

Notes on Automatic Differentiation and Differentiable Programming

Giulia Giusti

Contents

1	Automatic Differentiation in Machine Learning: a Survey	2
1.1	Introduction	2
1.2	What AD Is Not	3
1.2.1	AD Is Not Numerical Differentiation	3
1.2.2	AD Is Not Symbolic Differentiation	3
1.3	AD and Its Main Modes	4

1 Automatic Differentiation in Machine Learning: a Survey

Derivatives, mostly in the form of gradients and Hessians, are ubiquitous in machine learning. Automatic differentiation (AD) is a family of techniques similar to but more general than backpropagation for efficiently and accurately evaluating derivatives of numeric functions expressed as computer programs. Until very recently, the fields of machine learning and AD have largely been unaware of each other and, in some cases, have independently discovered each other's results. Despite its relevance, general-purpose AD has been missing from the machine learning toolbox, a situation slowly changing with its ongoing adoption under the names *dynamic computational graphs* and *differentiable programming*.

1.1 Introduction

Methods for the computation of derivatives in computer programs can be classified into four categories:

Method	Pros	Cons
Manual Differentiation		-Time consuming -Error prone
Numerical Differentiation	Easier to implement than the manual method	-Highly inaccurate due to round-off and truncation errors -Scales poorly for gradients (\Rightarrow inappropriate for machine learning)
Symbolic Differentiation	Addresses the weaknesses of both the manual and numerical methods	Often results in complex and cryptic expressions plagued with the problem of <i>expression swell</i>

Furthermore, manual and symbolic methods require models to be defined as closed-form expressions, ruling out or severely limiting algorithmic control flow and expressivity.

The last and most powerful method is represented by *Automatic Differentiation (AD)* which performs a non-standard interpretation of a given computer program by replacing the domain of the variables to incorporate derivative values and redefining the semantics of the operators to propagate derivatives per the chain rule of differential calculus. We would like to stress that AD as a technical term refers to a specific family of techniques that compute derivatives through accumulation of values during code execution to generate numerical derivative evaluations rather than derivative expressions. This allows accurate evaluation of derivatives at machine precision with only a small constant factor of overhead and ideal asymptotic efficiency.

In contrast with the effort involved in arranging code as closed-form expressions under the syntactic and semantic constraints of symbolic differentiation, AD can be applied to regular code with minimal change, allowing branching, loops, and recursion.

In machine learning, a specialized counterpart of AD known as the backpropagation algorithm has been the mainstay for training neural networks, with a colorful history of having been reinvented at various times by independent researchers. In simplest terms, backpropagation models learning as gradient descent in neural network weight space, looking for the minima of an objective function. The required gradient is obtained by the backward propagation of the sensitivity of the objective value at the output, utilizing the chain rule to compute partial derivatives of the objective with respect to each weight. The resulting algorithm is essentially equivalent to transforming the network evaluation function composed with the objective func-

tion under reverse mode AD, which, as we shall see, actually generalizes the backpropagation idea.

1.2 What AD Is Not

Without proper introduction, one might assume that AD is either a type of numerical or symbolic differentiation. Confusion can arise because AD does in fact provide numerical values of derivatives (as opposed to derivative expressions) and it does so by using symbolic rules of differentiation (but keeping track of derivative values as opposed to the resulting expressions), giving it a two-sided nature that is partly symbolic and partly numerical.

1.2.1 AD Is Not Numerical Differentiation

Numerical differentiation is the finite difference approximation of derivatives using values of the original function evaluated at some sample points. In its simplest form, it is based on the limit definition of a derivative. For example, for a multivariate function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ one can approximate the gradient $\nabla f = (\frac{\delta f}{\delta x_1}, \dots, \frac{\delta f}{\delta x_n})$ using

$$\frac{\delta f(x)}{\delta x_i} \approx \frac{f(x + h e_i) - f(x)}{h}$$

where e_i is the i -th unit vector (it is used to modify only the i -th direction of the point x) and $h > 0$ is a small step size.

Let's summarize the pros and cons of numerical differentiation with the following table:

Pros	Cons
Simple to implement	-O(n) evaluations of f for a gradient in n dimensions -Careful selection of the step size h

Numerical approximations of derivatives are inherently ill-conditioned and unstable because using the limit definition of the derivative for finite difference approximation then one commits both cardinal sins of numerical analysis: “thou shalt not add small numbers to big numbers”, and “thou shalt not subtract numbers which are approximately equal”. This is due to the introduction of truncation and round-off errors inflicted by the limited precision of computations and the chosen value of the step size h . Truncation error tends to zero as $h \rightarrow 0$. However, as h is decreased, round-off error increases and becomes dominant.

Numerical Differentiation and ML The major obstacle to applying numerical differentiation to machine learning is the complexity $O(n)$, because n can be as large as millions or billions in state-of-the-art deep learning models. In contrast, approximation errors would be tolerated in a deep learning setting thanks to the well-documented error resiliency of neural network architectures.

1.2.2 AD Is Not Symbolic Differentiation

Symbolic differentiation is the automatic manipulation of expressions for obtaining derivative expressions, it is carried out by applying transformations representing rules of differentiations such as

$$\begin{aligned} \frac{d}{dx}(f(x) + g(x)) &\rightarrow \frac{d}{dx}f(x) + \frac{d}{dx}g(x) \\ \frac{d}{dx}(f(x) \cdot g(x)) &\rightarrow \left(\frac{d}{dx}f(x)\right)g(x) + f(x)\left(\frac{d}{dx}g(x)\right) \end{aligned}$$

When formulae are represented as data structures, symbolically differentiating an expression tree is a perfectly mechanistic process.

Let's summarize the pros and cons of numerical differentiation with the following table:

Pros	Cons
In optimization, symbolic derivatives can give valuable insight into the structure of the problem domain and produce analytical solution of extrema that can eliminate the need for derivative calculation altogether.	No efficient runtime calculation of derivative values because symbolic expression can get exponentially larger than the expression whose derivative they represent.

Automatic differentiation Solution Automatic differentiation tries to solve the efficiency problem of Symbolic Differentiation. When we are concerned with the accurate numerical evaluation of derivatives and not so much with their actual symbolic form, it is in principle possible to significantly simplify computations by storing only the values of intermediate sub-expressions in memory. Moreover, for further efficiency, we can interleave as much as possible the differentiation and simplification steps. This interleaving idea forms the basis of AD and provides an account of its simplest form: *apply symbolic differentiation at the elementary operation level and keep intermediate numerical results, in lockstep with the evolution of the main function.*

1.3 AD and Its Main Modes