Two Use-cases of Uncertainty:
Active Learning and Bayesian Optimization

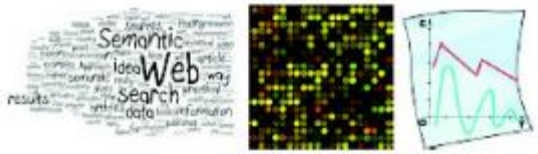
CS772A: Probabilistic Machine Learning

Piyush Rai

Active Learning

Passive Learning

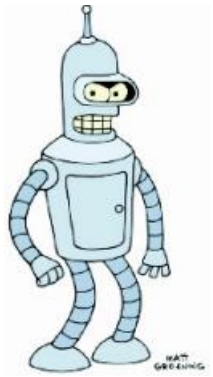
- Standard supervised learning is passive
  - Learner has no control over what labelled training examples it gets to learn from



raw unlabeled data

$x_1, x_2, x_3, \ldots$

Random Unlabeled Examples



Supervised Passive Learner

Labeled Training Examples

$(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots$

expert / oracle
analyzes experiments
to determine labels

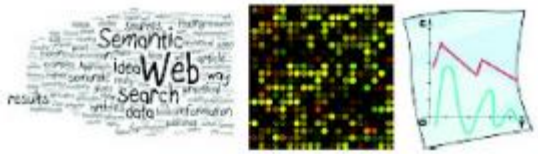
Active Learning

It is therefore also a sequential learning strategy (training data is not given all at once)

- In Active Learning, the learner can request specific labelled examples as it trains
  - In particular, examples that the learner thinks will be most useful to learn the underlying function

Will soon see what are some common notions of usefulness

Using the current model, identify the most useful example(s) from the unlabeled data pool



raw unlabeled data

$x_1, x_2, x_3, \ldots$

Although one example in each iteration is more common, labels of one or more than one examples can be queried ("batch" active learning")

Assumes some small amount of initial labelled training examples $\mathcal{D} = \{(x_n, y_n)\}_{n=1}^{N}$ are available to learn an initial model

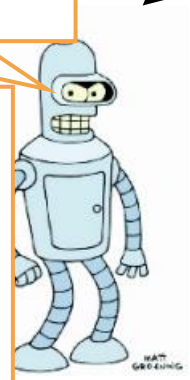
Query the expert for the true label of the selected unlabeled example, say x_1

$\langle x_1, ? \rangle$

$\langle x_1, y_1 \rangle$

$\langle x_2, ? \rangle$

$\langle x_2, y_2 \rangle$



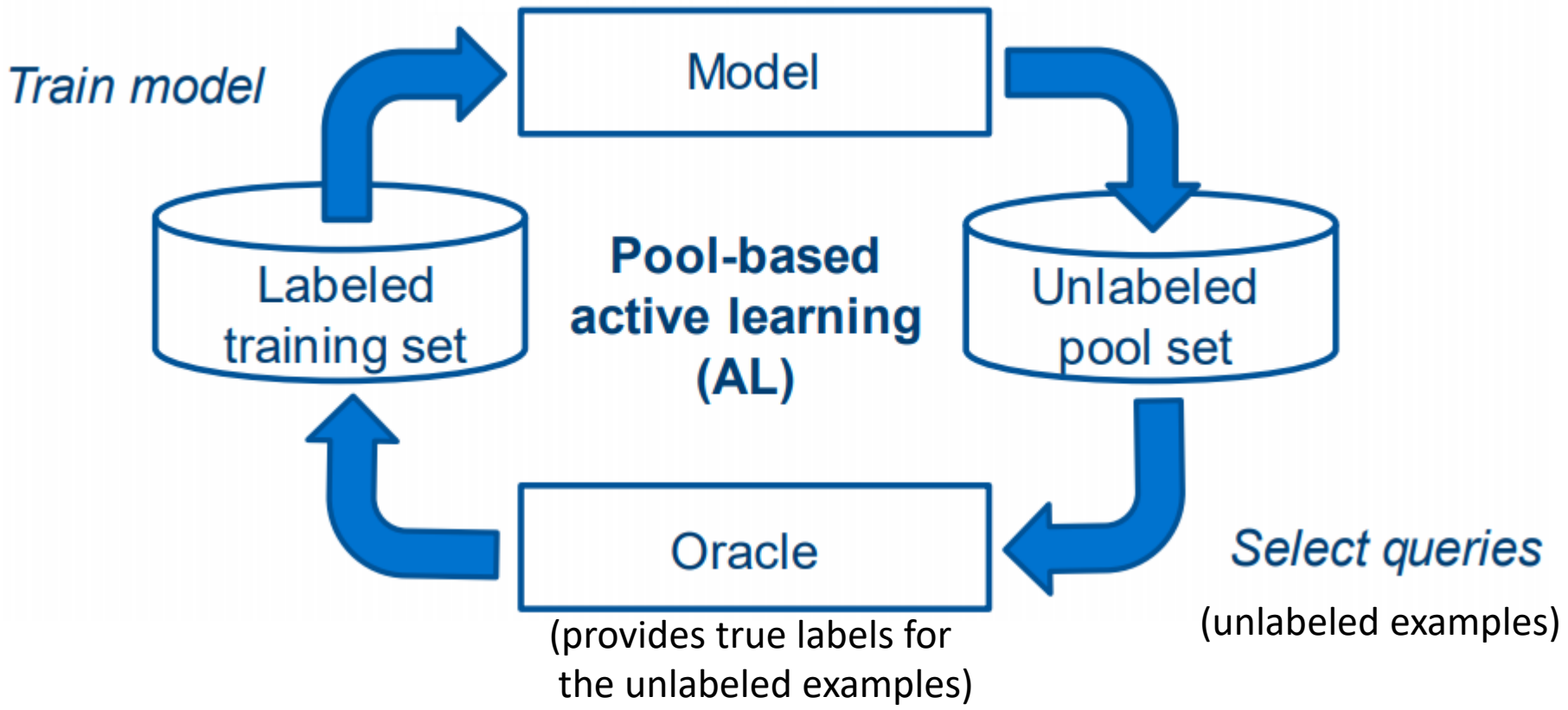
expert / oracle
analyzes experiments
to determine labels

The new labelled examples acquired "actively" are used to improve the initial model by retraining it using the updated training data $\mathcal{D} = \{\mathcal{D} \cup (x_*, y_*)\}$ and repeating the process until we get the desired accuracy or our budget exhausts

Supervised Active Learner

Active Learning

- The figure below is another illustration of AL



Measuring Usefulness in AL

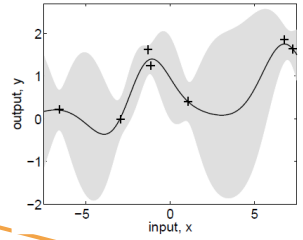
Given the acquisition function, the most useful example can be selected from the pool as

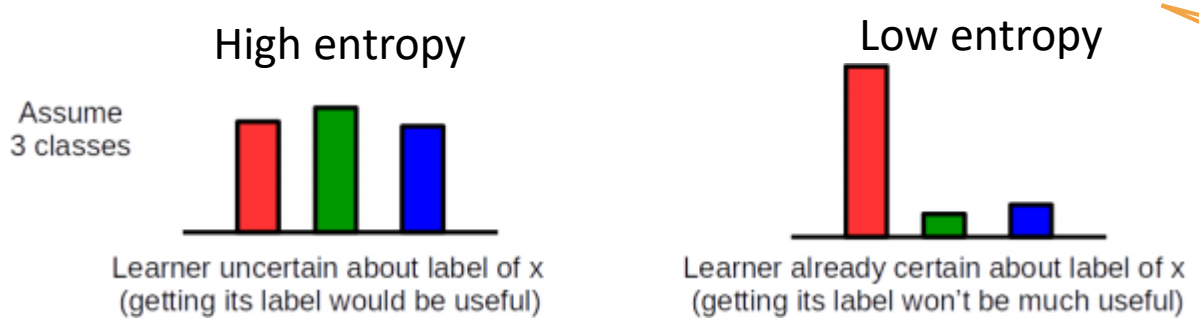
$\hat{\boldsymbol{x}}_* = \text{argmax}_{x_* \in \mathcal{X}_{pool}} A(\boldsymbol{x}_* | p(\theta|\mathcal{D}))$

Note: We will use shorthand $A(\boldsymbol{x}_*)$

- Various ways to measure the usefulness of an unlabeled example $\boldsymbol{x}_*$
  - Defined by an "acquisition function" $A(\boldsymbol{x}_*)$ (high value for most useful unlabeled examples)

- Approach 1: For $\boldsymbol{x}_*$, look at uncertainty in output $\boldsymbol{y}_*$ predicted by the current model
  - Can use variance in the posterior predictive distribution: $A(\boldsymbol{x}_*) = \text{var}(y_*)$
  - More generally, can use entropy of the PPD: $A(\boldsymbol{x}_*) = \mathbb{H}[p(y_*|\boldsymbol{x}_*, \mathcal{D})]$





Note that this is the "marginal entropy" of the output distribution since the posterior predictive of the output is obtained by marginalizing over the posterior

- Approach 2: Look at how much our model will improve if we add this unlabeled example with its true label, to our training set, and retrain the model

Mutual Information

$$A(x_*) = \mathbb{H}[p(\theta|\mathcal{D})] - \mathbb{E}_{p(y_*|x_*,\mathcal{D})}\mathbb{H}[p(\theta|\mathcal{D} \cup (\boldsymbol{x}_*, y_*))] = \mathbb{I}[\theta; y_*|\mathcal{D}, \boldsymbol{x}_*]$$

Entropy of the current posterior

Need to use expectation here since y_* is not known

Entropy of the new posterior after including the new example in our training set

Batch Active Learning

- Approaches we saw work by querying and adding one example at a time
- Expensive in practice since we have to retrain every time after including a new example
  - Especially true for deep learning models which are computationally expensive to train
- In practice, we want to use AL to jointly query the labels of $B > 1$ examples

$$(\hat{\boldsymbol{x}}_1, \hat{\boldsymbol{x}}_2, \ldots, \hat{\boldsymbol{x}}_B) = \text{argmax}_{(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_B) \in \mathcal{X}_{pool}} A\left(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_B | p(\theta|\mathcal{D})\right)$$

- Difficult to construct such joint acquisition function and maximize them
- A greedy scheme is to simply select the B highest scoring points

$$A\left(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_B | p(\theta|\mathcal{D})\right) = \sum_{b=1}^{B} \mathbb{I}[\theta;\ y_b | \mathcal{D}, \boldsymbol{x}_b]$$

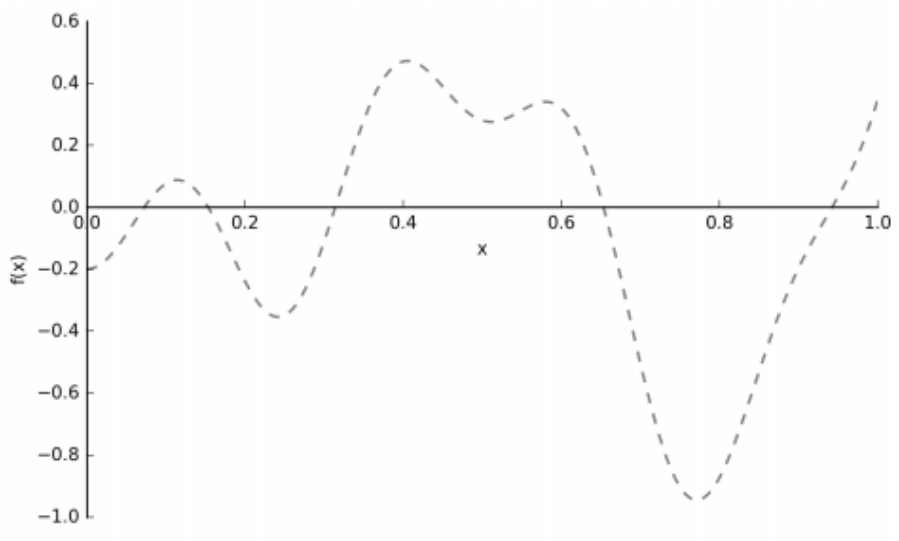
- The above however is myopic and ignores correlations among the selected points
  - Some recent works have addresses this issue[1]

[1] BatchBALD: Efficient and Diverse Batch Acquisition for Deep Bayesian Active Learning (Kirsch et al, NeurIPS 2019)

Bayesian Optimization

Bayesian Optimization: The Basic Formulation

- Consider finding the optima x_* (say minima) of a function $f(x)$



- Caveat: We don't know the form of the function; can't get its gradient, Hessian, etc

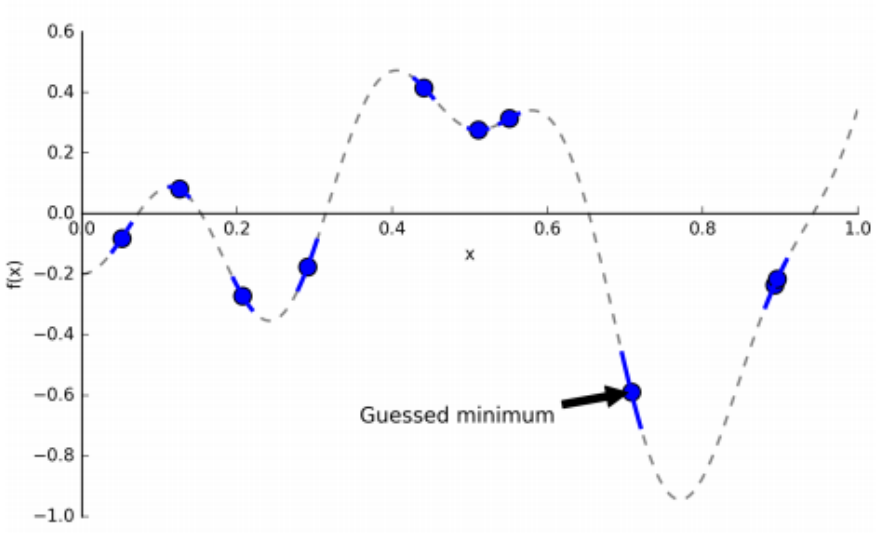
- Can only query the function's values at certain points (i.e., only "black-box" access)
  - The values may or may not be noisy (i.e., we may be given $f(x)$ or $f(x) + \epsilon$)

Bayesian Optimization: Some Applications

- Drug Design: Want to find the optimal chemical composition for a drug
  - Optimal composition will be the one that has the best efficacy
  - But we don't know the efficacy function
  - Can only know the efficacy via doing clinical trials
  - Each trial is expensive; can't do too many trials
- Hyperparameter Optimization: Want to find the optimal hyperparameters for a model
  - Optimal hyperparam values will be those that give the lowest test error
  - Don't know the true "test error" function
  - Need to train the model each time with different h.p. values and compute test error
  - Training every time will be expensive (e.g., for deep nets)
  - Note: Hyperparams here can even refer to the structure of a deep net (depth, width, etc)
- Many other applications: Website design via A/B testing, material design, optimizing physics based models (e.g., aircraft design), etc

Bayesian Optimization

- Can use BO to find maxima or minima
- Would like to locate the optima by querying the function's values (say, from an oracle)



Assuming the goal is to find the minima

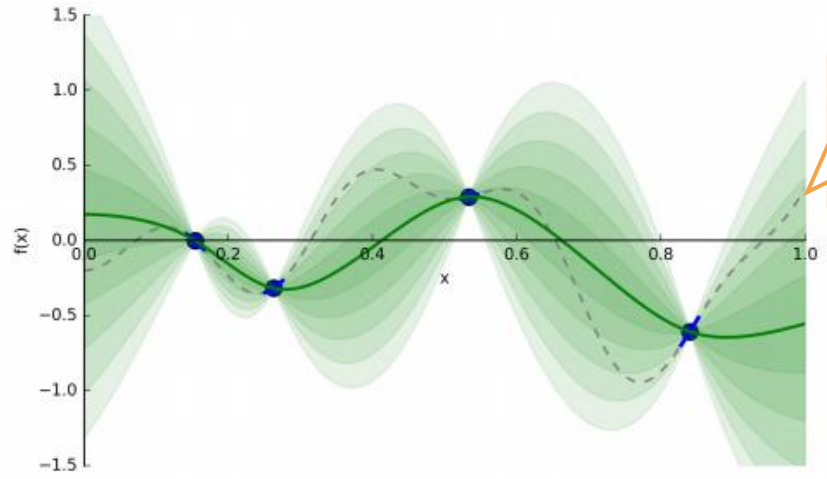
- We would like to do so using as few queries as possible
- Reason: The function's evaluation may be time-consuming or costly

Bayesian Optimization

Note: Function values can be noisy too, e.g., $f(x_n) + \epsilon_n$

- Suppose we are allowed to make the queries sequentially
- This information will be available to us in form of query-function value pairs $\{(x_n, f(x_n))\}_{n=1}^{N}$
- Queries so far can help us estimate the function

By solving a regression problem



Dotted curve: True function
Green curve: Current estimate ("surrogate") of the function
Shaded region: Uncertainty in the function's estimate

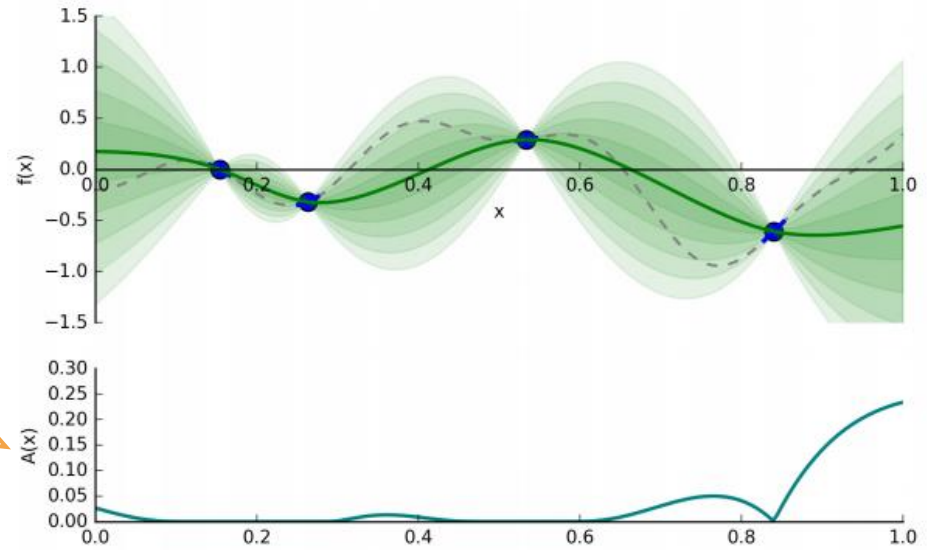
- BO uses past queries + function's estimate+uncertainty to decide where to query next
- Similar to Active Learning but the goal is to learn f as well as finds its optima

Bayesian Optimization

Note: Function values can be noisy too, e.g., $f(x_n) + \epsilon_n$

- BO requires two ingredients
  - A regression model to learn a surrogate of $f(x)$ given previous queries $\{(x_n, f(x_n))\}_{n=1}^{N}$
  - An acquisition function $A(x)$ to tell us where to query next

Assumption: $A(x)$ should be easier to optimize than $f(x)$



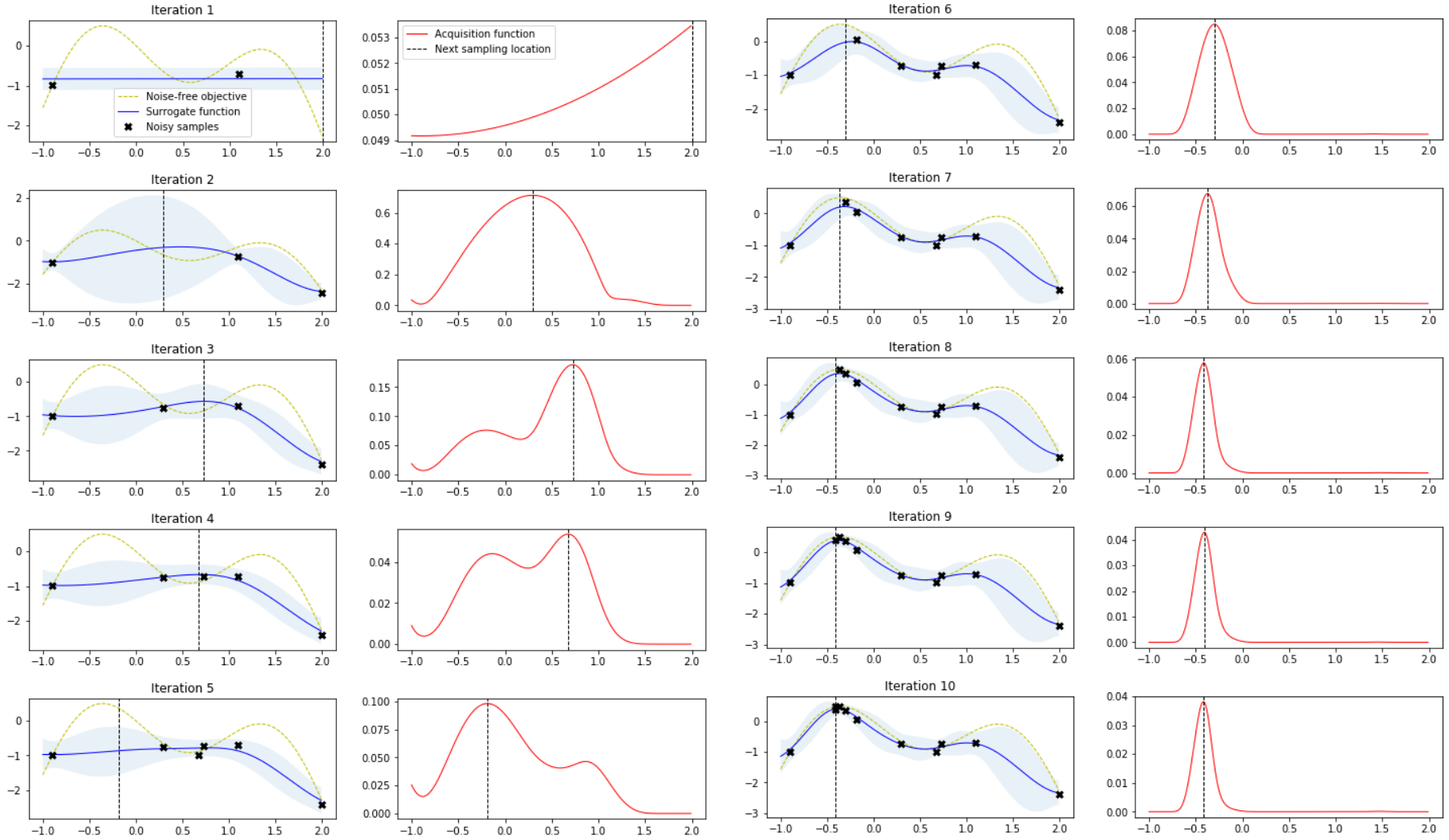
Dotted curve: True function
Green curve: Current surrogate of the function
Shaded region: Uncertainty in the function's estimate

A typical example of what $A(x)$ might look like, assuming that the goal is to find the maxima of $f(x)$

- Note: The regression model must also have estimate of function's uncertainty
  - Bayesian nonlinear regression, such as GP, Bayesian Neural network, etc would be ideal

Bayesian Optimization: An Illustration

- Suppose our goal is to find the maxima of $f(x)$ using BO



Pic source: http://krasserm.github.io/2018/03/21/bayesian-optimization/

Some Basic Acquisition Functions for BO

(assuming we are finding the minima)

Acquisition Functions: Probability of Improvement

- Assume past queries $\mathcal{D}_N = (\boldsymbol{X}, \boldsymbol{f}) = \left(x_n, f(x_n)\right)_{n=1}^{N}$ and suppose $f_{min} = \min \boldsymbol{f}$
- Suppose f_{new} denotes the function's value at the next query point x_{new}
- We have an <u>improvement</u> if $f_{new} < f_{min}$ (recall we are doing minimization)
- Assuming the function is real-valued, suppose the posterior predictive for x_{new} is

$$p(f_{new}|x_{new}, \mathcal{D}_N) = \mathcal{N}(f_{new}|\mu(x_{new}), \sigma^2(x_{new}))$$

- We can define a probability of improvement based acquisition function

$$A_{PI}(x_{new}) = p(f_{new} \leq f_{min}) = \int_{-\infty}^{f_{min}} \mathcal{N}(f_{new}|\mu(x_{new}), \sigma^2(x_{new}))df_{new} = \Phi\left(\frac{f_{min} - \mu(x_{new})}{\sigma(x_{new})}\right)$$

Exercise: Verify

$\Phi()$ denotes CDF of $\mathcal{N}(0,1)$

- The optimal query point will be one that maximizes $A_{PI}(x_{new})$

$$x_* = \text{argmax}_{x_{new}} A_{PI}(x_{new})$$

Acquisition Functions: Expected Improvement

- PI doesn't take into account the amount of improvement
- Expected Improvement (EI) takes this into account and is defined as

$$A_{EI}(x_{new}) = \mathbb{E}[f_{min} - f_{new}] = \int_{-\infty}^{f_{min}} (f_{min} - f_{new}) \mathcal{N}(f_{new} | \mu(x_{new}), \sigma^2(x_{new})) d f_{new}$$

Exercise: Prove this result

$$= (f_{min} - \mu(x_{new})) \Phi\left(\frac{f_{min} - \mu(x_{new})}{\sigma(x_{new})}\right) + \sigma(x_{new}) \mathcal{N}\left(\frac{f_{min} - \mu(x_{new})}{\sigma(x_{new})}; 0,1\right)$$

- The optimal query point will be one that maximizes $A_{EI}(x_{new})$

$$x_* = \text{argmax}_{x_{new}} A_{EI}(x_{new})$$

Focus on points where the function has small values (since we are looking for its minima)

Focus on points where the function has high uncertainty (so that including them improves our estimate of the function)

- Note that the above acquisition function trades off exploitation vs exploration
  - Will prefer points with small predictive mean $\mu(x_{new})$: Exploitation
  - Will prefer points with large predictive variance $\sigma(x_{new})$: Exploration

Acquisition Functions: Lower Confidence Bound

- Lower Confidence Bound (LCB) also takes into account exploitation vs exploration
- Used when the regression model is a Gaussian Process (GP)
- Assume the posterior predictive for a new point to be

$$p(f_{new}|x_{new}, \mathcal{D}_N) = \mathcal{N}(f_{new}|\mu(x_{new}), \sigma^2(x_{new}))$$

- The LCB based acquisition function is defined as

$$A_{LCB}(x_{new}) = \mu(x_{new}) - \kappa\, \sigma(x_{new})$$

- Point with the smallest LCB is selected as the next query point

$$x_* = \text{argmin}_{x_{new}} A_{LCB}(x_{new})$$

- κ is a parameter to trade-off exploitation (low mean) and exploration (high variance)
- Under certain conditions, the iterative application of this acquisition function will converge to the true global optima of f (Srinivas et al. 2010)

When using BO for maximization, we use Upper Confidence Bound (UCB) defined as $A_{UCB}(x_{new}) = \mu(x_{new}) + \kappa\, \sigma(x_{new})$ and $x_* = \text{argmax}_{x_{new}} A_{UCB}(x_{new})$

Thus prefer points at which the function has low mean but high variance

Bayesian Optimization: The Overall Algo

- Initialize $\mathcal{D} = \{\}$
- For $n = 1,2, \ldots, N$ (or until the budget doesn't exhaust)
  - Select the next query point x_n by optimizing the acquisition function

$$x_n = \text{argopt}_x \, A(x)$$

  - Get function's value from the black-box oracle: $f_n = f(x_n)$
  - $\mathcal{D} = \{\mathcal{D} \cup (x_n, f_n)\}$

Can get the function's minima from this set of function's values

  - Update the regression model for f using data $\mathcal{D}$

BO: Some Challenges/Open Problems

- Learning the regression model for the function
  - GPs are flexible but can be expensive as N grows
  - Bayesian neural networks can be a more efficient alternative to GPs (Snoek et al, 2015)
  - Hyperparams of the regression model itself (e.g., GP cov. function, Bayesian NN hyperparam)

- High-dimensional Bayesian Optimization (optimizing functions of many variables)
  - Most existing methods work well only for a moderate-dimensional x
  - Number of function evaluations required would be quite large in high dimensions
  - Lot of recent work on this (e.g., based on dimensionality reduction)

- Multitask Bayesian Optimization (joint BO for several related functions)
  - Basic idea: If two functions are similar their optima would also be nearby