Exercise 2

1. Algorithm:

Go through every x in the sample and check whether it belongs to our discrete domain $\mathcal{X}$.

If we find such x, then function h_z, where $z = x$ is the outcome of our algorithm. Due to realizability assumption, there can only be one such x in the sample and, therefore, $L_S(h_z)$ will be 0.

If we don't find such x, then h^- is the outcome of our algorithm. Since in this case we don't have any positives in the sample, $L_S(h^-)$ will be 0.

2. If the algorithm described above outputs h_z, then, due to the realizability assumption it will mean that our hypothesis h_z correctly identifies the only positive in our domain, and hence, $L_{D,f}(h_z)$ will be 0, which is less than ε for all $\varepsilon > 0$.

The only case in which our algorithm won't identify the correct labeling function is when the only positive in distribution (let's call it x_j) is not selected to our sample S_x and our algorithm incorrectly returns h^-. Since all items in the sample are i.i.d. selected, the probability of this happening is $(1 - P(x_j))^m$, where m is the size of our sample. We want this probability to be at most δ $(\delta > 0)$, in order for $\mathcal{H}_{singleton}$ to be PAC-learnable

Since in this case, the population risk will be equal to $P_D(x_j^i)$, we get the inequality for the size of the sample m:

$$(1-\varepsilon)^m \leq \delta$$

$$\Updownarrow$$

$$m \geq \lceil \log_{(1-\varepsilon)} \delta \rceil$$

the required upper bound on the sample complexity

Exercise 3 . Fix some distribution D over X.

Assuming realizability, ~~Assumin~~ Let R^* with radius r^* be the concentric circle that generates the labels and let f be the corresponding hypothesis. Let $r < r^*$ be ~~such that~~ one radius of the concentric circle R, such that the probability mass of the area between R and R^* is exactly ε. (Let's denote that area R')

~~If R' has a positive example from the samples~~

Let A be the algorithm that returns the smallest ~~rectangle~~ circle enclosing all positive examples in the training set. From realizability assumption we get that A does not mislable any negative examples (if it does, there should be smaller circle enclosing all positive examples, which contradicts definition of $A(S)$). Hence, A is an ERM.

Since $A(S)$ is the smallest circle enclosing all positive examples, $A(S) \subseteq R^*$. If R' contains any positive example, then the boundary of A lies between R^* and R. Since the probability mass of that region is ε, empirical risk of $A(S)$ in this case will be at most ε.

The probability of positive example being inside R is $1-\varepsilon$, hence the probability of all positive samples ~~to~~ be inside R is $(1-\varepsilon)^m$, where m is the size of the sample. Therefore, the probability that at least one positive is in R' is $1-(1-\varepsilon)^m$.

We get that $P(L_{D,f}(A(S)) < \varepsilon) \geq 1-(1-\varepsilon)^m \geq 1-e^{-m\varepsilon}$

δ

Rewriting this inequality, we get $m \geq \frac{\log(1/\delta)}{\varepsilon}$

Therefore, we have show that $\exists$ algorithm A, s.t. $\forall\ \varepsilon, \delta > 0$, $\forall$ distributions D, $\forall$ labeling fcns f, s.t. D, f realizable by $\mathcal{H}$, given $m \geq \lceil \frac{\log(1/\delta)}{\varepsilon} \rceil$, then w.p. at least $1-\delta$ over $S \sim D^m$, we have
$L_{D,f}(A(S)) < \varepsilon$

Hence, $\mathcal{H}$ is PAC-learnable and its sample complexity is bounded by $m_{\mathcal{H}}(\varepsilon, \delta) \leq \lceil \frac{\log(1/\delta)}{\varepsilon} \rceil$

q. e. d.