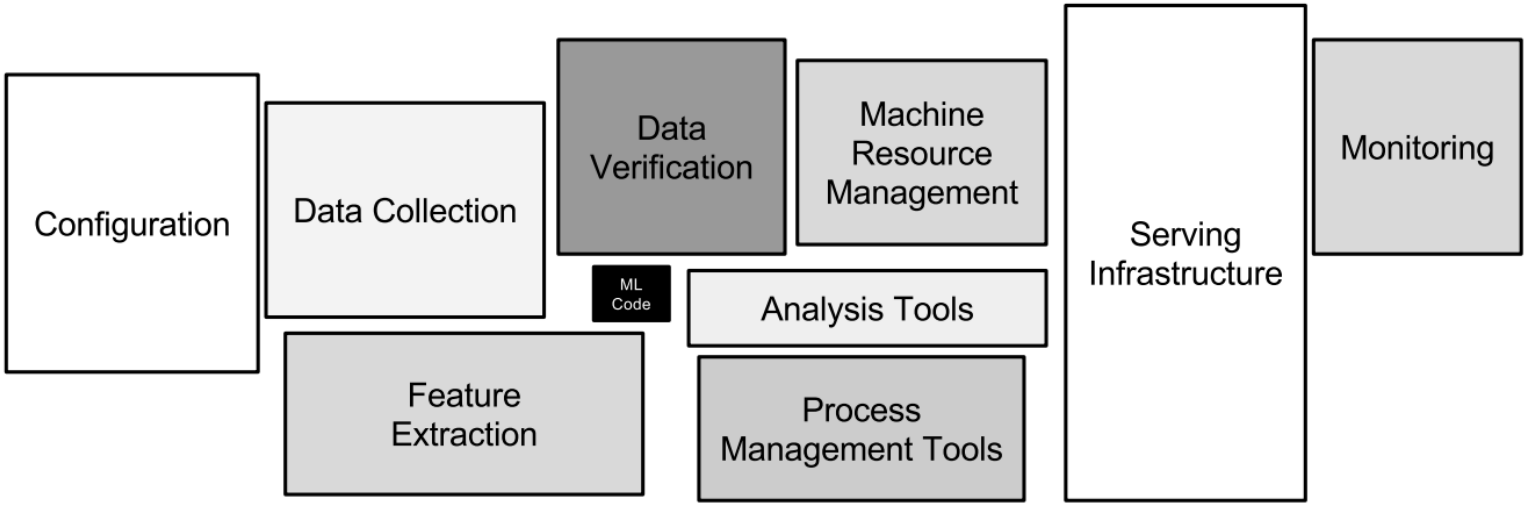
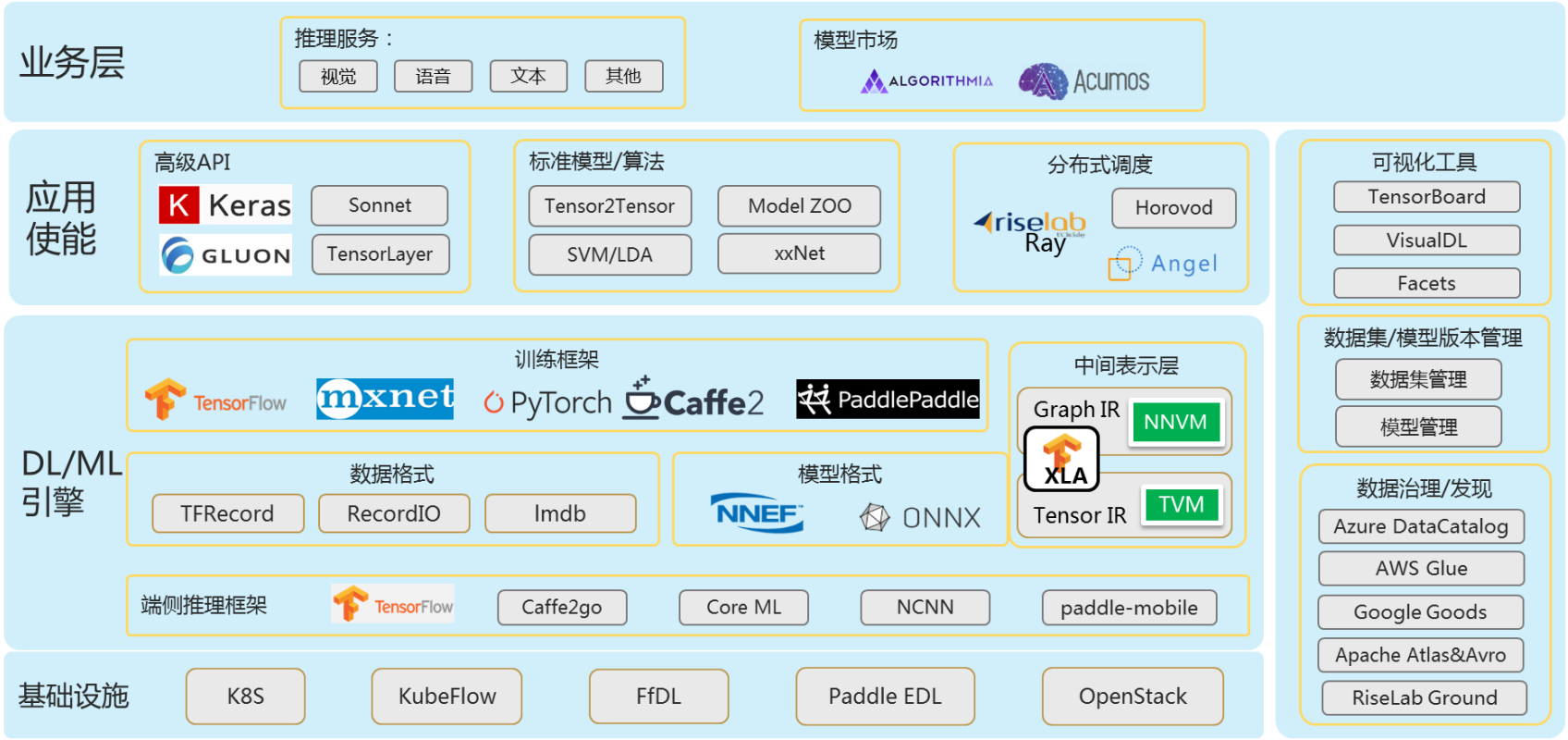
AI领域开源生态分析

机器学习系统隐藏的技术债务



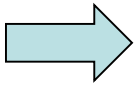
AI技术栈

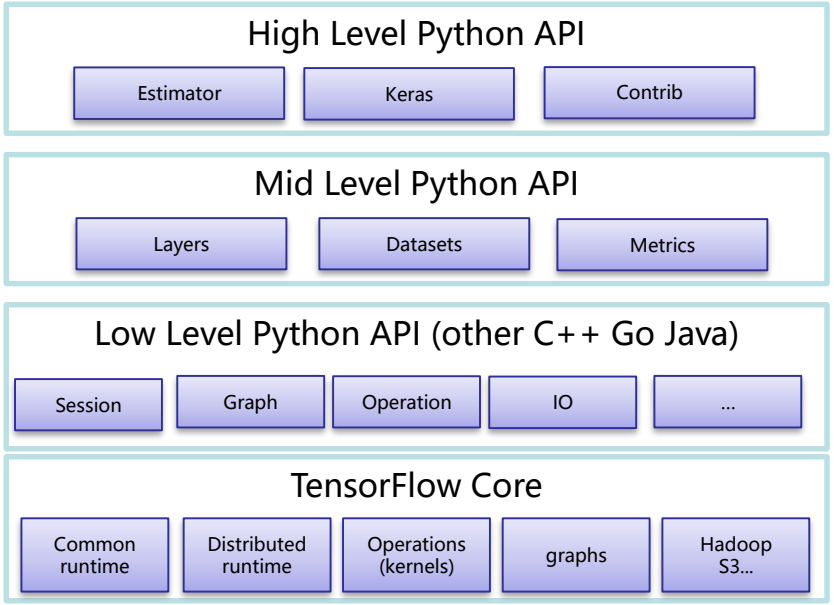

业务层
推理服务：
视觉
语音
文本
其他
模型市场
ALGORITHMIA
Acumos
应用使能
高级API
Keras
Sonnet
GLUON
TensorLayer
标准模型/算法
Tensor2Tensor
Model ZOO
SVM/LDA
xxNet
分布式调度
riselab
Ray
Horovod
Angel
可视化工具
TensorBoard
VisualDL
Facets
数据集/模型版本管理
数据集管理
模型管理
DL/ML引擎
训练框架
TensorFlow
mxnet
PyTorch
Caffe2
PaddlePaddle
中间表示层
Graph IR
NNVM
XLA
Tensor IR
TVM
数据格式
TFRecord
RecordIO
Imdb
模型格式
NNEF
ONNX
数据治理/发现
Azure DataCatalog
AWS Glue
Google Goods
Apache Atlas&Avro
RiseLab Ground
端侧推理框架
TensorFlow
Caffe2go
Core ML
NCNN
paddle-mobile
基础设施
K8S
KubeFlow
FfDL
Paddle EDL
OpenStack

AI训练框架-易用性融合发展

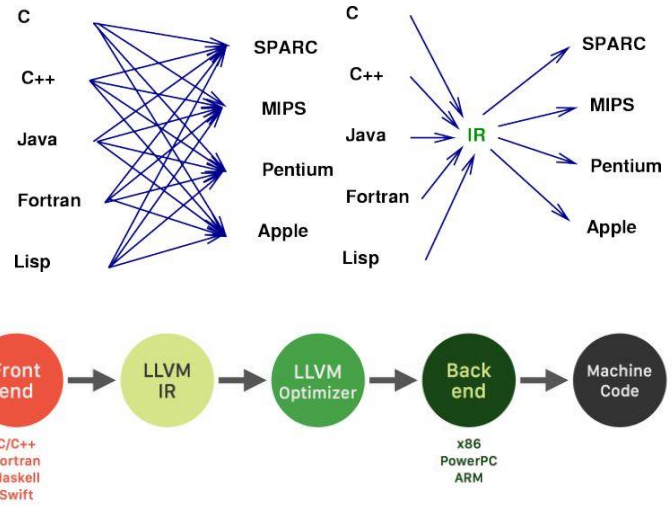
TensorFlow 技术栈

- **硬件对接**
  - 持续跟进NVIDIA 、Intel、TPU 版本支持
- **持续简化训练框架的使用**
  - Estimators、对接Keras 、更好的监控和调试能力
- **Graphs支持**
  - 静态图：静态图的开发支持执行效率高(声明式（declarative）编程)
  - 动态图：开发、调试方便（命令式（imperative）编程） Eager Execution
- **文件系统对接**
  - 默认支持 POSIX 、GCS 、S3 、memory-mapped-file
  - 可以扩展对接其他文件系统





AI的IR之争



TensorFlow XLA

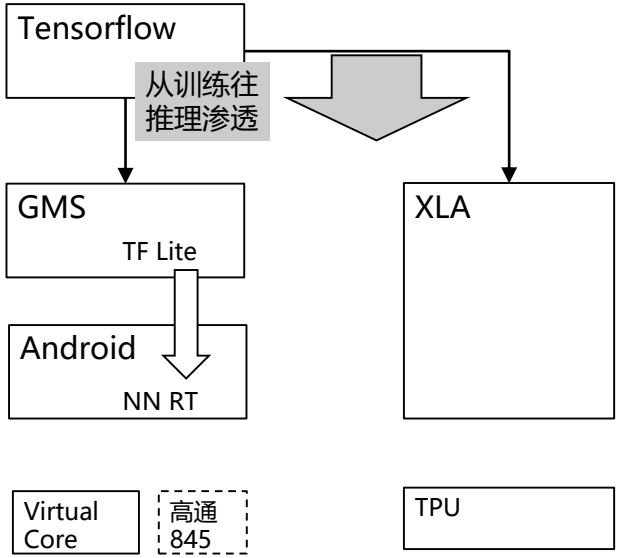
tvm

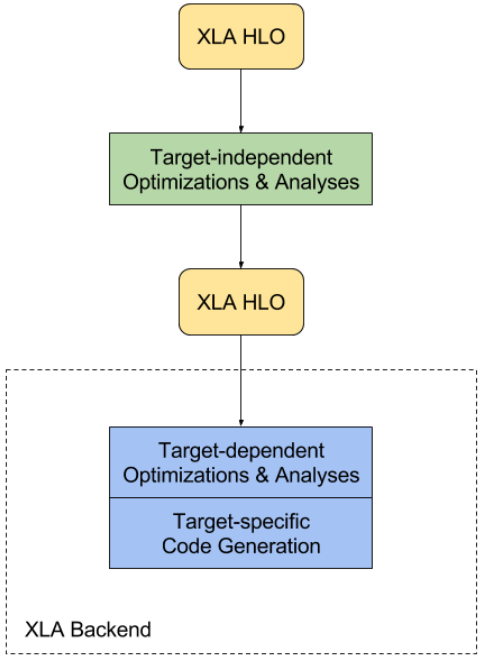
Tensor Comprehensions

JIT: 多个 operation 融合在一起并为它们形成高效的本地机器代码，能用于 CPU、GPU 和自定义加速器

AOT: 通过量化、压缩、编译将AI模型的尺寸复杂度减小到支持移动端设备执行推理的尺寸。

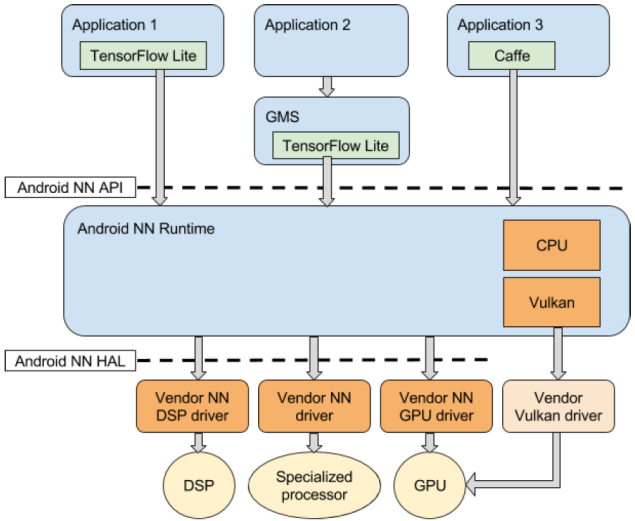
开源领域从训练框架向推理侧延伸，Google/Facebook开始布局





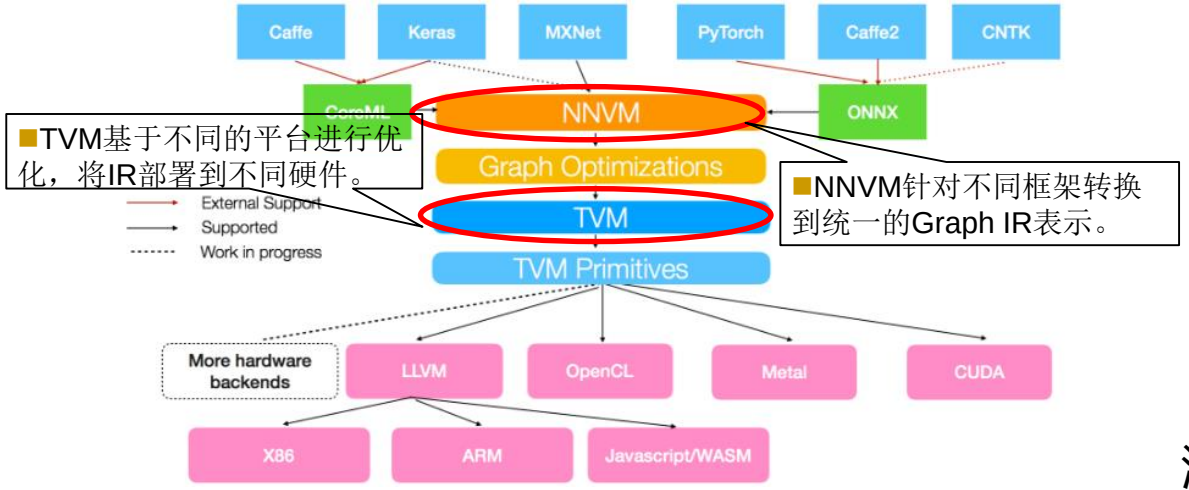
XLA通过两级优化，将TF模型转换为高效的模式放到云端执行。

端侧通过Android升级全面铺开NN架构，目标是全端侧平台支持TF Lite.



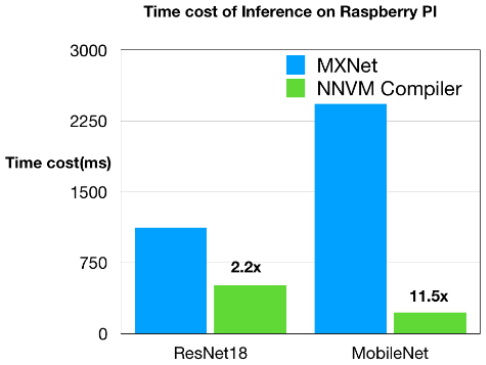
Google通过开源的XLA工具链，利用社区力量构建推理侧优化技术。在端侧升级NN接口，让所有Android成为天然推理机。打通从训练到推理链条。

UW陈天奇团队开源NNVM+TVM，解决了不同模型在推理侧不同后端部署执行问题



■TVM基于不同的平台进行优化，将IR部署到不同硬件。

■NNVM针对不同框架转换到统一的Graph IR表示。

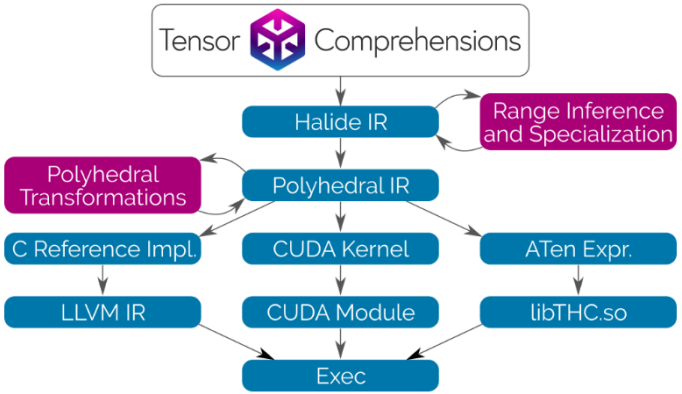


测试结果：效率提升2.2x-11.5倍

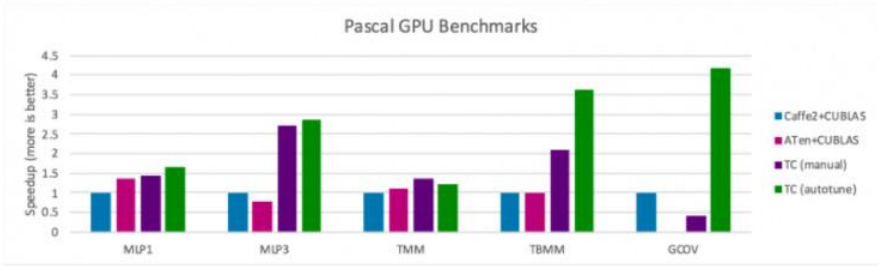
NNVM提供了兼容不同外部模型的能力，并将其转换到统一的IR；TVM采用了图形处理语言Halide的思路，将计算和schedule分开的优化策略，针对不同的硬件后端进行部署。NNVM+TVM提供了面向不同硬件的优化能力。

Facebook开源Tensor Comprehesions项目，提供模型在推理侧执行自动优化能力

业界问题：传统方法优化一次模型的执行效率需要耗费专家大量时间和人力。



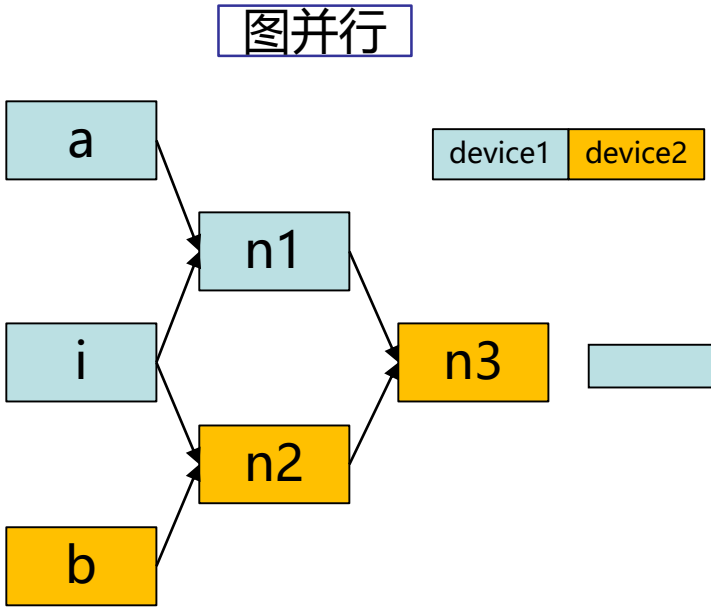
- 用简单语法表达一系列机器学习概念的数学符号
- 基于 Halide IR 数学符号的 C ++前端
- 基于整数集库（ISL）的 Just-in-Time 编译器，
- 一个基于进化搜索的多线程、多 GPU 自动调节器



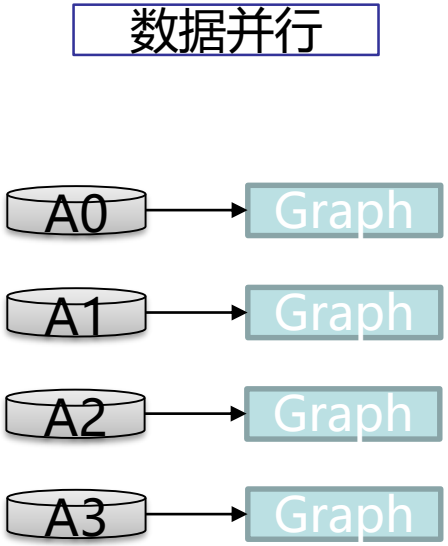
TC利用了多面编译优化技术和JIT编译技术，帮助Facebook解决了自身框架模型(Caffe2)在推理侧的自动优化问题。

测试数据：在Pascal上可获得1.5x-4.2x速度提升

分布式框架实现



Graph被切割运行在不同的Device(Sub Graph)



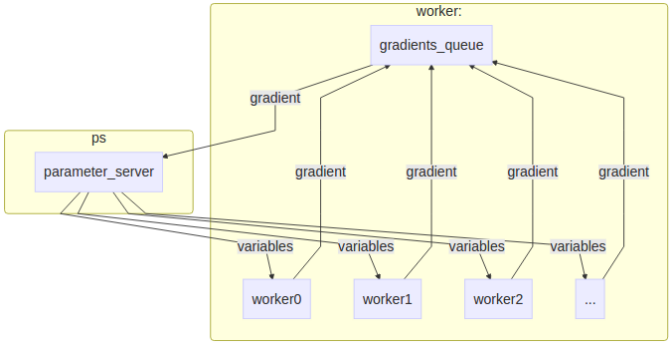
数据被分片运行在不同的Device，共享图权重、一样的图结构

数据并行方式：

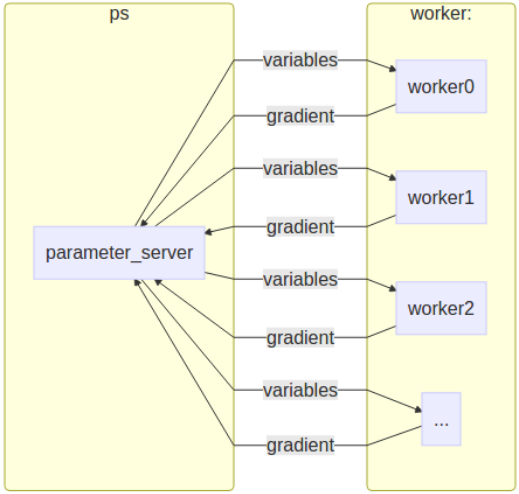
In-graph replication
- 一个Client、一个Session
- 通常同步更新
- 适用于TB级别以下的训练

Between-graph replication
- 多个Client、多个Session
- 同步更新、异步更新均可
- 适用于TB级别以上的训练

分布式参数的更新方式



Synchronous training



Asynchronous training

同步更新和异步更新

in-graph模式和between-graph模式都支持同步和异步更新

同步更新：每次梯度更新，要等所有分发出去的数据计算完成后，返回回来结果之后，把梯度累加算了均值之后，再更新参数。

这样的好处是loss的下降比较稳定， 但是这个的坏处也很明显， 处理的速度取决于最慢的那个分片计算的时间。

异步更新：所有的计算节点，各自算自己的， 更新参数也是自己更新自己计算的结果， 这样的优点就是计算速度快， 计算资源能得到充分利用，但是缺点是loss的下降不稳定， 抖动大。

在数据量小的情况下， 各个节点的计算能力比较均衡的情况下， 推荐使用同步模式；

数据量很大，各个机器的计算性能掺差不齐的情况下，推荐使用异步的方式。

腾讯/Angel（参数服务器）

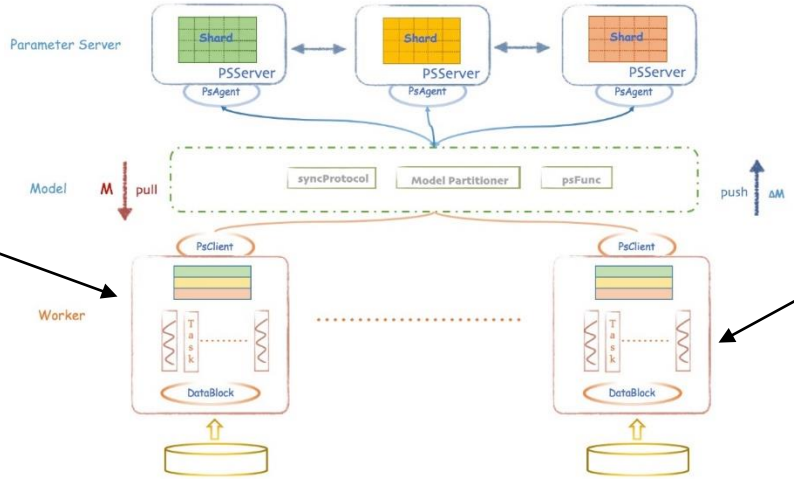
Angel定位解决在大规模机器学习训练侧数据调度问题

核心是通过分布式参数服务器（Parameter Server）将海量训练参数下发到计算节点

提供针对Spark在大规模训练中的性能瓶颈问题提供经过优化的调度策略

核心集成 常用矩阵、向量、特征、分类等基础算法的优化实现，可以单独作为机器学习节点工作

针对大规模机器学习训练的常用算法(聚类、优化、平均、矩阵分解等)提供根据框架模型定向优化过的实现，可以机制作为worker进行部署

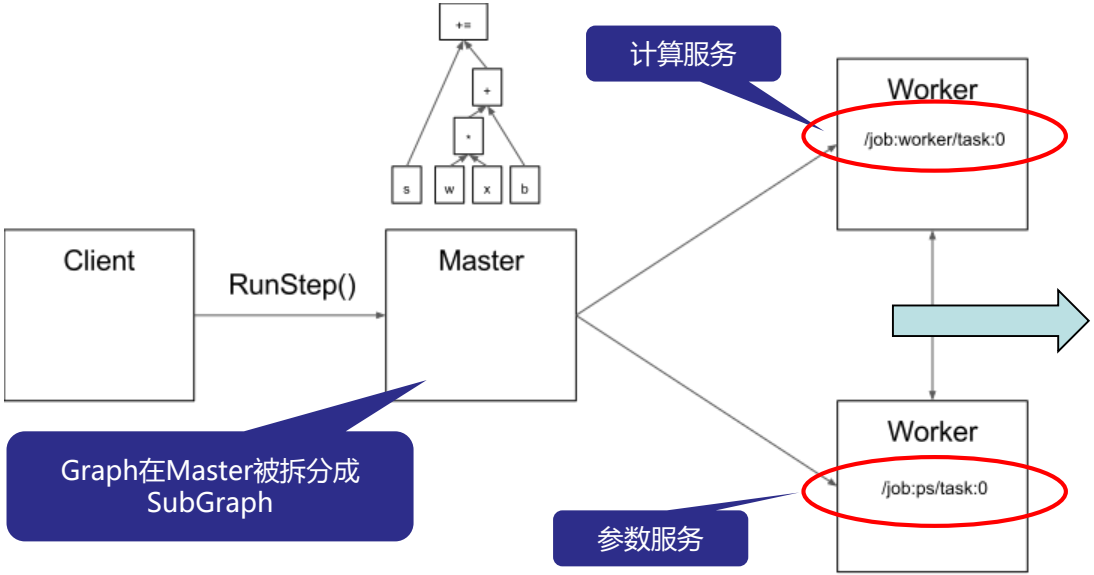


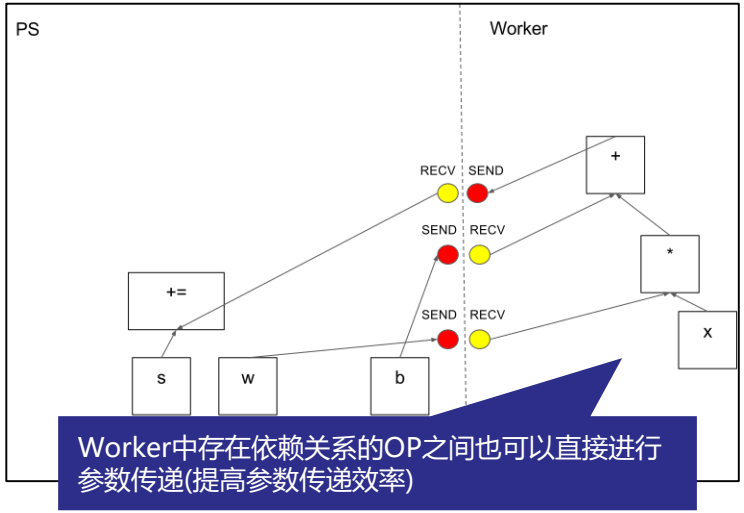
Worker 计算单元，可以通过接口对接其他AI学习平台

大规模机器学习训练侧的资源&时间效率问题现在突出，催生了参数服务器（Parameter Server）等技术

伯克利 REISLab 实验室 针对未来的大规模机器学习需求开源了 Ray 分布式计算框架，并开源了配套基础设施

TensorFlow分布式模型





send/recv：核心效率优化

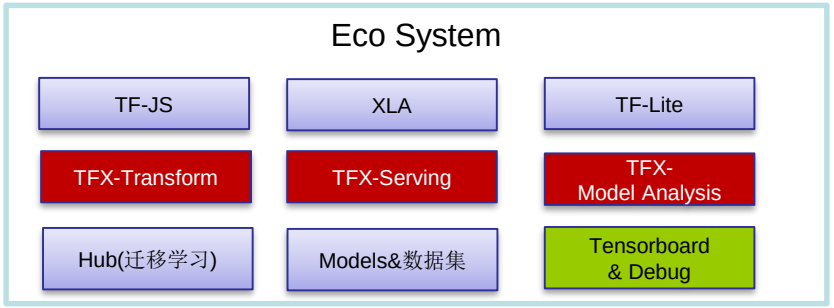
CPU 和 GPU 之间通过 cudaMemcpyAsync() 来 overlap 计算和数据传输

两个本地 GPU 之间通过 DMA 直接传输

在 task 之间（不同的 Worker 服务、不同的计算节点之间）通过 gRPC 或者后来增加的 RDMA 来传输

对NVIDIA的NCCL进行了初步支持（NCCL 2.0 多机多卡在开发计划中已经启动）

生态支撑- TensorFlow 最完善



端到端支持完善

常用Models、公开数据集、可视化支持

TensorFlow Hub:支持增量学习

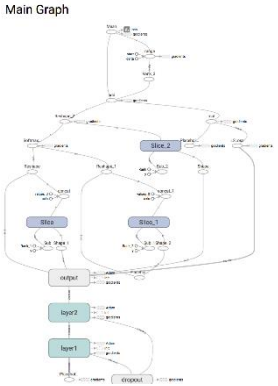
TensorFlow Extended:

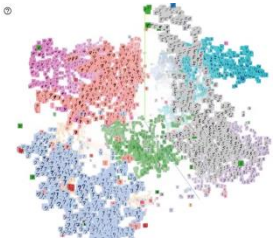
模型保存(TFX-Serving)、

数据处理(TFX-Transform)

模型分析(TFX-Model Analysis)

模型编译优化：XLA、TF-Lite





Keras

PyTorch

GLUON

Tensorboard & Debug

Caffe2

mxnet

TensorFlow

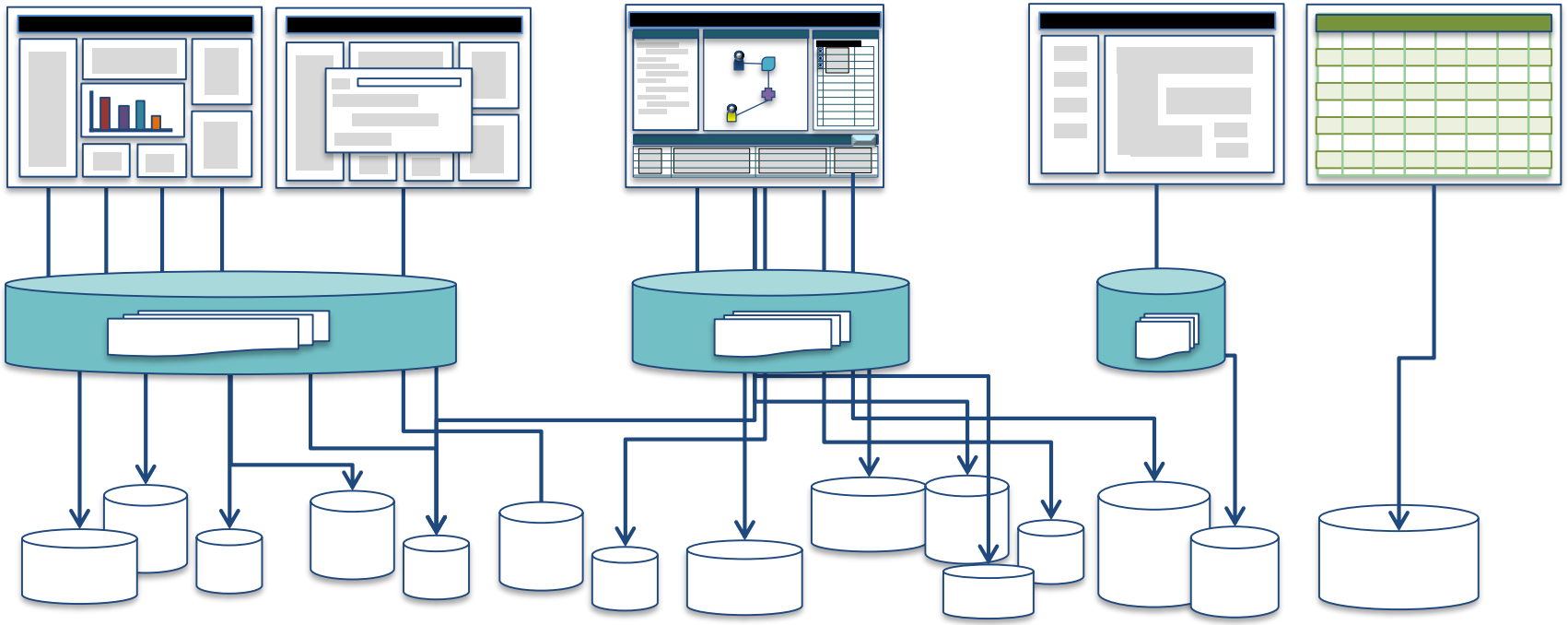
Acumos（端到端工作流与生命周期）

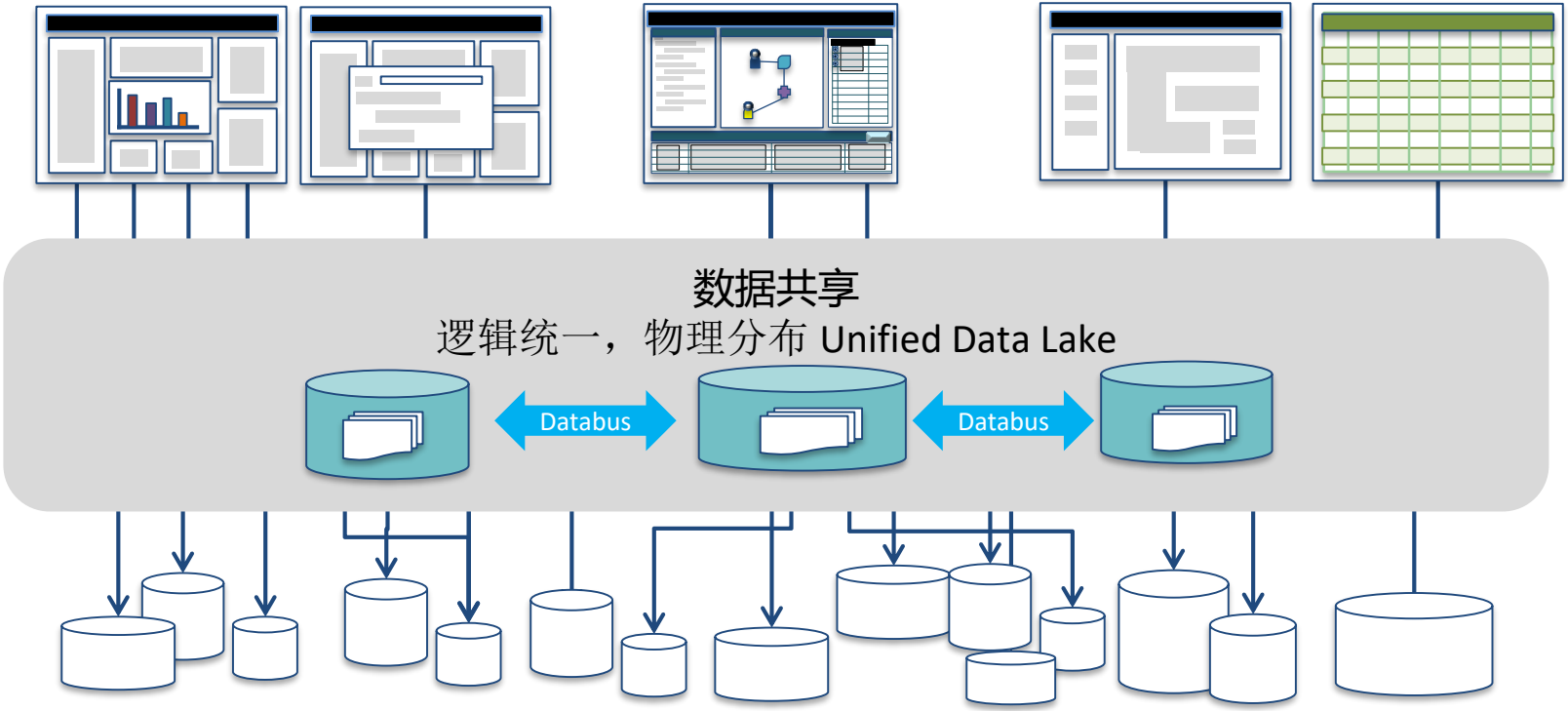
角色	Acumos提供的价值
数据科学家	AI模型提供者，通过微服务容器镜像来提供服务 Acumos 提供安全的微服务容器镜像
数据工程师	AI方案实现者，通过Acumos提供的设计器(DesignStudio) 调用微服务容器来使用AI模型 Acumos 提供商业License管理保证AI模型安全、通过数据代理服务(Data Broker)保证训练数据安全
方案验收	验收数据工程师的实现方案，并将通过验收的AI解决方案放入共享目录(catalog)
最终用户	Acumos 提供的AI市场(Marketplace portal) 发布需求、选择具体的实现 Acumos 通过数据代理服务(Data Broker)、缓存训练数据等安全机制，打通用户侧数据交换

技术	说明
容器	通过容器，将数据科学家提供的AI算法模型进行封装，保护AI算法模型资产
微服务规范	AI算法模型被进行容器封装后遵循Acumos定义的微服务规范对外提供服务
License管理	Acumos通过License形式保证商业使用AI模型和用户数据的法律保证
数据代理 DataBroker	通过提供数据代理(DataBroker)实现Lib，打通用户侧的公私有云数据交换
训练缓存&客户端	将用户的私有数据缓存在受控区域，并通过训练客户端进行隔离受控训练，最终导出结果

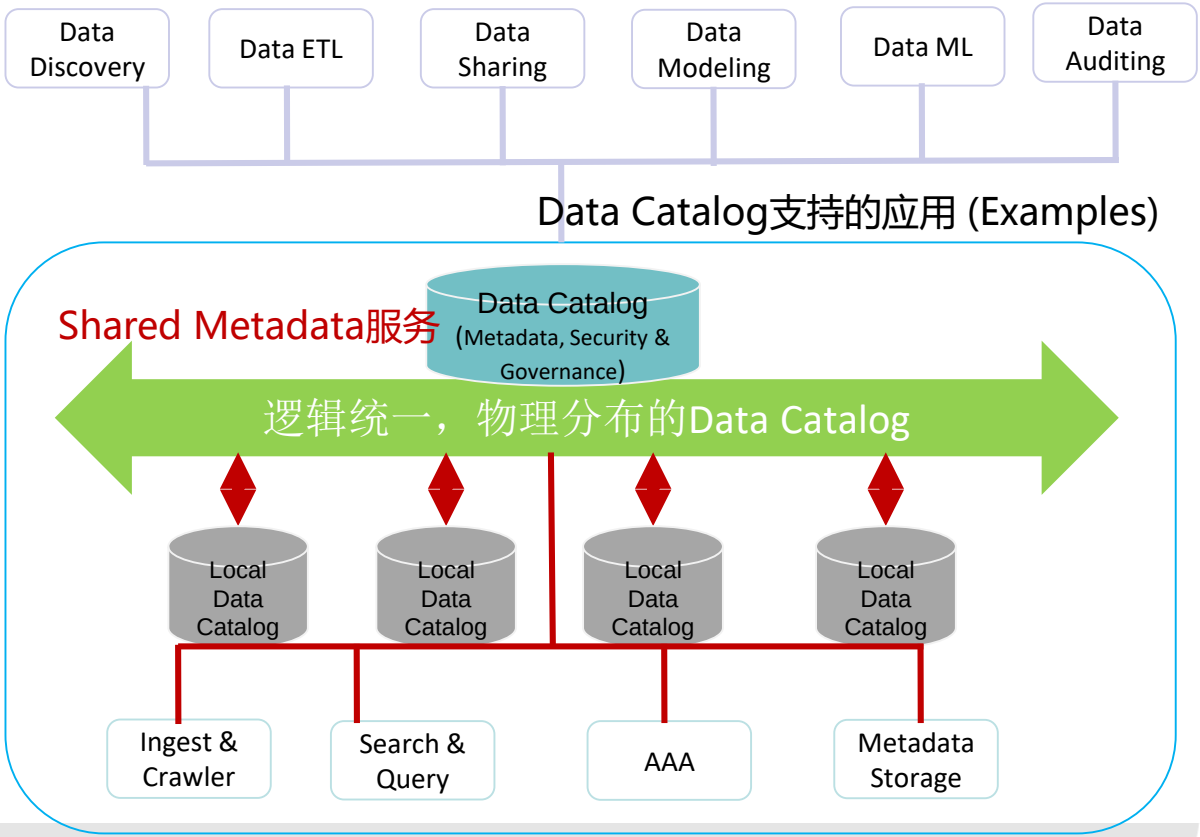
Acumos 主要通过提供一套受控的机制打通跨企业 AI 模型、设计、数据 等不同职责的隔阂，并通过AI市场(Marketplace portal)撮合AI应用需求

我们面临的数据问题




数据共享
逻辑统一，物理分布 Unified Data Lake
Databus
Databus

为AI服务的数据治理


Data Discovery
Data ETL
Data Sharing
Data Modeling
Data ML
Data Auditing
Data Catalog支持的应用 (Examples)
Shared Metadata服务
Data Catalog
(Metadata, Security & Governance)
逻辑统一，物理分布的Data Catalog
Local Data Catalog
Local Data Catalog
Local Data Catalog
Local Data Catalog
Ingest & Crawler
Search & Query
AAA
Metadata Storage

Thank You