Practice Questions for CS 181, Midterm 2 (Spring 2022)

Finale Doshi-Velez
Harvard College

April 19, 2022

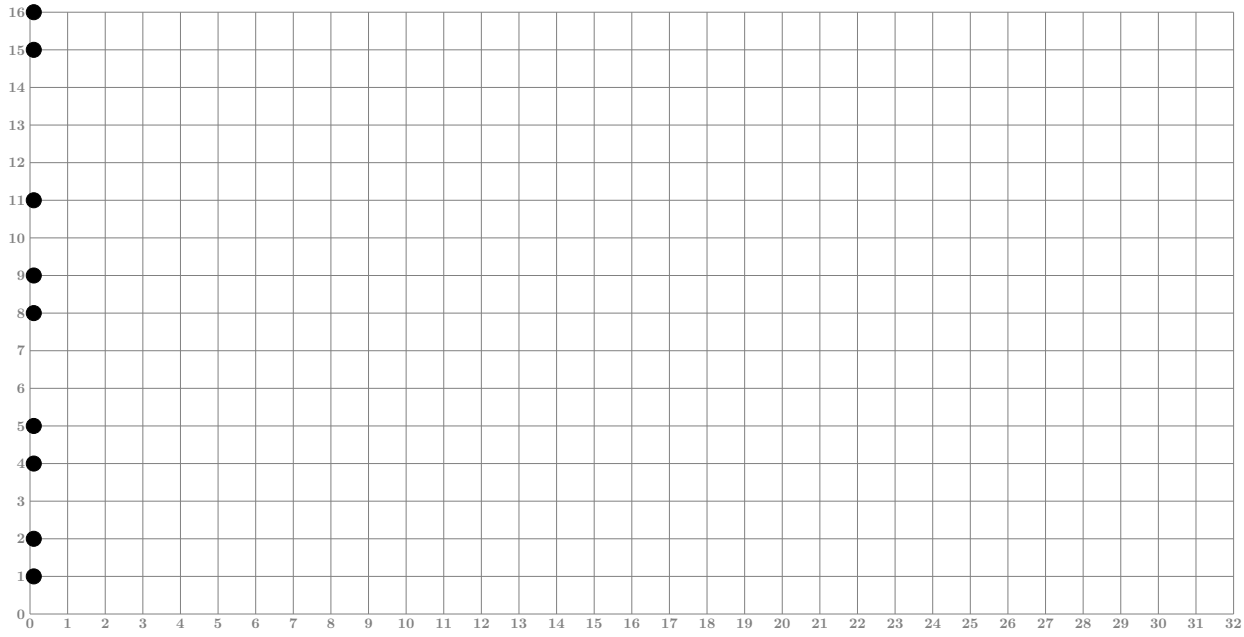
These practice questions are illustrative of the kinds of understanding that you should expect to be tested on the midterm. If anything they are slightly more difficult than the questions on the exam. You can expect around 5 questions on the midterm and you will have 75 minutes. This means that a typical question should take 15 minutes. But some will be shorter, some longer and say 10 mins vs 20 min questions. We've provide rough guidance here ("short"), ("typical") and ("long").

1. **Hierarchical Agglomerative Clustering** [Short]

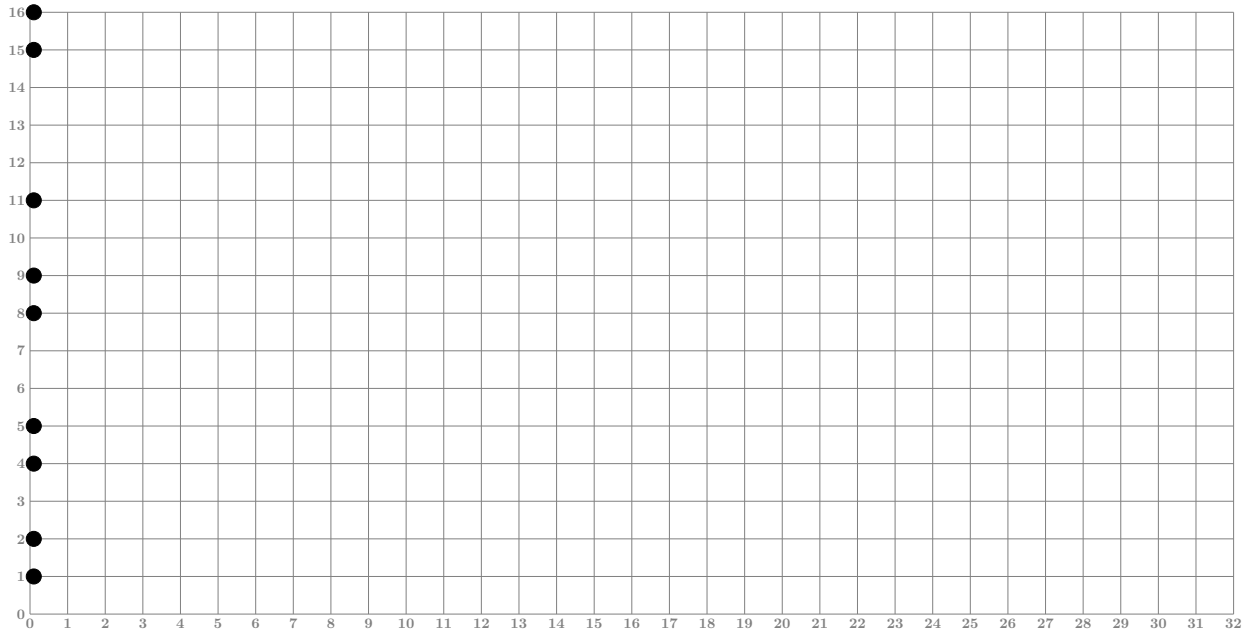
Consider nine points $x_1, \ldots, x_9$ shown below, where the y-axis provides their values. We define $d(x, x') = |x - x'|$, and consider two different cluster distances.

Draw the dendrogram for the data. Join together clusters one per step (on the horizontal-axis), breaking ties towards joining lower x values first. In the top figure, use the min-linkage distance and in the bottom figure use the max-linkage distance.

(a) Min Linkage:

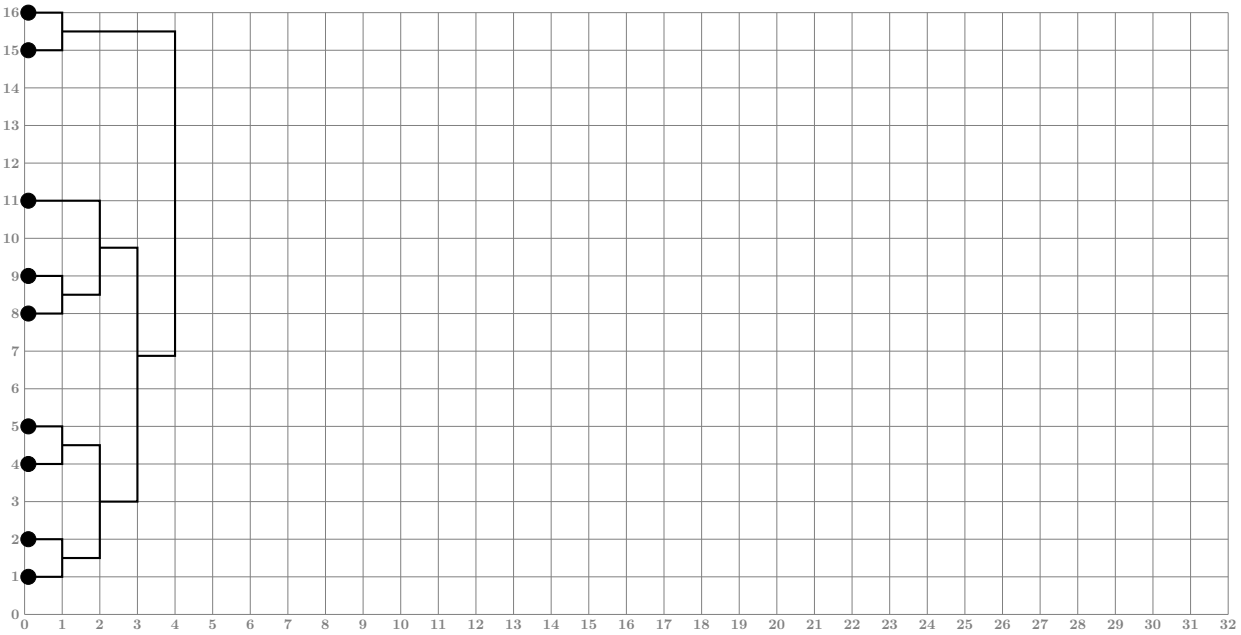


(b) Max Linkage:

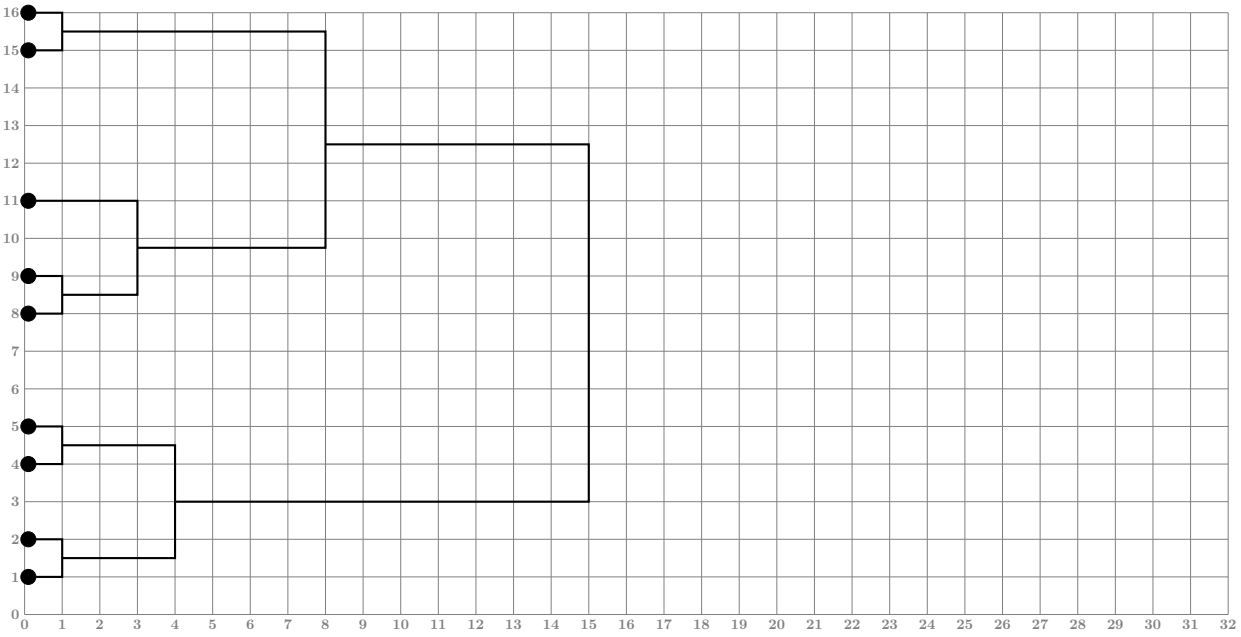


Solution:

(a) Min Linkage:

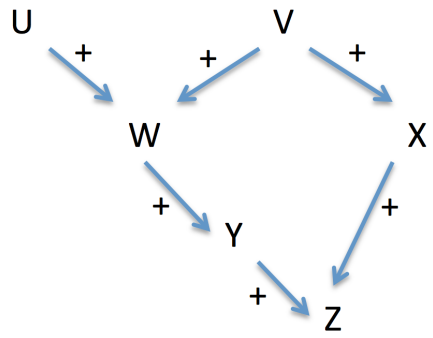


(b) Max Linkage:



2. **Bayesian networks** [Typical]

Consider the following Bayesian network, where the variables are all Boolean.



The '+' annotations indicate the direction of the local effect; e.g., the '+' from U to W means that for each value v of V,

$$p(W = true \,|\, U = true, V = v) > p(W = true \,|\, U = false, V = v).$$

For each of the following questions, select one of the following, and also state which (if any) undirected paths are blocked (in the sense of d-separation):

$=$ if the two probabilities are necessarily equal;
$<$ if the first probability is necessarily smaller;
$>$ if the first probability is necessarily larger;
? if none of these cases hold.

(a) $p(V = true \mid Y = false)$ $p(V = true \mid Y = true)$

(b) $p(V = true \mid Z = false)$ $p(V = true \mid Z = true)$

(c) $p(U = true \mid W = true, Y = false)$ $p(U = true \mid W = true, Y = true)$

(d) $p(Y = true \mid Z = true, X = false)$ $p(Y = true \mid Z = true, X = true)$

(e) $p(U = true \mid Y = true, Z = false)$ $p(U = true \mid Y = true, Z = true)$

Solution.

[We give more explanation here than you would expected to give!]

(a) $p(V = true \mid Y = false) \ < \ p(V = true \mid Y = true)$

First, let's ask whether $V \perp Y$, i.e., are V and Y independent?

Path VWY is not blocked, path $VXZY$ is blocked at Z (converging arrow). So, V is not independent of Y.

Considering the unblocked path, since the $V - W$ effect is positive and the $W - Y$ effect is positive, then we have Y being true makes V more likely to be true. Notice that this positive correlation goes in both directions, e.g., if V is positively correlated with W, then W is positively correlated with V. For this reason, we conclude "<".

(b) $p(V = true \mid Z = false) \ < \ p(V = true \mid Z = true)$

First let's ask whether $V \perp Z$? Neither paths V-W-Y-Z or V-X-Z are blocked, so these are not independent.

Now, the effect on each of the paths is positive, for the same reason as the positive correlation argument in in part (a). Since both effects go in the same direction we can answer affirmatively with a "<" inequality.

(c) $p(U = true \mid W = true, Y = false) \ = \ p(U = true \mid W = true, Y = true)$

Now we have W in the evidence. The relevant independent question is $U \perp Y \mid W = True$, i.e., are U and Y conditionally independent, given this evidence W?

There are two paths to check. Path $U - W - Y$ is blocked at W, and path $U - W - V - X - Z - Y$ is blocked at Z (converging arrow, no evidence). Note the second path is no longer blocked at W because there's a converging arrow on this path. But it is any way blocked, because Z is not in the evidence.

Since both paths are blocked, then U and Y are conditionally independent given $W = True$, and we have "=" as the answer.

(d) $p(Y = true \mid Z = true, X = false)$? $p(Y = true \mid Z = true, X = true)$

Now Z in evidence. We're interested in understanding $Y \perp X \mid Z = True$.

Path $YWVX$ is not blocked. In addition, $Y - Z - X$ is not blocked (converging arrows at Z, and we know Z).

There are two paths for information to flow between Y and X. On the first path $YWVX$ this is a positive effect for the reasons as the positive correlation argument in part (a). But on the second path YZX this is a negative effect because we have "explaining away" through Z. That is, knowing X is true reduces the probability that Y is true since it explains Z being true and means that it's less likely we also have the other possible reason of Y being true.

Because the effects go in different directions, the answer is "?".

(e) $p(U = true \mid Y = true, Z = false) \ > \ p(U = true \mid Y = true, Z = true)$

Now Y is in the evidence.

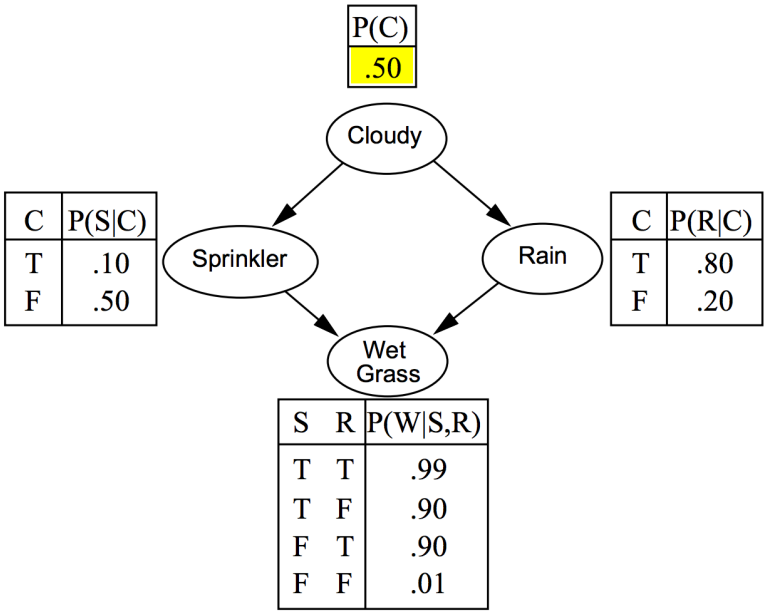
We're interested in understanding $U \perp Z \mid Y$. In this case path $U - W - Y - Z$ is blocked at Y. But path $U - W - V - X - Z$ is not blocked (we have converging arrows at W and a child of W is in the evidence, and so the path is not blocked at W).

We have a single unblocked path, and information can flow along $U - W - V - X - Z$. Now, if Z is true then this makes V more likely to be true by the positive correlation argument in (a), and note that Y being true makes W likely to be true. We now have an "explaining away" pattern at W where having Y be more likely to be true, conditioned on W being likely to be true, makes U less likely to be true.

Hence the ">" in the answer.

3. **Bayesian networks** [Long]

Consider this example of a Bayesian network with binary variables. It models a garden lawn and whether or not the grass is wet.



(a) Construct an alternative Bayesian network that models the same distribution for variable ordering, S, C, R, W. That is, add S, then C with any required edge, then R with any required edges, then W with any required edges. **Don't specify conditional probability tables.** [Hint: Use the given Bayesian network to determine which conditional Independence properties hold amongst preceding variables, and only include needed edges.]

(b) Is this new Bayesian network a correct model of the distribution? Which network do you consider to be preferable, if any?

(c) Going back to the original network, what is the probability that it is not cloudy, rains, sprinkler doesn't run, and grass is wet?

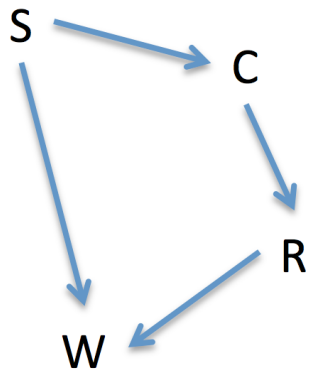
(d) In the original network: write down the first two steps of variable elimination for $p(W)$, eliminating C and then S. Perform the numerical calculations!

Solution.

(a) Construct the Bayesian Network for ordering S, C, R, W. [Note: written in full here, but you didn't need to provide this detail]

- Variable S: just add the node
- Variable C: check the following
  - can we add no in-edges? Is $C \perp S$? no!

  Conclude that we need edge $S \to C$.
- Variable R: check the following
  - can we add no in-edges? Is $R \perp C$? no!
  - can we add just one in-edge? Suppose we add C to R. Is $R \perp S \,|\, C$? yes! (in original network: R-C-S blocked at C, R-W-S blocked at W.) Conclude can just add C to R.
- Variable W: check the following
  - can we add no in-edges? Is $W \perp R$? No!
  - can we add just one in-edge?
    what if we just had the R-W edge? Is $W \perp C \,|\, R$? no, path $C - S - W$ not blocked in original network.
    what if we just had the C-W edge? Is $R \perp W \,|\, C$? no!
    what if we just had the S-W edge? Is $R \perp W \,|\, S$? no!
  - can we add just two in-edges? Consider edges S-W and R-W. Is $C \perp W \,|\, S, R$? checking original network, yes! paths CRW and CSW are both blocked. Conclude that it is sufficient to just add these two edges.



(b) Yes, it is correct.[1]

In this case, both have the same number of parameters ($1+2+2+4=9$), and thus one is not preferred for reasons of compactness.[2] But we might prefer the first network because it is constructed in a causal order and is therefore more interpretable (the $S \to C$ edge in the new network is hard to interpret!).

[1] Networks are correct for any ordering, but the ordering can affect compactness and interpretability.

[2] Compact networks are generally preferred because they have fewer parameters, need less data to learn, and are less likely to overfit if data is noisy.

(c)

$$p(C = false, R = true, S = false, W = true) = p(C = false)p(S = false \mid C = false)p(R \mid C = false)p(W$$
$$= 0.5 \cdot 0.5 \cdot 0.2 \cdot 0.9 = 0.045$$

(d)

$$\begin{aligned} p(W) &= \sum_{c,s,r} p(C)p(S \mid C)p(R \mid C)p(W \mid S, R) \\ &= \sum_{s,r} p(W \mid S, R) \sum_{c} p(C)p(S \mid C)p(R \mid C) \\ &= \sum_{s,r} p(W \mid S, R)\psi_1(S, R) \\ &= \sum_{r} \sum_{s} p(W \mid S, R)\psi_1(S, R) \\ &= \sum_{r} \psi_2(W, R) \end{aligned}$$

Calculations:

ψ_1		$C = false$				$C = true$				
S	R	$p(C)$	$p(S \mid C)$	$p(R \mid C)$	$\times$	$p(C)$	$p(S \mid C)$	$p(R \mid C)$	$\times$	$\sum$
T	T	0.5	0.5	0.2	0.05	0.5	0.1	0.8	0.04	0.09
T	F	0.5	0.5	0.8	0.2	0.5	0.1	0.2	0.01	0.21
F	T	0.5	0.5	0.2	0.05	0.5	0.9	0.8	0.36	0.41
F	F	0.5	0.5	0.8	0.2	0.5	0.9	0.2	0.09	0.29

ψ_2		$S = false$			$S = true$			
W	R	$p(W \mid S, R)$	$\psi_1(S, R)$	$\times$	$p(W \mid S, R)$	$\psi_1(S, R)$	$\times$	$\sum$
T	T	0.9	0.41	0.369	0.99	0.09	0.0891	0.4581
T	F	0.01	0.29	0.0029	0.9	0.21	0.189	0.1919
F	T	0.1	0.41	0.041	0.01	0.09	0.0009	0.0419
F	F	0.99	0.29	0.2871	0.1	0.21	0.021	0.3081

4. **Markov Decision Process (modeling).** [Long] [Harder than an MDP modeling question you'd expect on Spring 2021 midterm]

   You are asked to develop a Markov Decision Process (MDP) to be used for the control of a single elevator. To model:

   - There are three floors
   - There are three buttons inside the car
   - There is a single call button outside on each floor
   - The door of the elevator opens and closes.

   The "agent" here is the elevator itself, and the aim of the system is to get passengers to their appropriate floors.

   (a) Describe in words the states, actions, reward function, and transition model for a suitable MDP model. Make sure that the reward function is clear.

   (b) Explain your model as you introduce it. From your explanation the reader should understand the idea for why an optimal policy should lead to an efficient system.

   NOTE: **There is no single correct answer here.**

Solution.

There is no single correct answer to this problem, but your response should clearly identify the sets of states and actions, the reward function, and reasonable transitions.

States

A single state $s \in S$ is represented in a factored way through $s = (F, R, C)$, with

- (floor) $F \in \{1, 2, 3\}$
- (requests from inside car) $R \subseteq \{1, 2, 3\}$
- (call from outside elevator) $C \subseteq \{1, 2, 3\}$

Initial state: $F = 1, R = \emptyset, C = \emptyset$.

Note: we choose not to model whether the door is open or closed, where the elevator was in the past, or how long someone has been waiting.

Actions

An action is one of

- open-close (modeled as a single action, for simplicity)
- up (available if $F < 3$)
- down (available if $F > 1$)
- nothing

The 'nothing' action is to stop the elevator continually doing something

Reward

$$r(s, \text{open-close}) = \begin{cases} 1 & \text{if } (F \in C) \vee (F \in R) \\ -0.01 & \text{o.w.} \end{cases}$$

$$r(s, up) = r(s, down) = -0.01$$

$$r(s, nothing) = 0$$

We include positive reward when the open-close action is taken and the elevator is at a floor where it has been requested to go to or where it was called from. Other rewards are negative to dissuade it from doing things without need.

Transition

Define random variables $X_j \sim [\{j\} : 0.5,\ \emptyset : 0.5]$ that take on set value $\{j\}$ w.p. 0.5, and emptyset otherwise.

Define random variable $Y(C, F)$ that is $\emptyset$ if $F \notin C$ (was not called to this floor), or uniformly sampled from $\{1, 2, 3\} \setminus F$ otherwise (the floor the rider wants to go to.)

We can now define a transition model for next state $s' = (F', R', C')$ reached after action a in state s. We do this in factored way. First, in regard to floor:

- if $a = up$: then $F' = F + 1$
- if $a = down$: then $F' = F - 1$
- if $a = nothing$ or $a =$ open-close then $F' = F$

Second, in regard to calls:

- if $a \in \{up, down, nothing\}$ then $C' := C \cup X_1 \cup X_2 \cup X_3$ because we assume that there's a 50% probability of each floor being called from outside
- if $a =$ open-close then $C' := (C \setminus F) \cup X_1 \cup X_2 \cup X_3$ because open-close will drop any call button at that floor, but someone else can still call before the next period

Third, in regard to requests:

- if $a \in \{up, down, nothing\}$ then $R' := R$
- if $a =$ open-close then $R' := (R \setminus F) \cup Y(C, F)$

Note: this models that the effect of open-close is to drop any request that had been at that floor, and add a request only if there had been a call at the floor, and only going to a different floor.

5. **Alternate Reward Function for MDPs** [Short]

We have been assuming that the reward function for an MDP has the form $r(s, a)$. Also recall that we have written value iteration for infinite-horizon problems as:

$$V'(s) \leftarrow \max_a \left[r(s,a) + \gamma \sum_{s'} p(s' \mid s, a) V(s') \right] \tag{1}$$

Now, imagine that we have a reward function that depends on both the current state *and* the next state, i.e., $r(s, a, s')$.

(a) Explain why this kind of reward function can be useful from a modeling perspective

(b) Write an expression for the value iteration step that incorporates this alternative type of reward.

(c) Explain formally why this approach is neither more general nor less general than an MDP model that insists on just using $r(s, a)$.

Solution.

(a) This can be useful for modeling. For example, a room cleaning robot can have $r(s, pick - up, s') = 1$ if next state does not have a broken object and $r(s, pick - up, s') = -10$ if next state does have a broken object. Without this, we'd model $r(s, pick - up)$ as the expected reward for these two outcomes.

(b) The value iteration step becomes:

$$V'(s) \leftarrow \max_a \left[\sum_{s'} p(s' \mid s, a) r(s, a, s') + \gamma \sum_{s'} p(s' \mid s, a) V(s') \right]$$

(c) This approach can represent any $r(s, a)$ reward because we can always define $r(s, a, s') = r(s, a)$, for all values of s'. Any $r(s, a, s')$ function can be represented as an $r(s, a)$ function by defining $r(s, a) = \sum_{s'} p(s' \mid s, a) r(s, a, s')$.

6. **Planning in MDPs** [Typical]

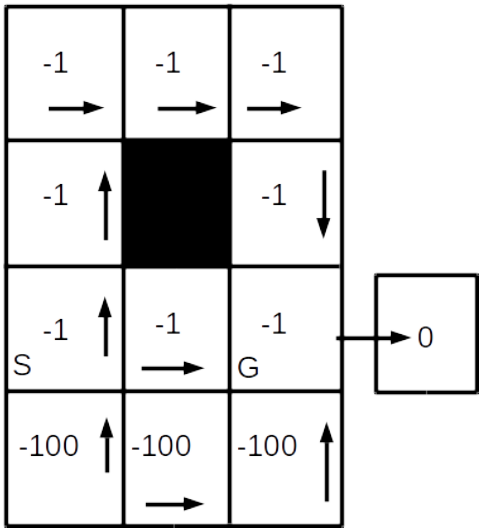
Consider a gridworld with the layout below. From each square, the agent may move into an adjoining square (up, down, left, right) or stay in place. If a policy specifies a move into a square which does not exist (i.e. down from one of the squares in the bottom row), the agent stays in place. Actions are deterministic, that is, they always have their intended effect. We use an infinite horizon with discount $\gamma = 1$. [This keeps the math simple in this example]

The robot starts in the state marked with an S. Upon reaching the state marked G the agent transitions into an absorbing state where it stays forever. **The rewards associated with a state are the reward for taking any action from that state**.

Recall the policy improvement step in policy iteration (where V^π is the value function of the current policy):

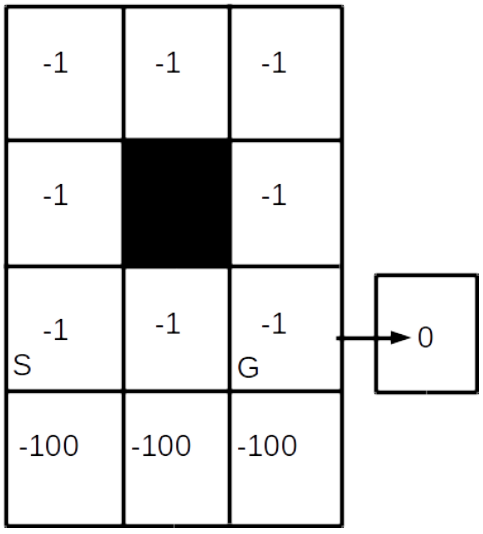
$$\pi'(s) \leftarrow \arg\max_{a \in A} \left[r(s,a) + \gamma \sum_{s' \in S} p(s' \mid s, a) V^\pi(s') \right], \quad \forall s$$

(a) Suppose that we follow the policy given by the arrows. What is the MDP value of each state under this policy? [You can figure this out by inspection of the policy and the environment]



(b) Can this policy be improved? To check this, (1) use policy improvement and draw the adjusted policy and (2) compute the new value function in each state.

(c) Is the new policy optimal? [Hint: you should be able to argue yes/no directly, without doing another round of policy iteration]



Solution.

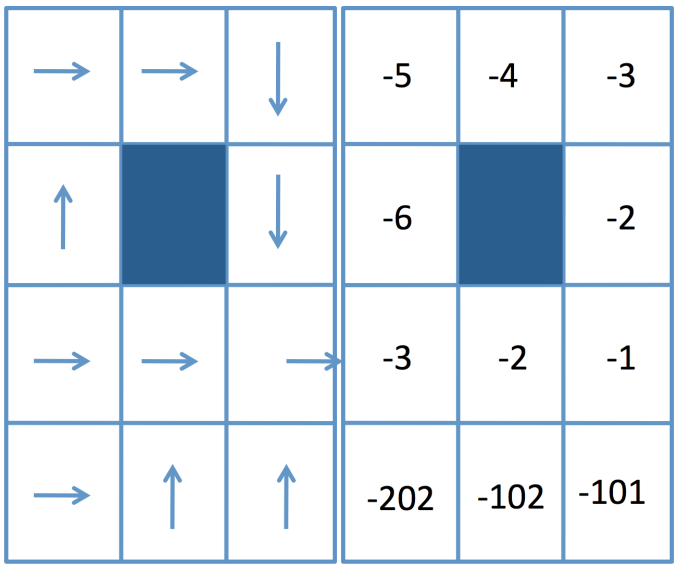
(a) See the following figure for the MDP value of each state under this policy. [Note: it is $-\infty$ in states for which the policy does not escape to the goal state because $\gamma = 1$ and thus there is no discount.]

-∞	-∞	-∞
-∞		-2
-∞	-2	-1
-∞	-201	-101

(b) See the following figure for the updated policy and MDP value function based on one round of policy iteration.

Here, we break ties by leaving the action unchanged if there is no better action relative to the last round of policy iteration.

We see the new policy is better in a number of states.



(c) The new policy is still not optimal; e.g, it moves right in the bottom-left state, whereas it would be optimal to move up. [Similarly, it moves up in the state to the left of the missing position, when it would be better to move down.]

7. **Reinforcement learning** [Typical]

The update rule for **SARSA** reinforcement learning is:

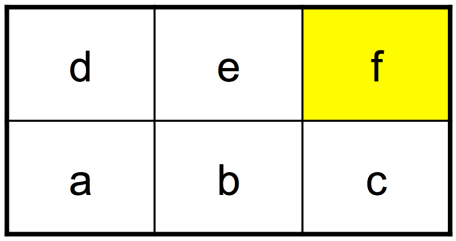
$$Q(s,a) \leftarrow Q(s,a) + \alpha[(r + \gamma Q(s',a')) - Q(s,a)]. \tag{2}$$

(a) What are the different quantities, how are they generated (e.g., which by the agent, which from the environment), and what is the idea of the update?

(b) What is meant by 'on-policy' and 'off-policy' reinforcement learning, and is SARSA an on-policy or off-policy method?

(c) What does it mean to **exploit** in the context of reinforcement learning?

(d) Consider this simple MDP world, where the reward is 100 for any action taken in state f and 0 in all other states and actions are deterministic (thus 'up' always moves 'up').



Assume the Q-values are initialized to 0, and the agent is initially in state c. What are the updates made by SARSA following each action (for $\alpha = 0.9$ and $\gamma = 0.9$).

Assume that no update is possible until the values of s, a, r, s', a' are all well-defined.

i. up (to state f)
ii. left (to state e)
iii. right (to state f)
iv. down (to state c)

Solution.

(a) s is current state, a is selected via an agent's policy such as ϵ-greedy, reward is given by the MDP for $r(s,a)$, state s' is given by the MDP for $p(s' \mid s,a)$, action a' is given by the agent's policy.

The idea is to use a single step observation to adjust the Q value for the state-action (s,a) closer to that which is consistent with the policy being followed by the agent. Eventually we hope Bellman equations will hold the and the Q values correspond to those of the optimal policy.

(b) On-policy: with enough observations, and a learning rate that becomes small in the limit, the Q-values learned will correspond to those of the policy we follow while learning (i.e., the one that we converge to as a result of learning, which would involve ϵ-exploration if using ϵ-greedy).

Off-policy: with enough observations, and a learning rate that becomes small in the limit, the Q-values learned will correspond to the optimal policy.

SARSA is on-policy.

(c) Exploit: this means to follow $\max_a Q(s,a)$ in state s, rather than also explore (e.g., by taking some other action with small probability $\epsilon > 0$).

(d) SARSA updates:

- up (to state f): have $s = c, a = up, r = 0, s' = f, a' =$??, and we cannot do an update yet
- left (to state e): now have $s = c, a = up, r = 0, s' = f, a' = \mathit{left}$, and we can do update to $Q(c, up)$:

$$Q'(c, up) \leftarrow Q(c, up) + 0.9((0 + 0.9Q(f, \mathit{left})) - Q(c, up)) = 0 + 0.9((0 + 0.9(0)) - 0) = 0$$

- right (to state f): now have $s = f, a = \mathit{left}, r = 100, s' = e, a' = right$, and we can do an update to $Q(f, \mathit{left})$:

$$\begin{aligned} Q'(f, \mathit{left}) &\leftarrow Q(f, \mathit{left}) + 0.9((100 + 0.9Q(e, right)) - Q(f, \mathit{left})) \\ &= 0 + 0.9((100 + 0.9(0)) - 0) = 90 \end{aligned}$$

- down (to state c): now we have $s = e, a = right, r = 0, s' = f, a' = down$, and we can do an update to $Q(e, right)$:

$$\begin{aligned} Q'(e, right) &\leftarrow Q(e, right) + 0.9((0 + 0.9Q(f, down)) - Q(e, right)) \\ &= 0 + 0.9((0 + 0.9(0)) - 0) = 0 \end{aligned}$$

8. **K-Means** [Typical]

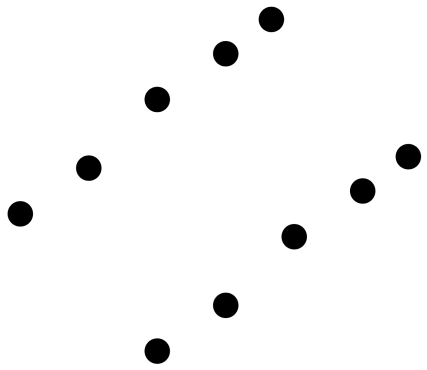
In K-Means, we are given a set of points $\mathbf{x}_1, \ldots, \mathbf{x}_N$ and a fixed number of clusters K. Our aim is to find cluster centers $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_K$ that represent the data.

(a) Define the K-Means loss function.

(b) What two steps does Lloyd's algorithm repeat in order to find a good clustering?

(c) What is the asympotic run-time of each step of Lloyd's algorithm, as a function of the number of examples N and the number of clusters K?

(d) Given data that falls on two parallel diagonal lines as shown below, can Lloyd's algorithm with $K = 2$ find two clusters, such that each line is in one of the clusters?



Solution.

(a) The objective is to find prototypes and an assignment to minimize

$$\sum_{n=1}^{N}\sum_{k=1}^{K} r_{nk}||\mathbf{x}_n - \boldsymbol{\mu}_k||^2$$

where r_n is a one-hot vector with 1 in the position corresponding to the index of the assigned cluster for the point $\mathbf{x}_n$.

(b) Step 1: assign each example to the closest prototype; step 2: for each cluster k, set $\boldsymbol{\mu}_k$ to the centroid of the assigned examples

$$\boldsymbol{\mu}_k := \frac{1}{N_k}\sum_n r_{nk}\mathbf{x}_n$$

where $N_k = \sum_n r_{nk}$ and $r_{nk} = 1$ if $\mathbf{x}_n$ assigned to cluster k, and 0 otherwise.

(c) Step 1 takes time NK because each example is checked for the closest of K prototypes.

Step 2 takes time N because each example is in exactly one cluster, and this is used once in the averaging step.

Overall, the complexity is $N + NK$ each iteration, and $O(NK)$. [Note: (1) we choose to ignore the dependence on number of features D.]

(d) Yes, for a suitable initialization.

Consider two clusters assignments, one to the top line and one to the bottom line, where the cluster centers lie approximately at the middle of the respective line segments.

We need to check this is a stable assignment for K-means.

In particular, is each point in a cluster closer to its centroid than the centroid of the other cluster?

This looks to be true, and thus K-means would converge on such a clustering if such centroids were ever found during LLoyd's algorithm.

Thus it is possible for K-means to find this clustering— so long as an appropriate initialization is given! One way to see this is that it would work if the prototypes were simply initialized to the cluster centers.

9. **Hidden Markov Models** [Long] [You would need a calculator for this one!]

Consider a weather domain, with observations $\mathbf{x}_t \in \{D, R\}$ (dry, rain) and hidden state $\mathbf{s}_t \in \{C, S\}$ (cloud, sun). Assume the following parameters:

- initial prob: $p(\mathbf{s}_1 = C) = 0.7$
- transition

$p(\mathbf{s}_{t+1} \mid \mathbf{s}_t)$		Next State C	Next State S
State	C	0.8	0.2
	S	0.1	0.9

- output

$p(\mathbf{x}_t \mid \mathbf{s}_t)$		Output D	Output R
State	C	0.25	.75
	S	0.6	0.4

(a) For a general HMM, if the total number of timesteps is n and $t < n$ is a timestep in the middle of the sequence, why is $p(\mathbf{s}_t \mid \mathbf{x}_1, \ldots, \mathbf{x}_n) \neq p(\mathbf{s}_t \mid \mathbf{x}_1, \ldots, \mathbf{x}_t)$? (An informal answer is fine.)

(b) (Forward-backward algorithm). Now suppose we observe $\mathbf{x}_1 = R$, $\mathbf{x}_2 = R$.
We can calculate:

$$\alpha_1(\mathbf{s}_1) = \begin{cases} 0.525 & \text{, if } \mathbf{s}_1 = C \\ 0.12 & \text{, if } \mathbf{s}_1 = S \end{cases}$$

Use

$$\alpha_2(\mathbf{s}_2) = p(\mathbf{x}_2 \mid \mathbf{s}_2) \sum_{\mathbf{s}_1} p(\mathbf{s}_2 \mid \mathbf{s}_1) \alpha_1(\mathbf{s}_1)$$

to compute the α_2-values.

(c) We have $\beta_2(\mathbf{s}_2) = 1$. In addition, we can calculate:

$$\beta_1(\mathbf{s}_1) = \begin{cases} 0.68 & , \text{if } \mathbf{s}_1 = C \\ 0.435 & , \text{if } \mathbf{s}_1 = S \end{cases}$$

Use these quantities, and

$$p(\mathbf{s}_2 \,|\, \mathbf{x}_1, \mathbf{x}_2) \propto \alpha_2(\mathbf{s}_2)$$
$$p(\mathbf{s}_1 \,|\, \mathbf{x}_1, \mathbf{x}_2) \propto \alpha_1(\mathbf{s}_1)\beta_1(\mathbf{s}_1)$$

to infer the values of $p(\mathbf{s}_1 \,|\, \mathbf{x}_1, \mathbf{x}_2)$ and $p(\mathbf{s}_2 \,|\, \mathbf{x}_1, \mathbf{x}_2)$.

(d) Use $p(\mathbf{x}_1, \mathbf{x}_2) = \sum_{\mathbf{s}_t} \alpha_t(\mathbf{s}_t)\beta_t(\mathbf{s}_t)$ to calculate the likelihood of the data.

Solution.

(a) The additional observations from $t+1$ to n may also be informative as to the hidden state at period t. For example, the observation at $\mathbf{x}_{t+1}$ might only be possible if $\mathbf{s}_t$ has a value that allows for $\mathbf{s}_{t+1}$ to have a value that can generate $\mathbf{x}_{t+1}$.

(b) Calculations for the $\alpha_2(\mathbf{s}_2)$ values are:

$\mathbf{s}_1$	$\mathbf{s}_2$	$p(\mathbf{s}_2 \mid \mathbf{s}_1)$	$p(R \mid \mathbf{s}_2)$	$\alpha_1(\mathbf{s}_1)$	$\times$ (product)
C	C	0.8	0.75	0.525	0.315
C	S	0.2	0.4	0.525	0.042
S	C	0.1	0.75	0.12	0.009
S	S	0.9	0.4	0.12	0.0432

and then summing out $\mathbf{s}_1$, we obtain

$\mathbf{s}_2$	$\alpha_2(\mathbf{s}_2)$
C	0.315+0.009=0.324
S	0.042+0.0432=0.0852

(c) For $t = 1$, we have

$$p(\mathbf{s}_1 \mid R, R) \propto \alpha_1(\mathbf{s}_1)\beta_1(\mathbf{s}_1)$$

For $\mathbf{s}_1 = C$:

$$\alpha_1(C)\beta_1(C) = (0.525)(0.68) = 0.357$$

For $\mathbf{s}_1 = S$:

$$\alpha_1(S)\beta_1(S) = (0.12)(0.435) = 0.0522$$

We conclude that $p(\mathbf{s}_1 = C \mid R, R) \approx 0.872$ and $p(\mathbf{s}_1 = S \mid R, R) \approx 0.128$.

For $t = 2$, we have

$$p(\mathbf{s}_2 \mid R, R) \propto \alpha_2(\mathbf{s}_2)$$

For $\mathbf{s}_2 = C$:

$$\alpha_2(C) = (0.324) = 0.324$$

For $\mathbf{s}_2 = S$:

$$\alpha_2(S) = (0.0852) = 0.0852$$

We conclude that $p(\mathbf{s}_2 = C \mid R, R) \approx 0.792$ and $p(\mathbf{s}_2 = S \mid R, R) \approx 0.208$.

(d) The likelihod of the data is

$$p(R, R) = \sum_{\mathbf{s}_1} \alpha_1(\mathbf{s}_1)\beta_1(\mathbf{s}_1) = (0.525)(0.68) + (0.12)(0.435) = 0.4092.$$

Equivalently, we could calculate using $t = 2$ alpha and beta values, and get

$$p(R, R) = \sum_{\mathbf{s}_2} \alpha_2(\mathbf{s}_2)\beta_2(\mathbf{s}_2) = (0.324)(1) + (0.0852)(1) = 0.4092$$

10. **Mean of a Mixture Model** [Short]

For some class conditional distribution p_{class}, the details of which don't matter for this question, we are given a mixture model of the form

$$p(\mathbf{x}; \{\boldsymbol{\pi}_k\}_{k=1}^K, \boldsymbol{\theta}) = \sum_{k=1}^K \theta_k \, p_{\text{class}}(\mathbf{x} \,|\, \mathbf{z} = C_k; \boldsymbol{\pi}_k) \tag{3}$$

where example $\mathbf{x} \in \mathbb{R}^D$.

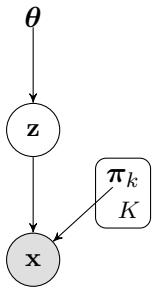
(a) Draw a graphical model with plates to show the form of this mixture distribution for a single example $\mathbf{x}$. [Note: if you're unfamiliar with the idea of "plate notation" for graphical models, take a quick look at p.363-365 in Bishop's book `https://bit.ly/3eajKx5`]

(b) Suppose that the mean of the class-conditional distribution for component k is given by $\boldsymbol{\mu}_k$. Show that the mean of the overall mixture model is given by

$$\mathbb{E}[\mathbf{x}] = \sum_{k=1}^K \theta_k \boldsymbol{\mu}_k.$$

Solution:

(a) We draw this for a single $\mathbf{x}$ variable. Since $\boldsymbol{\pi}_k$ and $\boldsymbol{\theta}$ are parameters that are not random variables, we don't have circles around them.



(b) For this, it is convenient to work with latent variable $\mathbf{z}$. We have

$$\begin{aligned}\mathbb{E}[\mathbf{x}] &= \sum_{k=1}^{K} p(\mathbf{z} = C_k; \boldsymbol{\theta}) \mathbb{E}_{\mathbf{x} \sim p_{\text{class}}(\mathbf{x}|\mathbf{z}=C_k;\boldsymbol{\pi}_k)}[\mathbf{x}] \\ &= \sum_{k=1}^{K} \theta_k \boldsymbol{\mu}_k\end{aligned}$$

11. **Expectation Maximization** [Typical]

We have a collection of binary images $\mathbf{x}_1, \ldots, \mathbf{x}_N$, each of which is 5×5. We treat each image $\mathbf{x}_n$ as a 25-dimensional binary vector where the dth pixel is $x_{n,d}$. We model an image as coming from a mixture distribution, with a product-of-Bernoulli distribution for each component k:

$$p(\mathbf{x}_n; \boldsymbol{\mu}_k) = \prod_{d=1}^{25} \mu_{k,d}^{x_{n,d}} (1 - \mu_{k,d})^{1 - x_{n,d}} \qquad \mathbf{x}_n \in \{0,1\}^{25} \qquad \boldsymbol{\mu}_k \in \{0,1\}^{25}.$$

Each of the K components has parameters $\boldsymbol{\mu}_k$, where each dimension $\mu_{k,d}$ specifies the probability that pixel d is black in an example from this component. The mixture weights are $\{\theta_k\}_{k=1}^K$ and known. You will use EM to estimate the $\{\boldsymbol{\mu}_k\}$ parameters.

(a) Write down the probability of generating a single image $\mathbf{x}$, i.e.,

$$p(\mathbf{x}; \{\boldsymbol{\mu}_k\}_{k=1}^K, \boldsymbol{\theta})$$

.

(b) What are the "latent variables" in this model? Draw the plate diagram for this model, writing it for N examples, and indicating what is known and unknown. [Hint: see the previous question for a pointer to plate diagrams]

(c) In the E-step, you find the probability with which example $\mathbf{x}_n$ belongs to each component fixing the parameters $\{\boldsymbol{\mu}_k\}_{k=1}^K$; i.e., $q_{n,k} = p(\mathbf{z}_n = C_k \,|\, \mathbf{x}_n; \{\boldsymbol{\mu}_k\}, \boldsymbol{\theta})$ for each k. Derive the expression for $q_{n,k}$.

(d) In the M-step, you update the parameters $\{\boldsymbol{\mu}_k\}_{k=1}^K$. Write down the expression for this, making use of the $\mathbf{q}$ values. [No need to derive the answer. As a hint, for the supervised case with class $\mathbf{z}_n$ of each image (one-hot coded), the MLE for the parameters of class k would be

$$\mu_{k,d} = \frac{\sum_{n=1}^N z_{n,k} x_{n,d}}{\sum_{n=1}^N z_{n,k}}$$

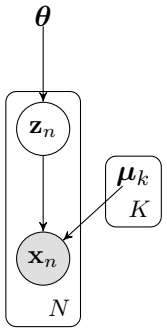
(intuitively, the percentage of times pixel d was black for the data in class k).]

Solution:

(a) Sum out over possible values of the latent variables $\mathbf{z}$:

$$p(\mathbf{x} \,|\, \{\boldsymbol{\mu}_k\}_{k=1}^K; \boldsymbol{\theta}) = \sum_{k=1}^{K} p(\mathbf{z} = C_k;\ \boldsymbol{\theta}) p(\mathbf{x} \,|\, \mathbf{z} = C_k; \boldsymbol{\mu}_k) = \sum_{k=1}^{K} \theta_k \prod_{d=1}^{25} \mu_{k,d}^{x_d} (1 - \mu_{k,d})^{1 - x_d}$$

(b) Plate diagram. The mixture weights $\boldsymbol{\theta}$ and the parameters $\boldsymbol{\mu}_k$ for each component k are parameters and drawn without a circle.



(c) For example $\mathbf{x}_n$, we need to compute

$$q_{n,k} = p(\mathbf{z}_n = C_k \,|\, \mathbf{x}_n; \{\boldsymbol{\mu}_k\}, \boldsymbol{\theta})$$

We do this by applying Bayes' rule:

$$q_{n,k} = p(\mathbf{z}_n = C_k \,|\, \mathbf{x}_x; \{\boldsymbol{\mu}_k\}, \boldsymbol{\theta}) \quad = \quad \frac{1}{Z} p(\mathbf{z}_n = C_k; \boldsymbol{\theta}) p(\mathbf{x}_n \,|\, \mathbf{z}_n = C_k; \boldsymbol{\mu}_k)$$

The normalization term can be computed as $Z = \sum_\ell q_{n,\ell}$.

(d) For EM we instead utilize the predicted assignments of each example to each component, and have

$$\mu_{k,d} = \frac{\sum_{n=1}^{N} q_{n,k} x_{n,d}}{\sum_{n=1}^{N} q_{n,k}}$$

12. **PCA** [Typical]

Consider a mean-centered data set of four points $\mathbf{x}_1 = (1, 0)$, $\mathbf{x}_2 = (-1, 0)$, $\mathbf{x}_3 = (0, -2)$, $\mathbf{x}_4 = (0, 2)$.

(a) Compute the empirical covariance matrix $\mathbf{S}$ for this dataset.

(b) Draw a rough sketch of the distribution $\mathcal{N}(0, \mathbf{S})$ formed with this covariance matrix.

(c) If we were to run PCA on this data, what algebraic properties of the empirical covariance matrix correspond to first and second principal components? What are the first and second principal components in this example? [Hint: you should be able to easily recognize them without computation]

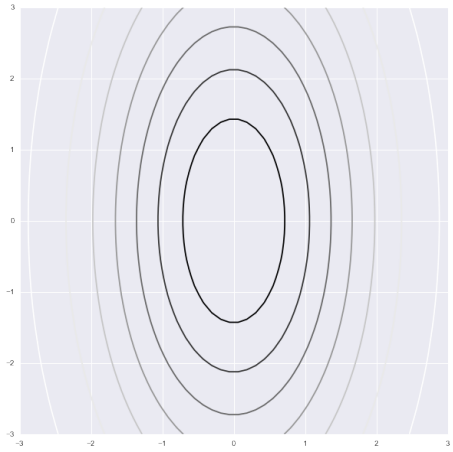
(d) Graph the four points after running PCA and projecting down to a single dimension. What is lost in this transformation?

Solutions:

(a) The empirical covariance matrix is defined as $\frac{1}{N}\sum_{n=1}^{N}(\mathbf{x}_n - \bar{\mathbf{x}})(\mathbf{x}_n - \bar{\mathbf{x}})^\top$.

$$\frac{1}{4}\left(\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 4 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 4 \end{bmatrix} \right) = \begin{bmatrix} 0.5 & 0 \\ 0 & 2 \end{bmatrix}$$

(b) Here's what it looks like. We'd hope for a rough sketch of this form, i.e. that it is an axis-aligned ellipse. The particular position of the contours wouldn't matter.



(c) The first and second principal components correspond to the eigenvectors with the first and second highest eigenvalues of the empirical covariance matrix, respectively. In this case they have a simple form $\mathbf{u}_1 = [0, 1]$ with $\mathbf{S}\mathbf{u}_1 = 2\mathbf{u}_1$ and $\mathbf{u}_2 = [1, 0]$ with $\mathbf{S}\mathbf{u}_2 = 0.5\mathbf{u}_2$. This can also be seen visually from the data.

(d) Projecting to one dimension corresponds to projecting onto the first principal component,

$$\mathbf{z}_n = (\mathbf{x}_n^\top \mathbf{u}_1)\mathbf{u}_1.$$

Given $\mathbf{u}_1$, this takes a simple form and drops the x_1 component of each data point. We have a projection to 1-D of:

$$\mathbf{z}_1 = 0, \mathbf{z}_2 = 0, \mathbf{z}_3 = -2, \mathbf{z}_4 = 2$$

This has the effect of collapsing $\mathbf{x}_1$ and $\mathbf{x}_2$ to the same point, but keeps the distinction between $\mathbf{x}_3$ and $\mathbf{x}_4$.