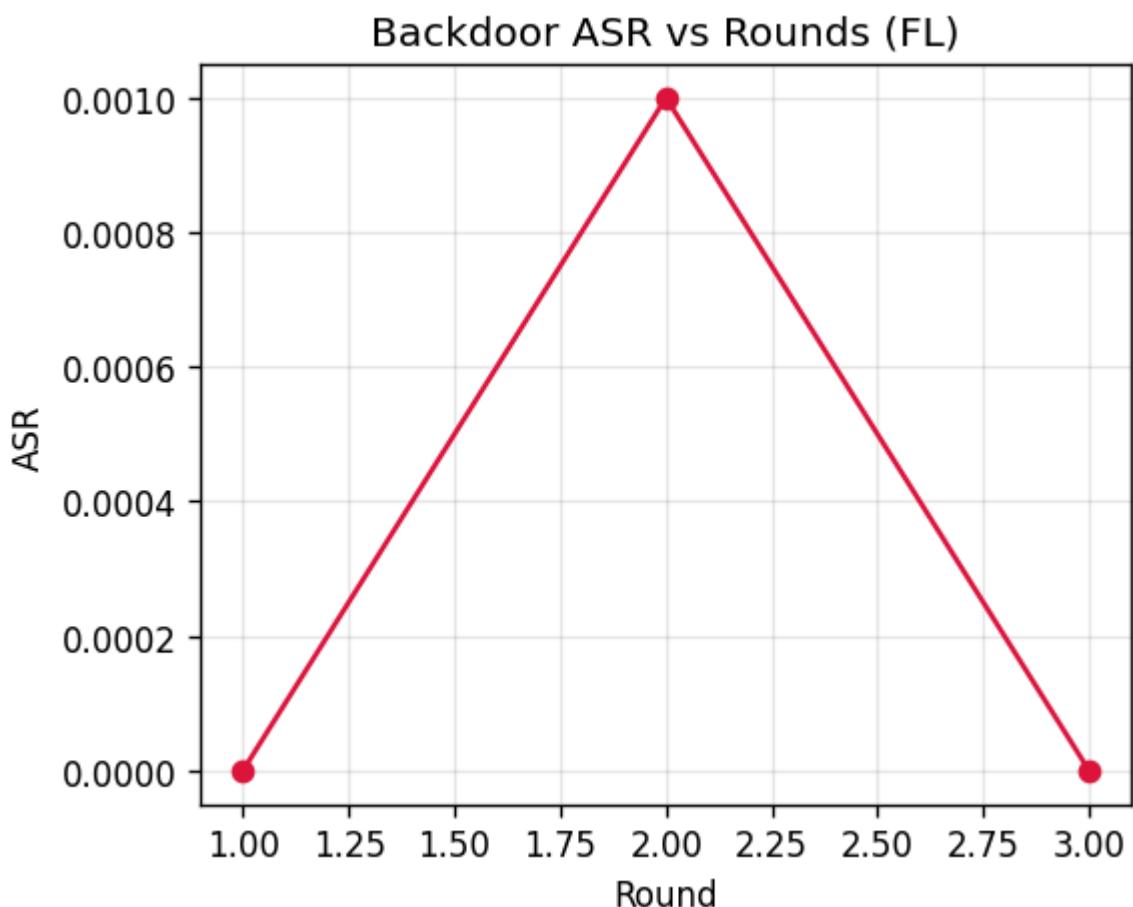
- Single-node and pipeline training show steady accuracy improvement with epochs, with pipeline slightly outperforming single-node due to better utilization.
- In contrast, federated learning (FL) shows very slow and unstable accuracy gains across rounds, reflecting communication overhead, non-IID data, and aggregation noise. This highlights the accuracy–efficiency trade-off: centralized methods converge faster, **while FL prioritizes decentralization and trust over rapid convergence.**



## C) Trustworthiness: ASR & Accuracy under Attack

```
In [ ]: #@title ⚡ Backdoor ASR vs Rounds (FL)
def plot_asr(f1_log):
    rounds = range(1, len(f1_log["asr_hist"])+1)
    plt.figure(figsize=(5,4))
    plt.plot(rounds, f1_log["asr_hist"], marker='o', color="crimson")
    plt.title("Backdoor ASR vs Rounds (FL)")
    plt.xlabel("Round")
    plt.ylabel("ASR")
    plt.grid(True, alpha=0.3)
    plt.show()

plot_asr(f1_log)
```



### Inference:

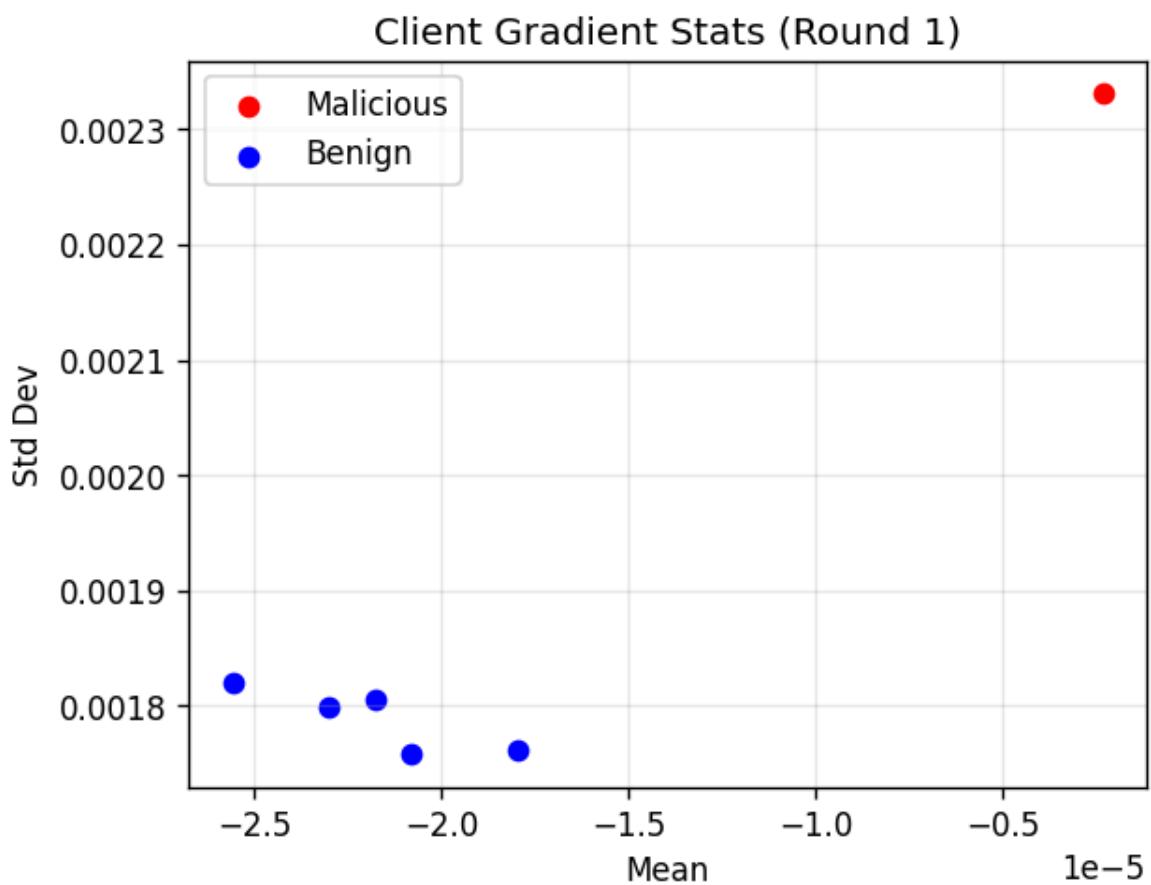
The backdoor ASR remains near zero across rounds, with only a small spike in round 2, indicating limited attack success. This shows that robust aggregation and clipping effectively suppress backdoor influence. Overall, the FL system maintains strong robustness against backdoor attacks while training progresses.

=====

◀ ▶

## D) Attack Detection: Gradient Mean vs Std

```
In [ ]: #@title 📈 Gradient mean vs std scatter (round 1)
gs = fl_log["grad_scatter_round"]
plt.figure(figsize=(5.5,4.2))
for mean, std, mal in zip(gs["mean"], gs["std"], gs["is_mal"]):
    if mal: plt.scatter(mean, std, c="red", label="Malicious" if "Malicious" not in p
    else: plt.scatter(mean, std, c="blue", label="Benign" if "Benign" not in p
plt.xlabel("Mean")
plt.ylabel("Std Dev")
plt.title("Client Gradient Stats (Round 1)")
plt.legend()
plt.grid(True, alpha=0.3)
plt.show()
```



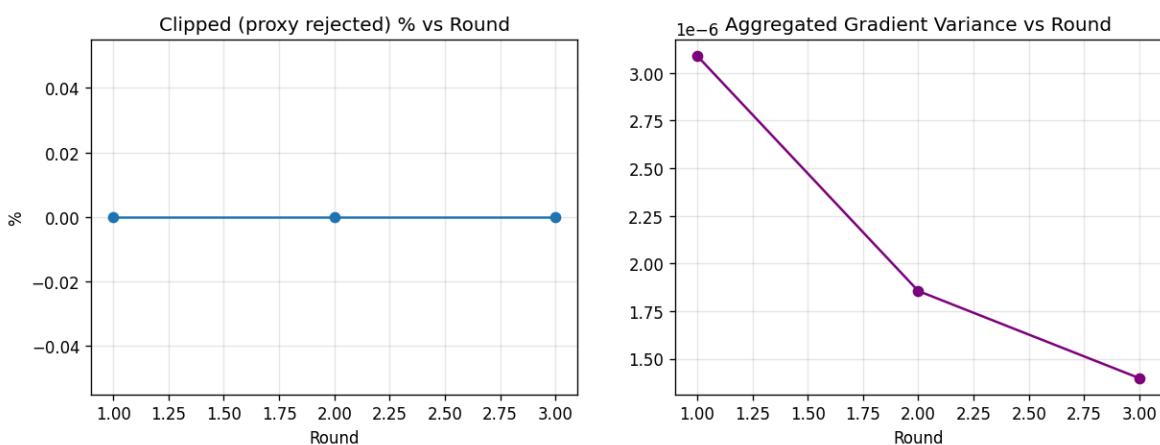
### Inference:

The gradient scatter clearly separates the malicious client (red outlier) from the tight benign cluster (blue), indicating strong detectability.



## E) Robust Aggregation Signals: Rejected Ratio & Gradient Variance

```
In [ ]: #@title ⚽ Rejected (clipped) ratio & Gradient variance
rounds = range(1, len(f1_log["reject_ratio_hist"])+1)
fig, axs = plt.subplots(1,2, figsize=(12,4))
axs[0].plot(rounds, np.array(f1_log["reject_ratio_hist"])*100, marker='o');
axs[1].plot(rounds, f1_log["grad_var_hist"], marker='o', color="purple");
for ax in axs:
    ax.set_xlabel("Round")
    ax.grid(True, alpha=0.3)
plt.show()
```



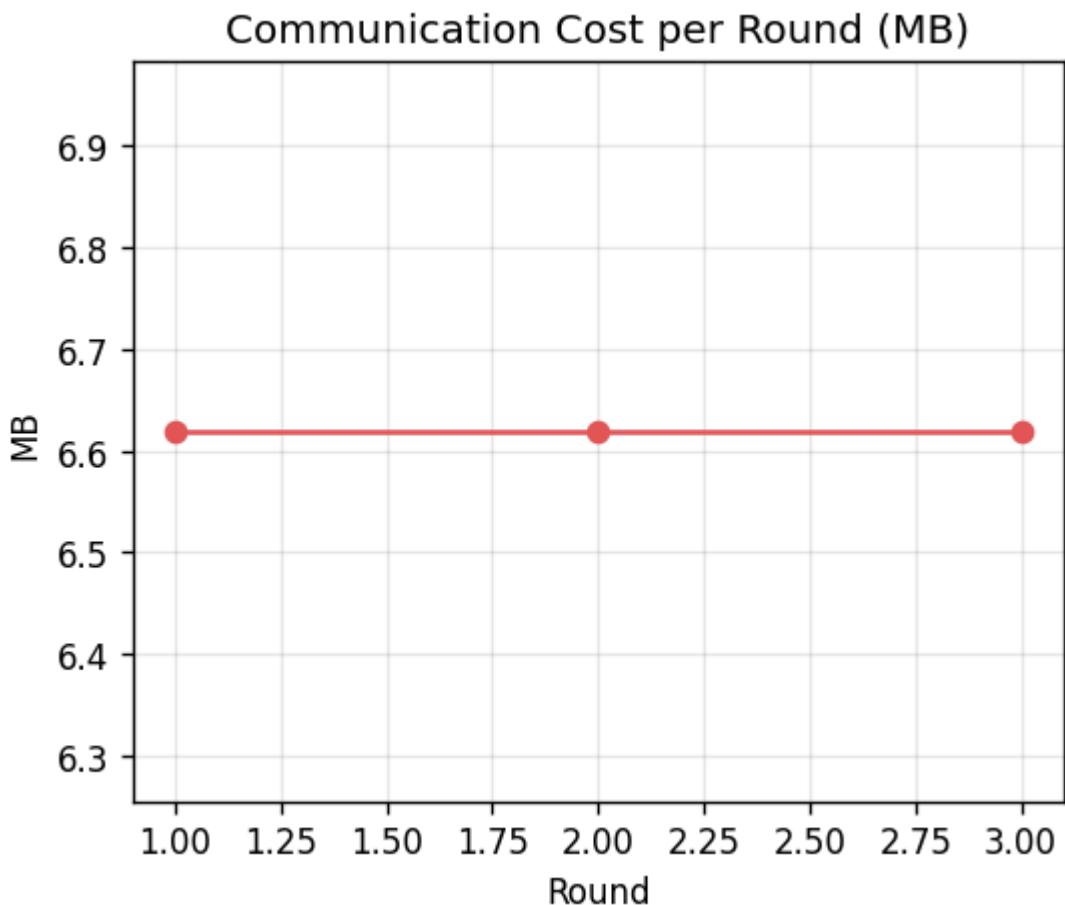
### Inference:

- Clipped (proxy-rejected) = 0% across rounds  $\Rightarrow$  all client updates stayed within the  $\ell_2$  bound; current clip threshold is conservative.
- Aggregated gradient variance drops from  $\sim 3.1\text{e-}6 \rightarrow 1.4\text{e-}6$ , showing the robust aggregator is stabilizing training despite the outlier.
- Overall, the **FL defense is effective**; if you want stricter screening, lower the clip bound or add a cosine-similarity filter to proactively remove outliers.



## F) Communication Cost per Round

```
In [ ]: #@title 🌐 Communication cost per round (MB)
plt.figure(figsize=(5,4))
plt.plot(range(1, len(f1_log["comm_cost_mb_hist"])+1), f1_log["comm_cost_mb_hist"])
plt.title("Communication Cost per Round (MB)")
plt.xlabel("Round")
plt.ylabel("MB")
plt.grid(True, alpha=0.3)
plt.show()
```

**Inference:**

Communication cost per FL round is flat at ~6.6 MB, indicating it's dominated by model/gradient size  $\times$  #clients and is independent of training progress or attacks.

=====

## Conclusion

The TDML framework presents a significant advancement toward solving the limitations of existing distributed machine learning techniques. By integrating blockchain technology for reliability and security, it provides a scalable, efficient, and cost-effective solution for training large deep learning models in environments characterized by resource constraints and malice threats. The experimental evaluations underscore the framework's pragmatic capabilities and position it as a robust alternative to traditional DML architectures.

===== End

=====