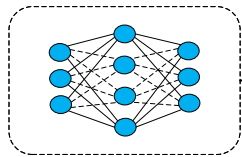


小噪声
+
源数据

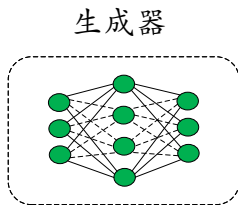


源模型

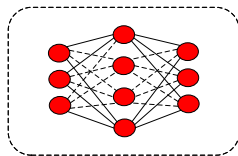


靠近分类
边界的对
抗性样本

训练



生成器

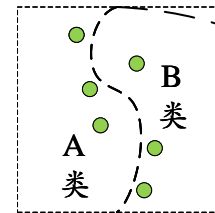


判定器

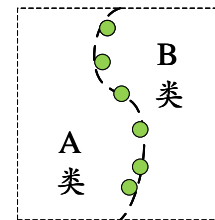


私有近边
界数据

微调

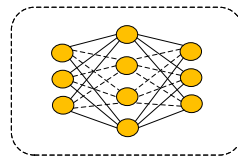


分类边界



最终源模型

推断模型所有权



最终源模型