Deep Networks as *hidden* Metric Learners

- N training instances: $x_1, \ldots, x_n, \ldots, x_N$

- Ground truth training labels: $y_1, \ldots, y_n, \ldots, y_N$

- Seek a function, $f : \mathbb{X} \rightarrow \mathbb{Y}$, to predict $\hat{y}_{N+1}$ for a new, unseen instance x_{N+1}, with minimal *distance* between $\hat{y}_{N+1}$ and y_{N+1}

- New view: Back-out a metric learner from the parametric deep network:
$f = c \circ g$, where $g : \mathbb{X} \rightarrow \mathbb{R}^M$, $c : \mathbb{R}^M \rightarrow \mathbb{Y}$, and $r \in \mathbb{R}^M$ is a dense representation of the input under the parametric model

- Sense in which: $f\left(x_{N+1}\right) \approx \sum_{n=1}^{N} y_n \cdot \alpha_n \cdot k\left(||r_n - r_{N+1}||_2\right)$

I.e., a test prediction is approx. a distance-weighting (between "***exemplar***" representations) over the training set

- Enables interpretable/introspectable decision rules & various analyses (hence, "***auditing***"): E.g., only admit true positive (TP) matches:
$\hat{y}_{N+1} = f(x_{N+1}) \cdot \left[f(x_{N+1}) = f(x_n) \wedge f(x_n) = y_n\right] + NULL \cdot \left[f(x_{N+1}) \neq f(x_n) \vee f(x_n) \neq y_n\right]$, where $n = \underset{n \in \{1,\ldots,N\}}{\arg\min} ||r_n - r_{N+1}||_2$

We use such training set matching as a post-processing mask (with decision rules) over $f\left(x_{N+i}\right)$, but in principle, with the model presented here, we could directly train against this (via the similarity loss)

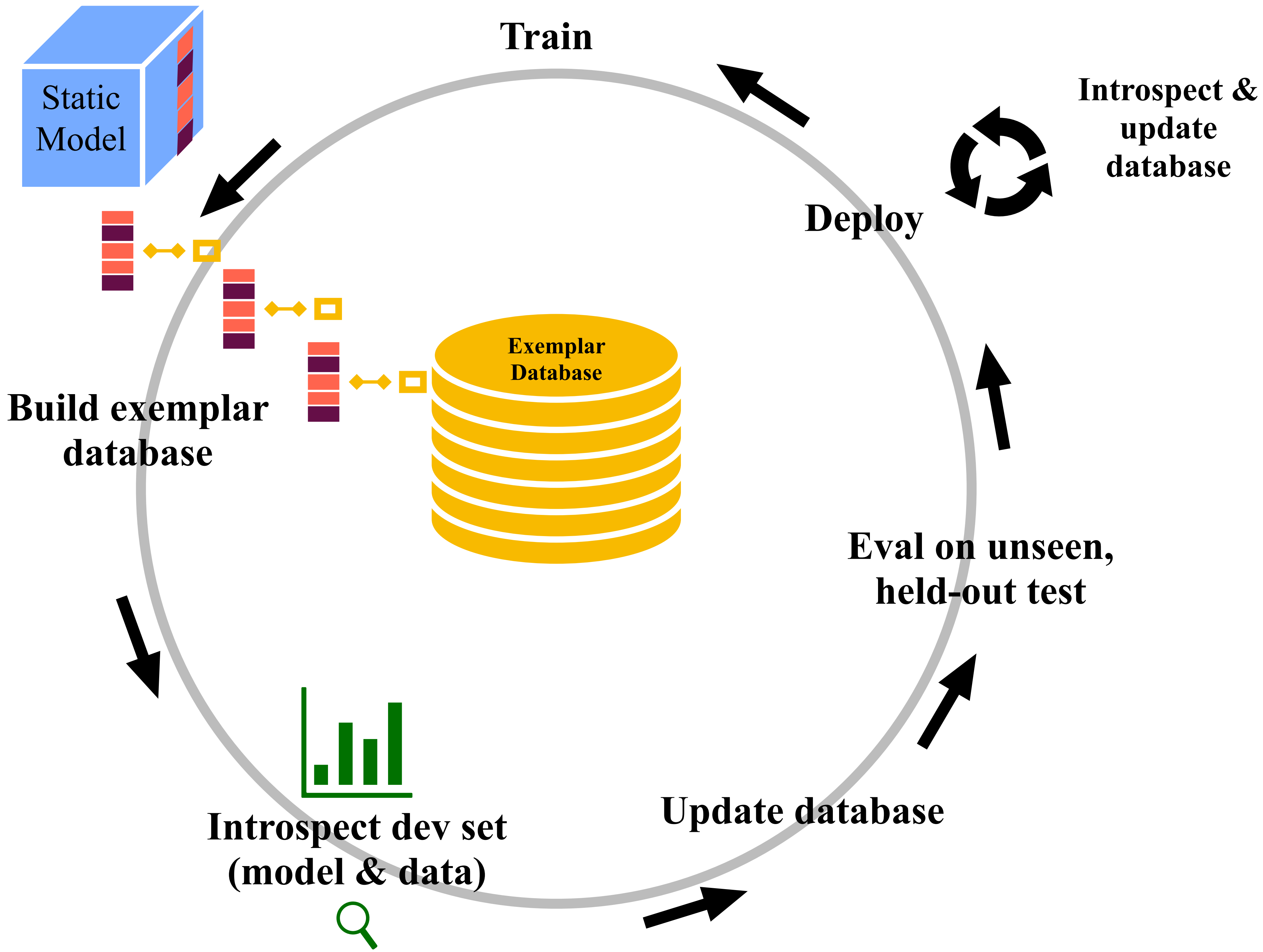
- Enables updatability/adaptability:

    - Label changes: $y'_n = y_n + \Delta_n$

    - Data additions (a.k.a., continual/lifelong learning):
    $\mathbb{D}^N = \left\{(x_1, y_1), \ldots, (x_N, y_N)\right\}$ becomes $\mathbb{D}^{N'} = \left\{(x_1, y_1), \ldots, (x_N, y_N), \ldots, (x_{N'}, y_{N'})\right\}$

    - New lightweight models over representations (e.g., using data additions): $c' : \mathbb{R}^M \rightarrow \mathbb{Y}'$

Exemplar Auditing Lifecycle

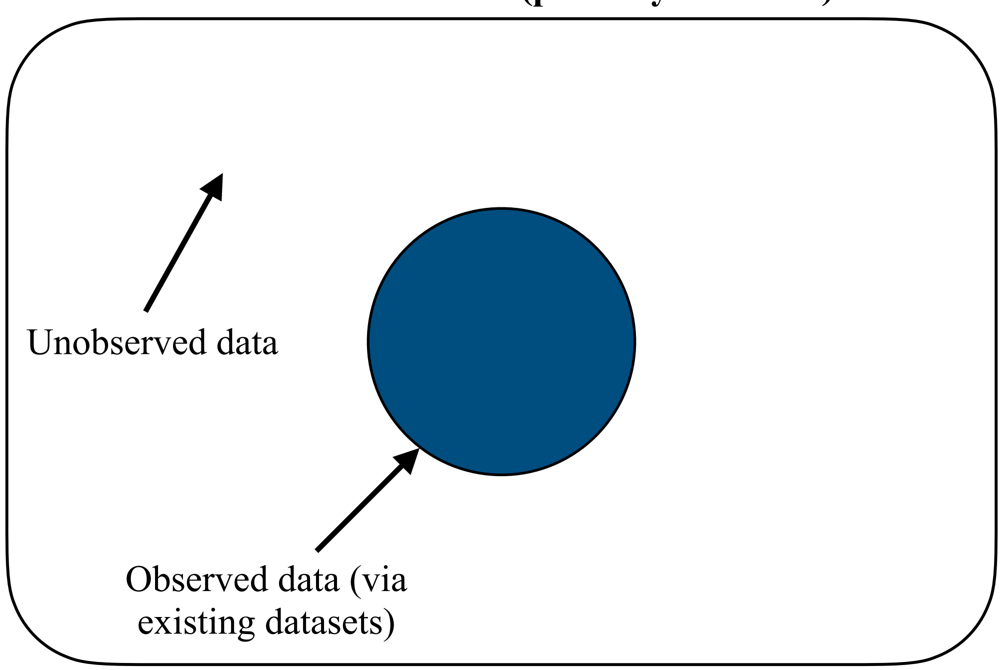


Allen Schmaltz

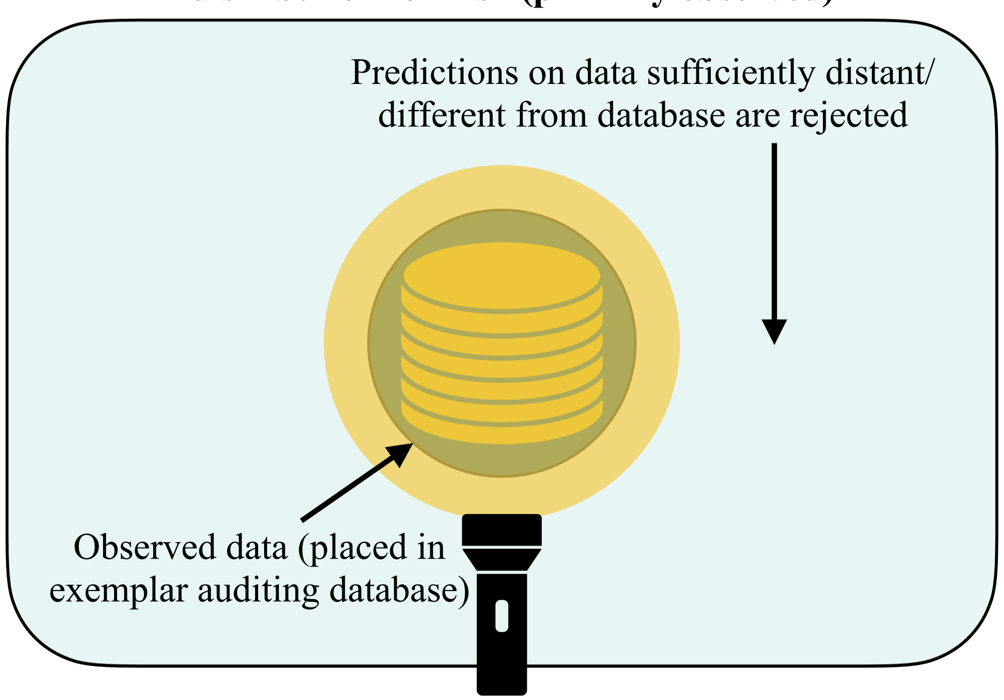
Out-of-Domain Settings

- Pre-train with as much data as possible
- Add as much data as possible to the database, including data not seen in training
  - Corral the in-domain space, around the ball of the observed data
  - Never predict over out-of-domain data in high-risk settings. Instead: Rearrange the deployment to handle non-admitted predictions.

Data distribution for task (partially observed)



Data distribution for task (partially observed)



Memory Matching Model

- Approach (*high-level*): Run the same shared network, g, over all of Wikipedia, $\mathbb{D}$, caching the representations, & then perform search by matching the query representation with progressively built-up support sequences

q = **Query sequence**

s = **Support sequence**

A Wikipedia sentence

Search Level 1 $g\left(q\right) = r_q \in \mathbb{R}^M$

$$g\left(s_1\right) = r_{s_1} \in \mathbb{R}^M$$

$$\vdots$$

$$g\left(s_{|\mathbb{D}|}\right) = r_{s_{|\mathbb{D}|}} \in \mathbb{R}^M$$

$r_{s_1}, \ldots, r_{s_{|\mathbb{D}|}}$ can be cached

$$s_i \in \mathbb{D}$$

Set of K nearest Wikipedia sentences

$$s'_k \in \arg K \min_{s_i} || r_q - r_{s_i} ||_2$$

Search Level 2 r_q

$$g\left((q, s'_1)\right) = r_{(q,s'_1)} \in \mathbb{R}^M$$

$$\vdots$$

$$g\left((q, s'_K)\right) = r_{(q,s'_K)} \in \mathbb{R}^M$$

Set of Z nearest Wikipedia sentences from Search Level 2

$$s''_z \in \arg Z \min_{s'_k} || r_q - r_{(q,s'_k)} ||_2$$

Search Level 3

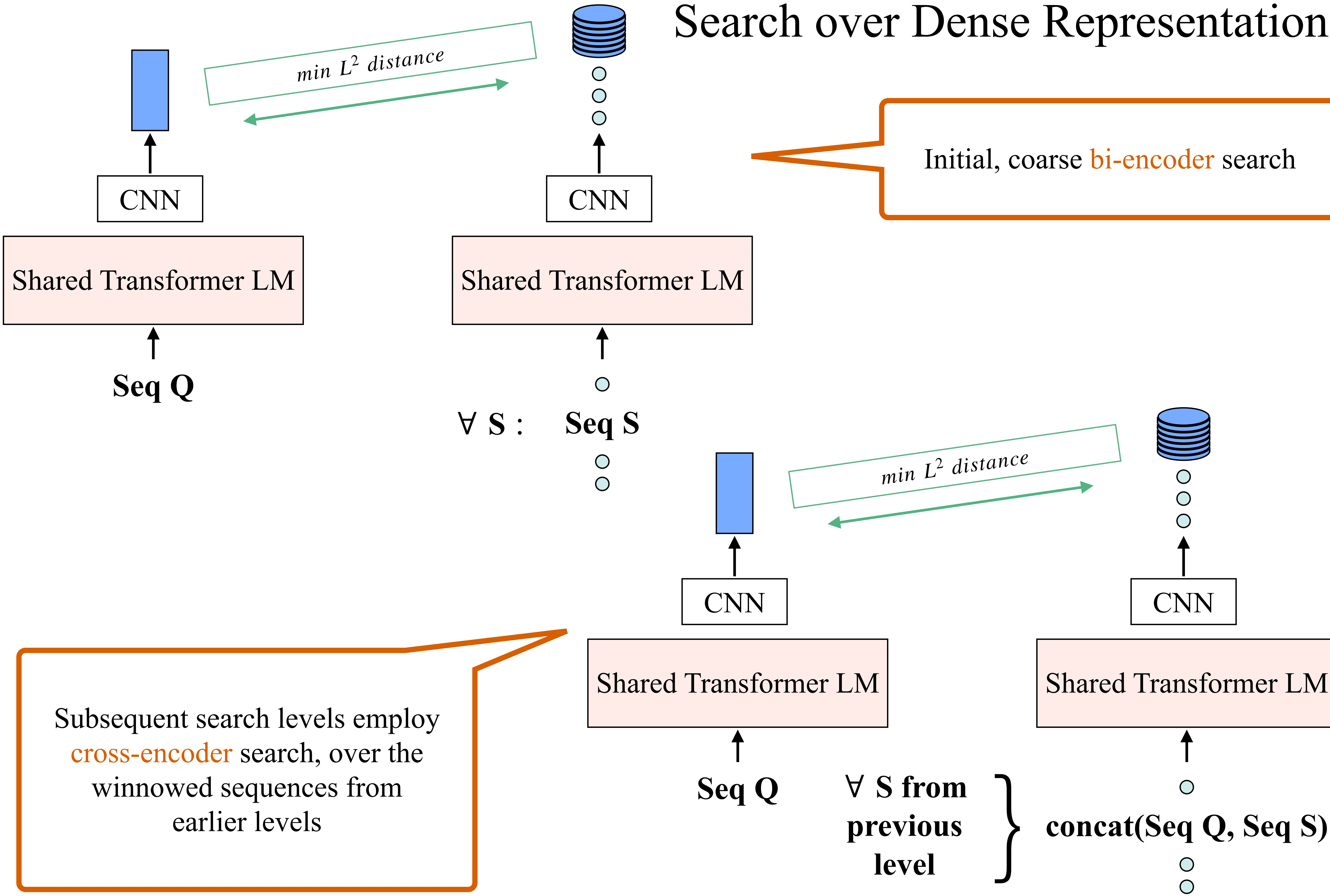
$$\hat{y} = \arg\min_{y \in \{\text{Supports, Refutes, Unverifiable}\}} || r_q - r_{(y,q,s''_1,\ldots,s''_Z)} ||_2$$

$\hat{y}$ is the label prediction

$\{s''_1, \ldots, s''_Z\}$ is the set of Wikipedia support sentences

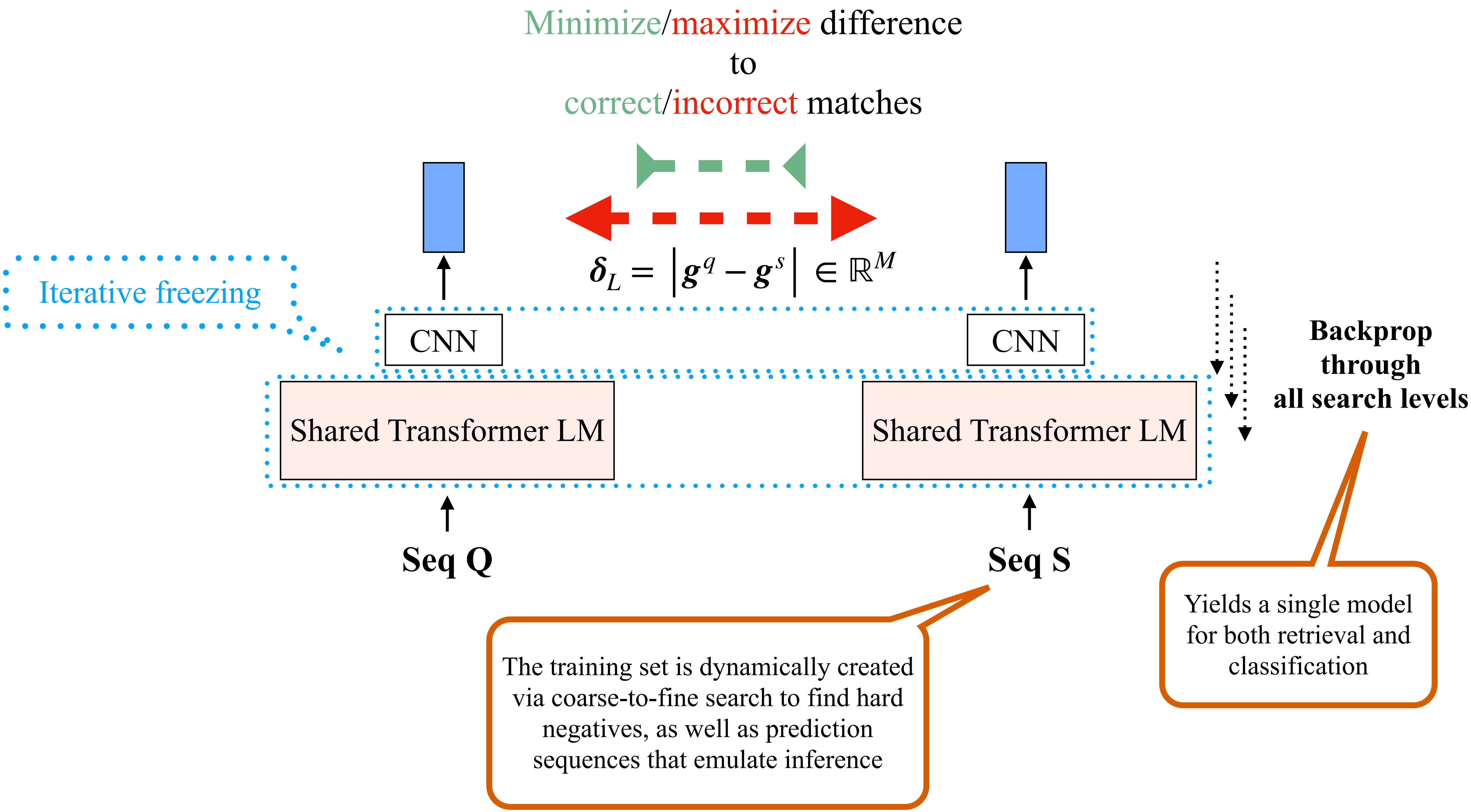
Allen Schmaltz

An End-to-End Retrieval-Classification Model via a Coarse-to-Fine Search over Dense Representations



Allen Schmaltz

Joint Retrieval and Classification Training



Multi-Sequence Representation Composition for Exemplar Auditing