Introduction to Machine Learning (IML)

LECTURE #7: OPTIMIZATION

236756 - 2022-2023 WINTER - TECHNION

LECTURER: YONATAN BELINKOV

Today

- Part II: the different aspects of learning
 - 1. Statistics: generalization and PAC theory
 - 2. Modeling:
 - Error decomposition
 - Regularization
 - Model selection
 - 3. Optimization: convexity, gradient descent (today)
 - 4. Practical aspects and potential pitfalls

Optimization

• Regularized Risk Minimization (RRM):

$$\underset{w \in \mathbb{R}^d}{\operatorname{argmin}} \underbrace{\frac{1}{m} \sum_{i=1}^m \ell(y_i, w^\top x_i)}_{\text{loss}} + \lambda R(w)$$
regularization

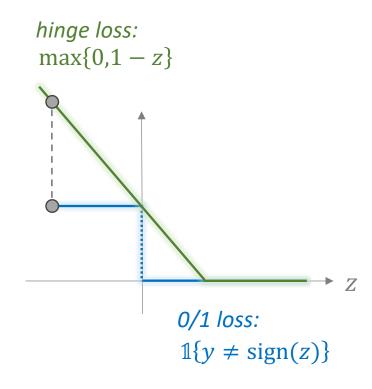
- **Recall**: ERM of 0/1 is hard (discrete)
- **Solution**: continuous proxy

Regularized Risk Minimization (RRM):

$$\underset{w \in \mathbb{R}^d}{\operatorname{argmin}} \frac{1}{m} \sum_{i=1}^m \ell(y_i, w^\top x_i) + \lambda R(w)$$

$$\underset{\text{regularization}}{\operatorname{loss}}$$

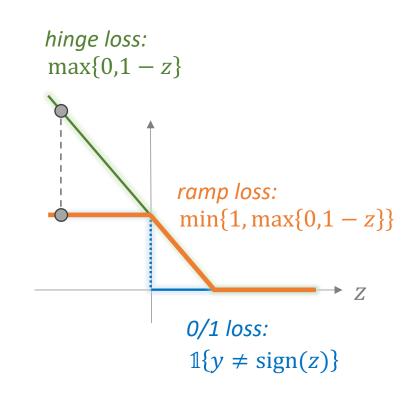
- Recall: ERM of 0/1 is hard (discrete)
- **Solution**: continuous proxy
- Soft SVM's hinge loss is one option
- Problem: unnecessarily large penalties for far from margin



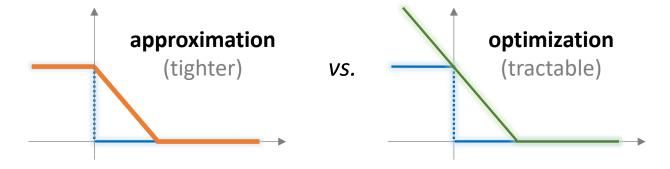
Regularized Risk Minimization (RRM):

$$\underset{w \in \mathbb{R}^d}{\operatorname{argmin}} \frac{1}{m} \sum_{i=1}^m \frac{\ell(y_i, w^\top x_i)}{\operatorname{loss}} + \lambda R(w)$$
regularization

- **Recall**: ERM of 0/1 is hard (discrete)
- **Solution**: continuous proxy
- Soft SVM's hinge loss is one option
- Problem: unnecessarily large penalties for far from margin
- Alternative: ramp loss
- **Problem**: optimization... (today we'll see why)

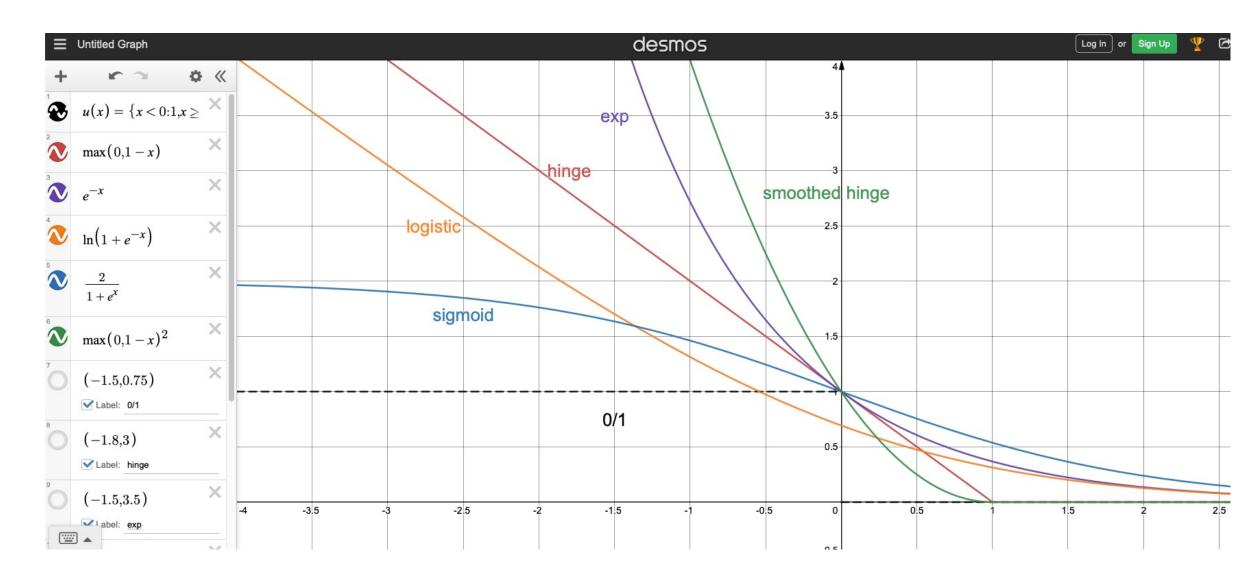


• Tradeoff:

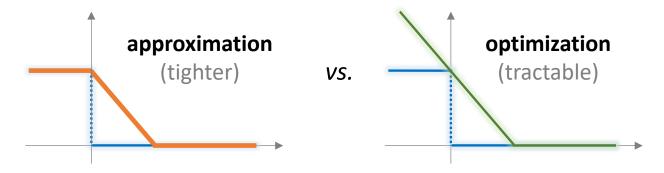


- Many proxies out there!
- [DESMOS]

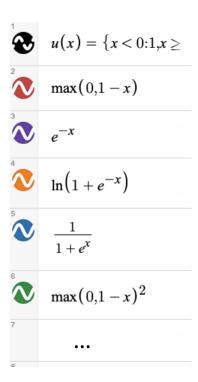
Proxy losses



• Tradeoff:



- Many proxies out there which is better?
- No definite answer
- But we can say some things sometimes
- Today: focus on optimization (but also generalization)
- Functional properties that give optimization guarantees:



- (sub-)differentiable
- > convex
- > Lipschitz
- > smooth
- bounded



One algorithm to rule them all

- Goal: solve $\min_{w \in \mathbb{R}^d} f(w)$
- (in learning: f is the learning objective, w are model parameters)
- Approach: Gradient Descent (GD) [~Cauchy 1847]

$$w_{t+1} = w_t - \eta \nabla f(w_t)$$

- "First order iterative method"
- Forms the basis for many other optimization algorithms (we'll see some today)

• Definition:

The gradient of f w.r.t. w is a vector function of partial derivatives,

$$\nabla f = \begin{pmatrix} \frac{\partial f}{\partial w_1} \\ \vdots \\ \frac{\partial f}{\partial w_d} \end{pmatrix}$$

• Gradient evaluation at $\overline{w} \in \mathbb{R}^d$:

$$\nabla f(\overline{w}) \in \mathbb{R}^d$$

Gradient Descent (GD)

- Initialize w_0 (e.g., $w_0 = \vec{0}$)
- Repeat:

•
$$w_{t+1} = w_t - \eta \nabla f(w_t)$$

• Until convergence (e.g., $||w_{t+1} - w_t|| \le \epsilon$)

- View I: fog in mountains
- View II: local greedy descent
- View III: optimize simple approximations

$$@t: f(w) \approx f(w_t) + \nabla f(w_t)^{\mathsf{T}}(w - w_t)$$

- View IV: Taylor expansion + tradeoff
 - $f(w_t + \delta) \approx f(w_t) + \nabla f(w_t)^{\mathsf{T}} \delta, \ \delta \in \mathbb{R}^d$
 - $w_{t+1} = w_t + \delta$ close to w_t , i.e., $\|\delta\|_2$ is small
 - $w_{t+1} = \underset{w}{\operatorname{argmin}} \frac{1}{2} \|w w_t\|_2^2 + \eta (f(w_t) + \nabla f(w_t)^{\mathsf{T}} (w w_t))$
 - $\partial = 0 \Rightarrow w_{t+1} = w_t \eta \nabla f(w_t)$

Gradient Descent (GD)

- Initialize w_0 (e.g., $w_0 = \vec{0}$)
- Repeat:

•
$$w_{t+1} = w_t - \eta \nabla f(w_t)$$

• Until convergence (e.g., $||w_{t+1} - w_t|| \le \epsilon$)

- View I: fog in mountains
- View II: local greedy descent
- View III: optimize simple approximations

@t:
$$f(w) \approx \nabla f(w_t)^{\mathsf{T}} w$$

- View IV: Taylor expansion + tradeoff
 - $f(w_t + \delta) \approx f(w_t) + \nabla f(w_t)^{\mathsf{T}} \delta, \ \delta \in \mathbb{R}^d$
 - $w_{t+1} = w_t + \delta$ close to w_t , i.e., $||\delta||_2$ is small
 - $w_{t+1} = \underset{w}{\operatorname{argmin}} \frac{1}{2} ||w_t w||_2^2 + \eta (f(w_t) + \nabla f(w_t)^{\mathsf{T}} (w w_t))$
 - $\partial = 0 \Rightarrow w_{t+1} = w_t \eta \nabla f(w_t)$

Gradient Descent (GD)

- Initialize w_0 (e.g., $w_0 = \vec{0}$)
- Repeat:

•
$$w_{t+1} = w_t - \eta \nabla f(w_t)$$

• Until convergence (e.g., $||w_{t+1} - w_t|| \le \epsilon$)

Need to determine:

- 1. Step size or learning rate η
- 2. Stopping criterion

• **Definition**: Let $B_{\epsilon}(w) = \{v: \|w - v\| \le \epsilon\}$ be a ball of radius ϵ around w. Then w is a *local minimum* of f if

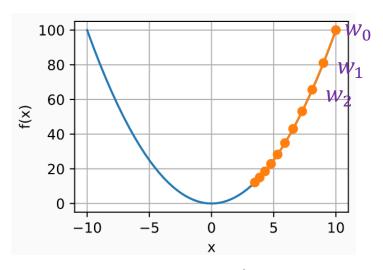
$$\exists \epsilon > 0 \ \forall v \in B_{\epsilon}(w), \ f(w) \leq f(v)$$

- Claim: if η is small enough, then $f(w_{t+1}) < f(w_t)$ for any non-minimum w_t (this is the "descent" part of "gradient descent")
- **Proof**: consider non-minimum w_t and negate
- Corollary: GD converges* to a local minimum (or saddle point!) * for an appropriate choice of η
- **Trick**: use time-varying learning rate η_t , for example, $\eta_t = 1/t$
- Note: if w_t is a local minimum then $\nabla f(w_t) = 0$ (but not iff!)

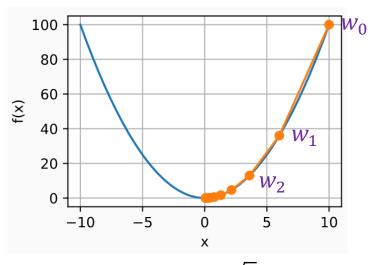
Learning rate

• **Q1**: So GD converges for learning rate $\eta_t = 1/t$. Are we done?

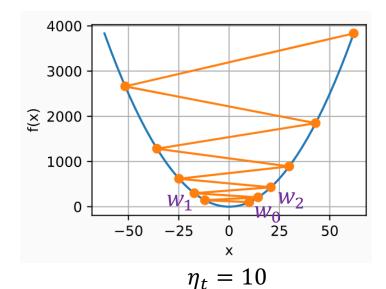
• **A1**: No!



 $\eta_t = 1/t$ slow convergence (too slow!)



 $\eta_t = 1/\sqrt{t}$ "just right" (how can we know?)



divergence

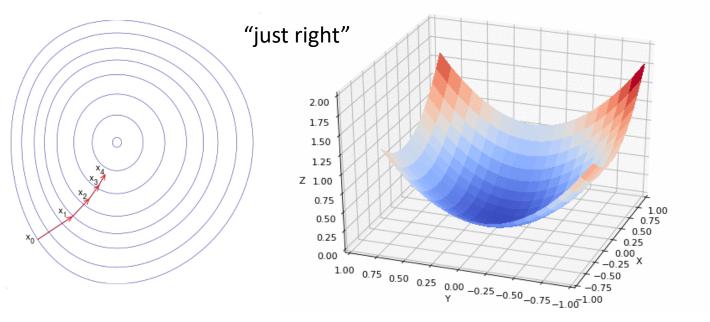
(too fast!)

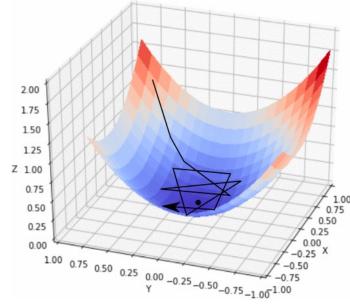
Learning rate

• **Q1**: So GD converges for learning rate $\eta_t = 1/t$. Are we done?

• **A1**: No!

divergence? slow convergence?



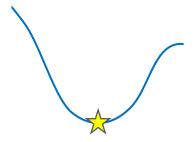


• Choosing the learning rate can be tricky – we will return to this.

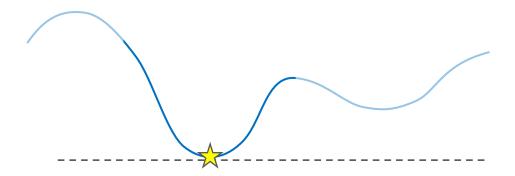
When to stop

- Q2: So GD converges in theory. But in practice, how do we know when (and if) it did?
- A2: Can't "know", but can estimate.
- Set criteria for stopping, for example:
 - stop when $||w_{t+1} w_t|| \le \epsilon$
 - or when $||f(w_{t+1}) f(w_t)|| \le \epsilon$
 - or when $\|\nabla f(w_t)\| \le \epsilon$
 - or ...
- Actually, knowing when to stop is (also) tricky and has statistical implications!
 We will return to this as well.

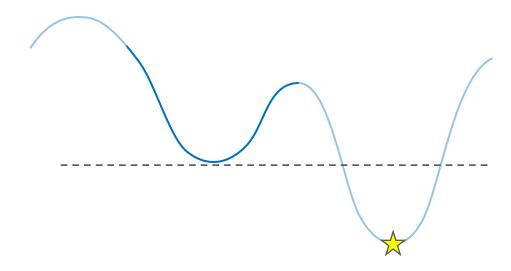
- Q3: So GD can converge to a local minimum. Should we be happy?
- A3: It depends...



- Q3: So GD can converge to a local minimum. Should we be happy?
- A3: It depends...

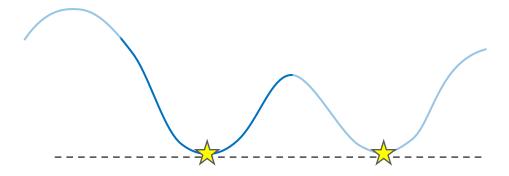


- Q3: So GD can converge to a local minimum. Should we be happy?
- A3: It depends...



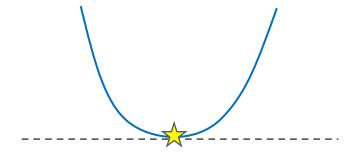
• Q3: So GD can converge to a local minimum. Should we be happy?

• A3: It depends...



• **Goal:** find conditions on *f* for which GD is guaranteed to work well

- Q3: So GD can converge to a local minimum. Should we be happy?
- A3: It depends...



• **Goal:** find conditions on *f* for which GD is guaranteed to work well

Convexity

Descending with guarantees

- Recall foggy mountain story
- When will the "going down" approach help you reach your cabin?
- When mountain range is:
 - 1. continuous
 - 2. smooth
 - 3. has a single valley
- Enter convexity.
- [on board]



Convex sets

• **Definition:** convex combination:

$$\alpha u + (1 - \alpha)v$$
 for $u, v \in \mathbb{R}^d$, $\alpha \in [0,1]$

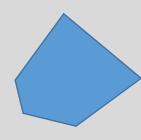
- As interpolation point on line between u, v
- **Definition**: *C* is a *convex set* if

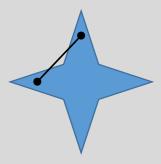
 $\forall u, v \in C$, any convex combination of u, v is also in C

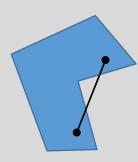
 \mathbb{R}^d

• Examples:









$$H_{w,b} = \{x : w^{\mathsf{T}} x \ge b\}$$

• **Definition:** For C convex set, $f: C \to \mathbb{R}$ is convex function if $\forall u, v \in C$, $\alpha \in [0,1]$: $f(\alpha u + (1-\alpha)v) \le \alpha f(u) + (1-\alpha)f(v)$

GD convergence rates

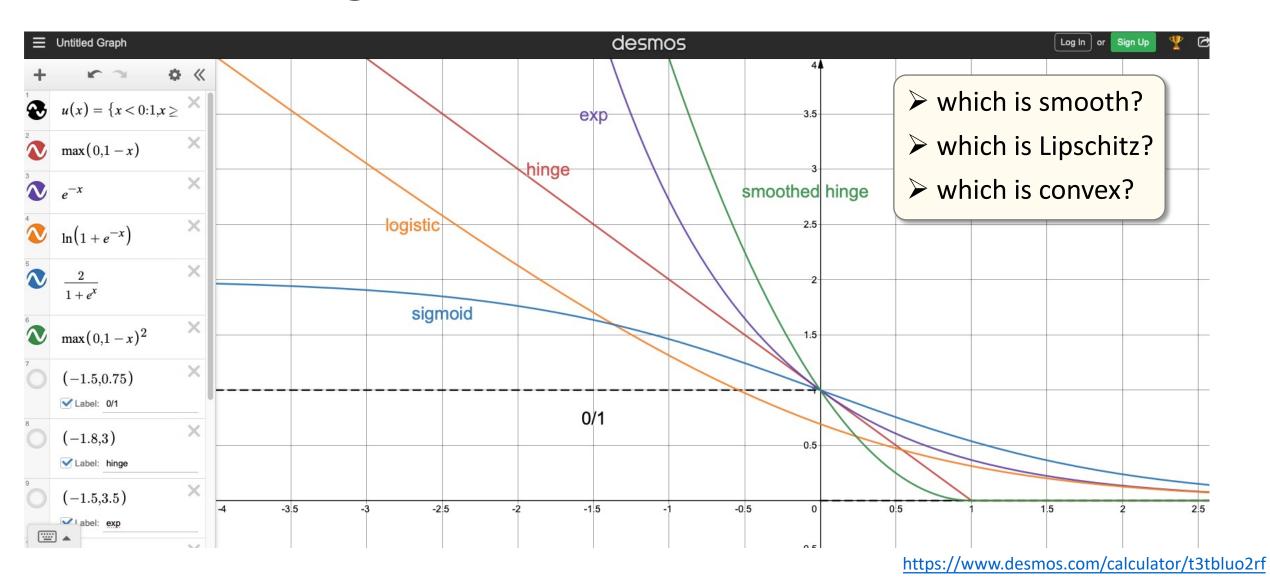
- β -Smooth: $f(x_t) f(x^*) \le \frac{2\beta \|x_0 x^*\|}{t+4} = O\left(\frac{\beta}{t}\right)$
 - Lower bound: $\Omega\left(\frac{\beta}{t^2}\right)$
- L-Lipschitz: $f(x_t) f(x^*) = O\left(\frac{L}{\sqrt{t}}\right)$
- σ -Strongly convex: $f(x_t) f(x^*) = O(e^{-2\sigma t})$
- Depends on:
 - Type
 - Parameter
 - Initial guess!

```
f is \beta-Smooth if \|\nabla f(u) - \nabla f(w)\| \le \beta \|u - w\|
```

$$f$$
 is L-Lipschitz if
$$\|f(u) - f(w)\| \le L\|u - w\|$$

```
f is \sigma-Strongly convex if f(\alpha w + (1 - \alpha)u) \leq \alpha f(w) + (1 - \alpha)f(u) - \frac{\sigma}{2}\alpha(1 - \alpha)\|u - w\|^2
```

GD convergence rates



Optimization for learning

• Recall ERM/RLM:

$$\underset{\theta}{\operatorname{argmin}} \frac{1}{m} \sum_{i=1}^{m} \ell(y_i, f_{\theta}(x_i)) + \lambda R(\theta)$$

How can we tell if the learning objective is convex?

Composition rules

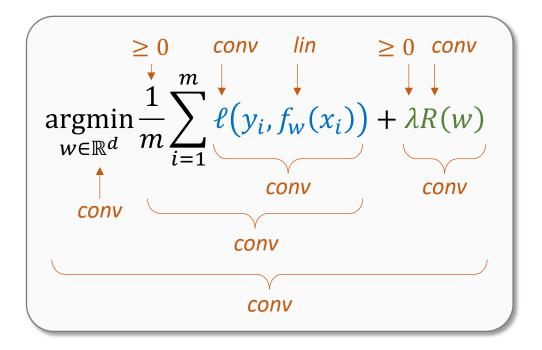
- Convexity-preserving operations:
 - 1. **scaling**: f convex, $\alpha \ge 0 \Rightarrow \alpha f$ convex [easy]
 - 2. **sum**: f, g convex $\Rightarrow f + g$ convex [tirgul]
 - 3. **noneg. weighted sum**: f_i convex, $\alpha_i \ge 0 \Rightarrow \sum_i \alpha_i f_i$ convex
 - 4. **composition**: f convex, g linear $\Rightarrow f \circ g$ convex [on board]
 - 5. ...
- (these are sufficient conditions, but not necessary)

Composition of convex and linear is convex

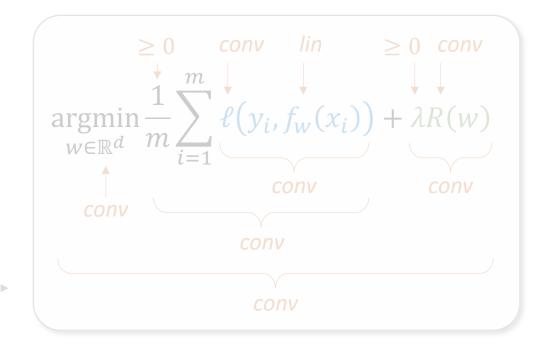
- Claim: if g is convex and h is linear, then $f = g \circ h$ is convex
- **Proof**: $f(\alpha u + (1 \alpha)v) = g(h(\alpha u + (1 \alpha)v)) =_{h \ linear}$ $g((\alpha u + (1 - \alpha)v)^T x + b) = g(\alpha u^T x + (1 - \alpha)v^T x + b) =$ $g(\alpha u^T x + (1 - \alpha)v^T x + (\alpha + 1 - \alpha)b) =$ $g(\alpha (u^T x + b) + (1 - \alpha)(v^T x + b)) = g(\alpha h(u) + (1 - \alpha)h(v))$ $\leq_{g \ convex} \alpha g(h(u)) + (1 - \alpha)g(h(v)) = \alpha f(u) + (1 - \alpha)f(v)$

- **Claim**: The following conditions are sufficient for the learning objective to be convex (in w):
 - 1. $\ell(\cdot,\cdot)$ is convex (in it's second argument)
 - 2. $R(\cdot)$ is convex
 - 3. f_w is linear (in w, i.e., $f_w(x) = w^T x$)

- **Claim**: The following conditions are sufficient for the learning objective to be convex (in w):
 - 1. $\ell(\cdot,\cdot)$ is convex (in it's second argument)
 - 2. $R(\cdot)$ is convex
 - 3. f_w is linear (in w, i.e., $f_w(x) = w^T x$)
- Let's try



- Claim: The following conditions are sufficient for the learning objective to be convex (in w):
 - 1. $\ell(\cdot, \cdot)$ is convex (in it's second argument)
 - 2. $R(\cdot)$ is convex
 - 3. f_w is linear (in w, i.e., $f_w(x) = w^T x$)
- Let's try
- Claim: The Soft SVM objective is convex
- Need to prove:
 - 1. $\max\{0, 1 z\}$ is convex [ex]
 - 2. ℓ_2 -norm squared is convex [tirgul]
- Corollary: can solve with GD!



$$\underset{w \in \mathbb{R}^d}{\operatorname{argmin}} \frac{1}{m} \sum_{i=1}^m \max\{0, 1 - y_i \cdot w^{\mathsf{T}} x_i\} + \lambda ||w||_2^2$$

Variations, extensions, and beyond

The computational cost of GD

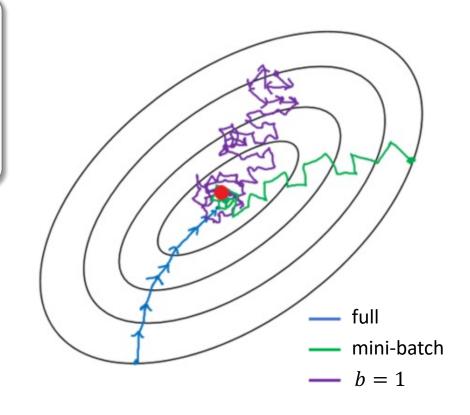
For running GD we need to compute gradients of the learning objective.

• Note:
$$\nabla \left(\frac{1}{m}\sum_{i=1}^{m}\ell(y_i,f_w(x_i))\right) = \frac{1}{m}\sum_{i=1}^{m}\nabla\ell(y_i,f_w(x_i))$$

- For Soft SVM:
 - Each $\nabla \max\{0,1-y_i\cdot w^{\top}x_i\}$ costs: O(d)
 - Overall: O(dm)
- GD can be costly!
- **Solution**: use *approximate* gradients

Taking approximate gradient steps

- Observation: sampling average is unbiased (but noisy) estimator
- Idea: replace full gradient with average of small random set of examples
- Stochastic Gradient Descent (SGD):*
 - 1. Sample small random "mini-batch" $B \subset S$ of size b
 - 2. Compute average gradient $\overline{\nabla} = \frac{1}{b} \sum_{i \in B} \nabla_i$
 - 3. Apply *approximate* gradient step $x_{t+1} = x_t \eta \bar{\nabla}$
- **Pros**: reduces compute time (significantly!)
- Cons: adds noise (but often worth it)
- Hyper parameter b trades off compute time with noise



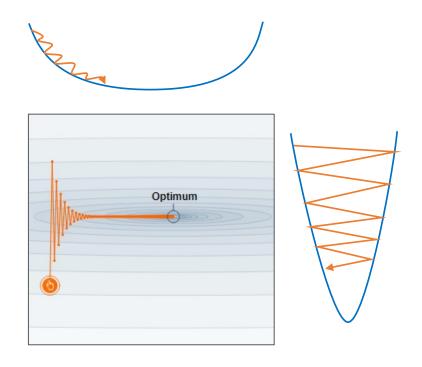
Looking back

- Consider 2D quadratic with highly varying curvatures
 - On low-curvature dimension, GD crawls hesitantly
 - On high-curvature dimension, GD oscillates frantically
- Adding "momentum" sorts this out:

(imagine a rolling ball)

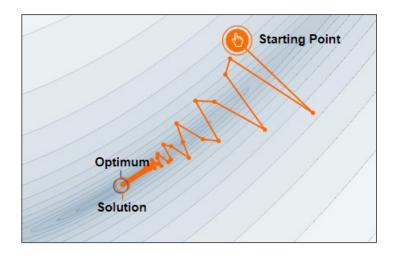


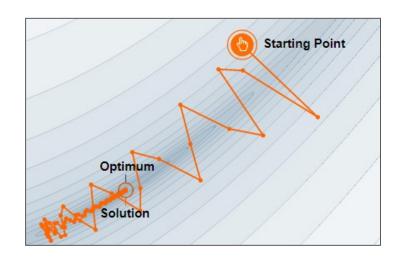
- increases in dimensions where gradient preserves direction
- *decreases* in dimensions where gradient direction varies
- Typical β values: 0.9, 0.95, 0.99



Looking forward

- Momentum is great, but can overshoot
- **Solution**: look into *future*
- **Idea:** *imagine* momentum has been applied, then compute gradient





Looking forward

- Momentum is great, but can overshoot
- **Solution**: look into *future*
- Idea: imagine momentum has been applied, then compute gradient
- Nesterov's accelerated gradient:

$$\widetilde{w}_{t+1} = w_t + \beta v_t$$

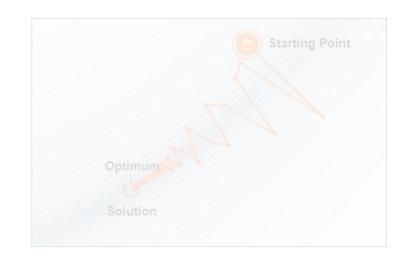
$$v_{t+1} = \beta v_t - \eta \nabla f(\widetilde{w}_{t+1})$$

$$w_{t+1} = w_t + v_{t+1}$$

• Equivalent:

$$v_{t+1} = \beta v_t - \eta \nabla f(w_t)$$

$$w_{t+1} = w_t + (1+\beta)v_{t+1} - \beta v_t$$



Vs. momentum:

$$\begin{aligned} v_{t+1} &= \beta v_t - \eta \nabla f(w_t) \\ w_{t+1} &= w_t + v_{t+1} \\ &= w_t - \eta \nabla f(w_t) + \beta v_t \end{aligned}$$

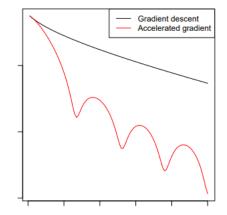
Looking forward

Nesterov's accelerated gradient:

$$v_{t+1} = \beta v_t - \eta \nabla f(w_t)$$

$$w_{t+1} = w_t + (1+\beta)v_{t+1} - \beta v_t$$

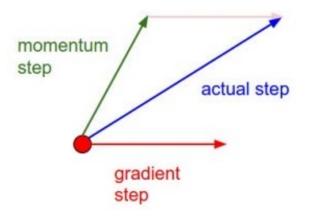
This is not a descent method!



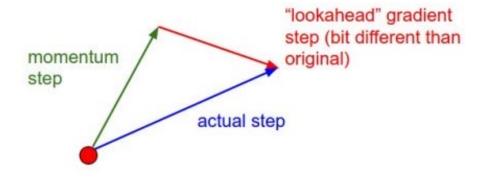
Nonetheless, converges faster:

$$f(x_t) - f(x^*) \le \frac{2\beta \|x_0 - x^*\|}{t^2} = O\left(\frac{\beta}{t^2}\right)$$

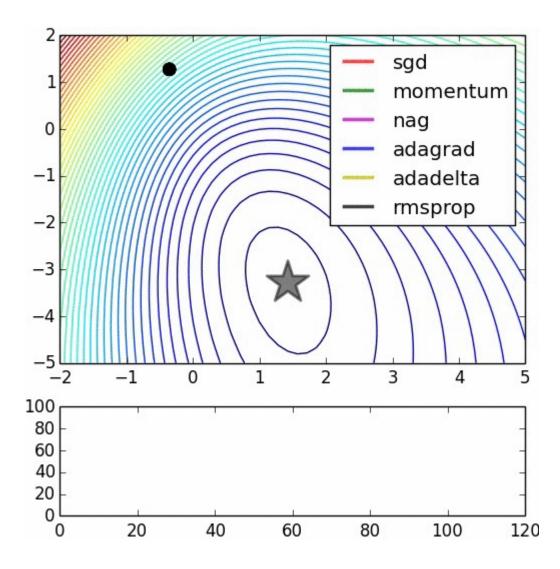
Momentum update



Nesterov momentum update



matches lower bound!



Beyond convexity

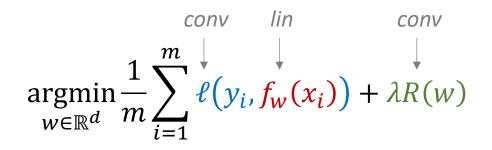
Back to modelling

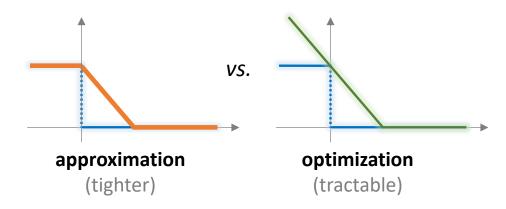
Recall:

- Really want to optimize 0/1 loss
- Instead optimize a continuous proxy
- Proxies trade off in approximation vs. optimization
- GD provides strong guarantees for *convex* objectives
- But can still be applied to non-convex objectives!
 - > non-convex losses
 - > non-convex regularizers
 - > non-convex predictive models

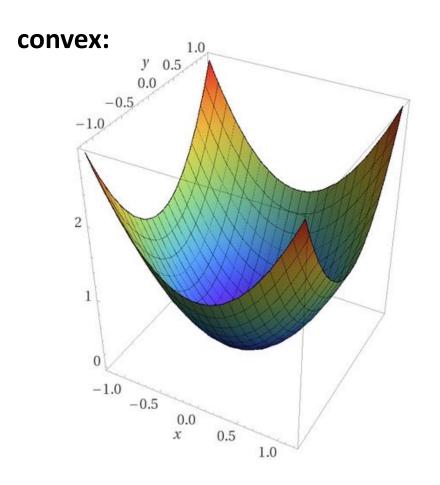
(just need differentiability)

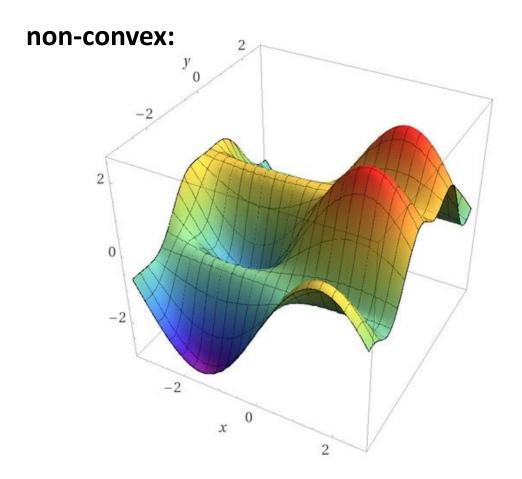
• Finds only <u>local</u> minimum, but many "tricks" for ending up at good local minimum

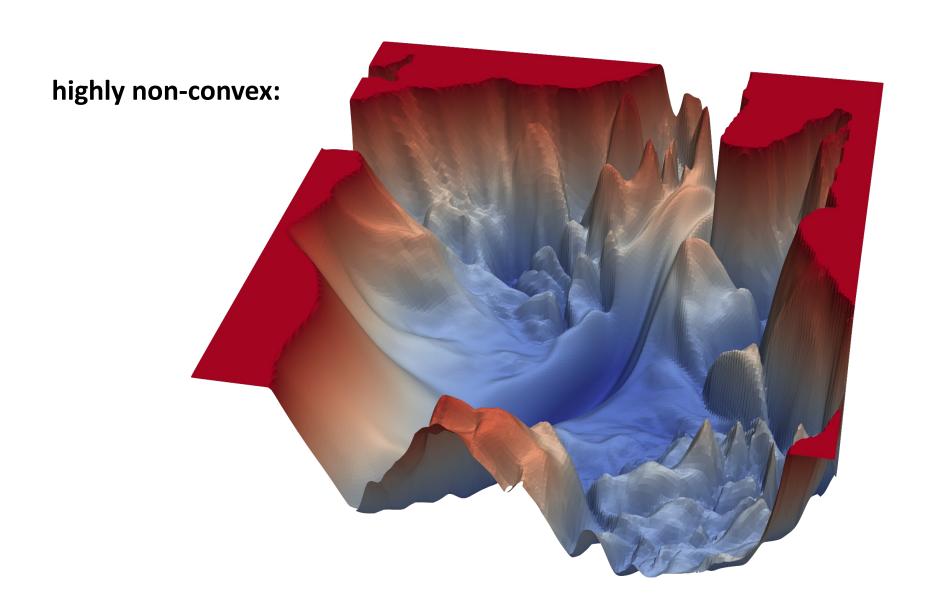


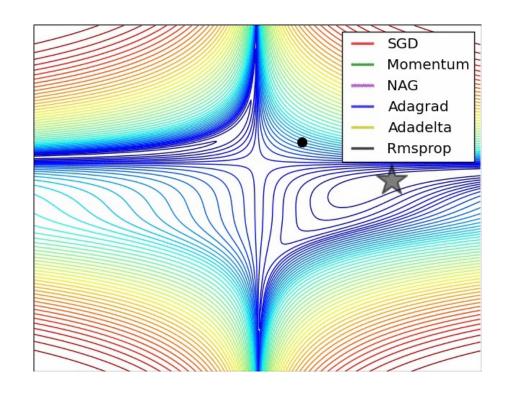


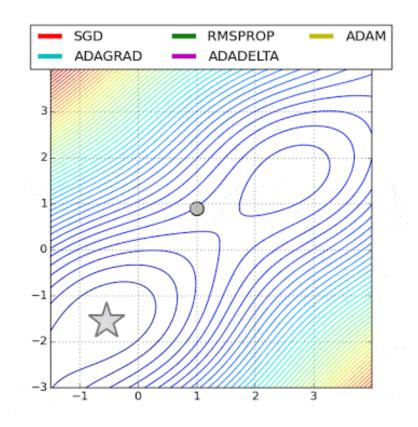
Optimization landscape



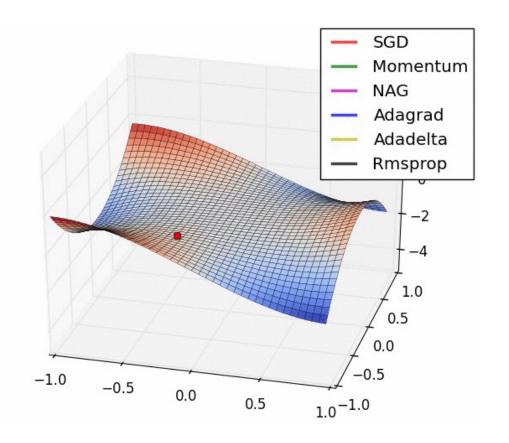


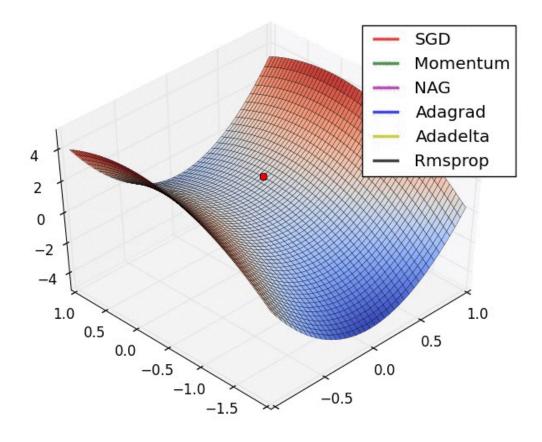






Can still apply gradient methods!





Automatic differentiation

- GD requires access to gradients
- Stone age: had to compute gradients by hand -

$$P_{k} = \frac{e^{f_{k}}}{\sum_{j} e^{f_{j}}}$$
 $L_{i} = -\sum_{k} p_{i,k} \log P_{k}$ $f_{m} = (x_{i}W)_{m}$

when
$$k = m$$
,
$$\frac{\partial P_k}{\partial f_m} = \frac{e^{f_k} \sum_j e^{f_j} - e^{f_k} \cdot e^{f_k}}{(\sum_j e^{f_j})^2} = P_k (1 - P_k)$$

when
$$k \neq m$$
, $\frac{\partial P_k}{\partial f_m} = -\frac{e^{f_k}e^{f_m}}{(\sum_j e^{f_j})^2} = -P_k P_m$

then:

$$\frac{\partial L_i}{\partial f_m} = -\sum_k p_{i,k} \frac{\partial \log P_k}{\partial f_m}$$

$$= -\sum_k p_{i,k} \frac{1}{P_k} \frac{\partial P_k}{\partial f_m}$$

$$= -\sum_{k=m} p_{i,k} \frac{1}{P_k} P_k (1 - P_k) + \sum_{k \neq m} p_{i,k} \frac{1}{P_k} P_k P_m$$

$$= \sum_{k \neq m} p_{i,k} P_m - \sum_{k=m} p_{i,k} (1 - P_k)$$

$$= \begin{cases} P_m & , & m \neq y_i \\ P_m - 1 & , & m = y_i \end{cases}$$

$$= P_m - p_{i,m}$$

Last:

$$\frac{\partial L_i}{\partial W_k} = \frac{\partial L_i}{\partial f_m} \frac{\partial f_m}{\partial W_k} = x_i^T (P_m - p_{i,m})$$

$$\nabla_{W_{k}} L = -\frac{1}{N} \sum_{i} x_{i}^{T} (p_{i,m} - P_{m}) + 2\lambda W_{k}$$

nttp://blog:/badpcnet/sz/usl995

Automatic differentiation

- GD requires access to gradients
- Stone age: had to compute gradients by hand
- Modern age: automatic differentiation (AutoDiff)

$$forward$$
 $(y, dy/dx) = foo(x)$
 $backward$

- Gradient computation completely abstracted away
- Building blocks + composition = differentiable programs
- We'll return to this when we discuss deep learning

$$P_k = \frac{e^{f_k}}{\sum_{j} e^{f_j}} \qquad L_i = -\sum_{k} p_{i,k} \log P_k \qquad f_m = (x_i W)_m$$

when
$$k = m$$
, $\frac{\partial P_k}{\partial f_m} = \frac{e^{f_k} \sum_{j} e^{f_j} - e^{f_k} \cdot e^{f_k}}{(\sum_{j} e^{f_j})^2} = P_k (1 - P_k)$

when
$$k \neq m$$
, $\frac{\partial P_k}{\partial f_m} = -\frac{e^{f_k} e^{f_m}}{(\sum_j e^{f_j})^2} = -P_k P_m$

then

$$\frac{\partial L_i}{\partial f_m} = -\sum_k p_{i,k} \frac{\partial \log P_k}{\partial f_m}$$

$$= -\sum_k p_{i,k} \frac{1}{P_k} \frac{\partial P_k}{\partial f_m}$$

$$= -\sum_{k=m} p_{i,k} \frac{1}{P_k} P_k (1 - P_k) + \sum_{k \neq m} p_{i,k} \frac{1}{P_k} P_k P_m$$

$$= \sum_{k \neq m} p_{i,k} P_m - \sum_{k=m} p_{i,k} (1 - P_k)$$

$$= \begin{cases} P_m & , & m \neq y_i \\ P_m - 1 & , & m = y_i \end{cases}$$

$$= P_m - p_i \dots$$

Last:

$$\frac{\partial L_i}{\partial W_k} = \frac{\partial L_i}{\partial f_m} \frac{\partial f_m}{\partial W_k} = x_i^T (P_m - p_{i,m})$$

$$\nabla_{W_{k}} L = -\frac{1}{N} \sum_{i} x_{i}^{T} (p_{i,m} - P_{m}) + 2\lambda W_{k}$$

Up next

- Part II: the different aspects of learning
 - 1. Statistics: generalization and PAC theory
 - 2. Modeling:
 - Error decomposition
 - Regularization
 - Model selection
 - 3. Optimization: convexity, gradient descent
 - 4. Practical aspects and potential pitfalls

Perceptron

```
input: sample set S = \{(x_i, y_i)\}_{i=1}^m
```

algorithm:

- initialize $w_0 = \vec{0}$
- for t = 1, 2, ...
 - if $\exists i \in [m]$ s.t. $y_i w_t^{\mathsf{T}} x_i \leq 0$ #wrong classification
 - $w_{t+1} = w_t + y_i x_i$
 - else
 - return w_t

