Learning from Corrupted Binary Labels via Class-Probability Estimation (Full Version)

Aditya Krishna Menon* ADITYA.MENON@NICTA.COM.AU
Brendan van Rooyen† BRENDAN.VANROOYEN@NICTA.COM.AU
Cheng Soon Ong* CHENGSOON.ONG@NICTA.COM.AU
Robert C. Williamson* BOB.WILLIAMSON@NICTA.COM.AU

* National ICT Australia and The Australian National University, Canberra
† The Australian National University and National ICT Australia, Canberra

Abstract

Many supervised learning problems involve learning from samples whose labels are *corrupted* in some way. For example, each label may be flipped with some constant probability (learning with *label noise*), or one may have a pool of unlabelled samples in lieu of negative samples (learning from *positive and unlabelled data*). This paper uses class-probability estimation to study these and other corruption processes belonging to the *mutually contaminated distributions* framework (Scott et al., 2013), with three conclusions. First, one can optimise balanced error and AUC *without knowledge* of the corruption parameters. Second, given estimates of the corruption parameters, one can minimise a range of classification risks. Third, one can estimate corruption parameters via a class-probability estimator (e.g. kernel logistic regression) *trained solely on corrupted data*. Experiments on label noise tasks corroborate our analysis.

1. Learning from corrupted binary labels

In many practical scenarios involving learning from binary labels, one observes samples whose labels are *corrupted* versions of the actual ground truth. For example, in learning from *class-conditional label noise* (*CCN learning*), the labels are flipped with some constant probability (Angluin & Laird, 1988). In *positive and unlabelled learning* (*PU learning*), we have access to some positive samples, but in lieu of negative samples only have a pool of samples whose label is unknown (Denis, 1998). More generally, suppose there is a notional *clean* distribution D over instances and labels. We say a problem involves learning from *corrupted binary labels* if we observe training samples drawn from some *corrupted* distribution D_{corr} such that the observed labels do not represent those we would observe under D.

A fundamental question is whether one can minimise a given performance measure with respect to D, *given access only to samples from* D_{corr}. Intuitively, in general this requires knowledge of the parameters of the corruption process that determines D_{corr}. This yields two further questions: are there measures for which knowledge of these corruption parameters is *unnecessary*, and for other measures, can we *estimate* these parameters?

In this paper, we consider corruption problems belonging to the *mutually contaminated distributions* framework (Scott et al., 2013). We then study the above questions through the lens of class-probability estimation, with three conclusions. First, optimising balanced error (BER) as-is on corrupted data equivalently optimises BER on clean data, and similarly for the area under the ROC curve (AUC). That is, these measures can be optimised *without knowledge of the corruption process parameters*; further, we present evidence that these are essentially the *only* measures with this property. Second, given estimates of the corruption parameters, a range of classification measures can be minimised by thresholding corrupted class-probabilities. Third, under some assumptions, these corruption parameters may be estimated from the range of the corrupted class-probabilities.

For all points above, observe that learning requires *only corrupted data*. Further, corrupted class-probability estimation can be seen as *treating the observed samples as if they were uncorrupted*. Thus, our analysis gives justification (under some assumptions) for this apparent heuristic in problems such as CCN and PU learning.

While some of our results are known for the special cases of CCN and PU learning, our interest is in determining to

Proceedings of the 32^{nd} *International Conference on Machine Learning*, Lille, France, 2015. JMLR: W&CP volume 37.

what extent they generalise to other label corruption problems. This is a step towards a unified treatment of these problems. We now fix notation and formalise the problem.

2. Background and problem setup

Fix an instance space $\mathcal{X}$. We denote by D some distribution over $\mathcal{X} \times \{\pm 1\}$, with $(\mathsf{X}, \mathsf{Y}) \sim D$ a pair of random variables. Any D may be expressed via the *class-conditional distributions* $(P, Q) = (\mathbb{P}(\mathsf{X} \mid \mathsf{Y} = 1), \mathbb{P}(\mathsf{X} \mid \mathsf{Y} = -1))$ and *base rate* $\pi = \mathbb{P}(\mathsf{Y} = 1)$, or equivalently via *marginal distribution* $M = \mathbb{P}(\mathsf{X})$ and *class-probability function* $\eta \colon x \mapsto \mathbb{P}(\mathsf{Y} = 1 \mid \mathsf{X} = x)$. When referring to these constituent distributions, we write D as $D_{P,Q,\pi}$ or $D_{M,\eta}$.

2.1. Classifiers, scorers, and risks

A *classifier* is any function $f \colon \mathcal{X} \to \{\pm 1\}$. A *scorer* is any function $s \colon \mathcal{X} \to \mathbb{R}$. Many learning methods (e.g. SVMs) output a scorer, from which a classifier is formed by thresholding about some $t \in \mathbb{R}$. We denote the resulting classifier by $\mathrm{thresh}(s, t) \colon x \mapsto \mathrm{sign}(s(x) - t)$.

The *false positive* and *false negative rates* of a classifier f are denoted $\mathrm{FPR}^D(f), \mathrm{FNR}^D(f)$, and are defined by $\underset{\mathsf{X} \sim Q}{\mathbb{P}}(f(\mathsf{X}) = 1)$ and $\underset{\mathsf{X} \sim P}{\mathbb{P}}(f(\mathsf{X}) = -1)$ respectively.

Given a function $\Psi \colon [0,1]^3 \to [0,1]$, a *classification performance measure* $\mathrm{Class}_\Psi^D \colon \{\pm 1\}^{\mathcal{X}} \to [0,1]$ assesses the performance of a classifier f via (Narasimhan et al., 2014)

$$\mathrm{Class}_\Psi^D(f) = \Psi(\mathrm{FPR}^D(f), \mathrm{FNR}^D(f), \pi).$$

A canonical example is the *misclassification error*, where $\Psi \colon (u, v, p) \mapsto p \cdot v + (1 - p) \cdot u$. Given a scorer s, we use $\mathrm{Class}_\Psi^D(s; t)$ to refer to $\mathrm{Class}_\Psi^D(\mathrm{thresh}(s, t))$.

The Ψ*-classification regret* of a classifier $f \colon \mathcal{X} \to \{\pm 1\}$ is

$$\mathrm{regret}_\Psi^D(f) = \mathrm{Class}_\Psi^D(f) - \inf_{g \colon \mathcal{X} \to \{\pm 1\}} \mathrm{Class}_\Psi^D(g).$$

A *loss* is any function $\ell \colon \{\pm 1\} \times \mathbb{R} \to \mathbb{R}_+$. Given a distribution D, the ℓ*-risk* of a scorer s is defined as

$$\mathbb{L}_\ell^D(s) = \underset{(\mathsf{X},\mathsf{Y}) \sim D}{\mathbb{E}} \left[\ell(\mathsf{Y}, s(\mathsf{X})) \right]. \tag{1}$$

The ℓ-regret of a scorer, regret_ℓ^D, is as per the Ψ-regret.

We say ℓ is *strictly proper composite* (Reid & Williamson, 2010) if $\mathrm{argmin}_s \mathbb{L}_\ell^D(s)$ is some strictly monotone transformation ψ of η, i.e. we can recover class-probabilities from the optimal prediction via the *link function* ψ. We call *class-probability estimation* (*CPE*) the task of minimising Equation 1 for some strictly proper composite ℓ.

The conditional Bayes-risk of a strictly proper composite ℓ is $L_\ell \colon \eta \mapsto \eta \ell_1(\psi(\eta)) + (1 - \eta) \ell_{-1}(\psi(\eta))$. We call ℓ *strongly proper composite* with modulus λ if L_ℓ is λ-strongly concave (Agarwal, 2014). Canonical examples of such losses are the logistic and exponential loss, as used in logistic regression and AdaBoost respectively.

Quantity	**Clean**	**Corrupted**
Joint distribution	D	$\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$ or D_{corr}
Class-conditionals	P, Q	$P_{\mathrm{corr}}, Q_{\mathrm{corr}}$
Base rate	π	π_{corr}
Class-probability	η	η_{corr}
Ψ-optimal threshold	t_Ψ^D	$t_{\mathrm{corr},\Psi}^D$

Table 1. Common quantities on clean and corrupted distributions.

2.2. Learning from contaminated distributions

Suppose $D_{P,Q,\pi}$ is some "clean" distribution where performance will be assessed. (We do *not* assume that D is separable.) In MC learning (Scott et al., 2013), we observe samples from some *corrupted* distribution $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$ over $\mathcal{X} \times \{\pm 1\}$, for some *unknown* noise parameters $\alpha, \beta \in [0,1]$ with $\alpha + \beta < 1$; where the parameters are clear from context, we occasionally refer to the corrupted distribution as D_{corr}. The corrupted class-conditional distributions $P_{\mathrm{corr}}, Q_{\mathrm{corr}}$ are

$$\begin{aligned} P_{\mathrm{corr}} &= (1 - \alpha) \cdot P + \alpha \cdot Q \\ Q_{\mathrm{corr}} &= \beta \cdot P + (1 - \beta) \cdot Q, \end{aligned} \tag{2}$$

and the corrupted base rate π_{corr} in general has *no relation* to the clean base rate π. (If $\alpha + \beta = 1$, then $P_{\mathrm{corr}} = Q_{\mathrm{corr}}$, making learning impossible, whereas if $\alpha + \beta > 1$, we can swap $P_{\mathrm{corr}}, Q_{\mathrm{corr}}$.) Table 1 summarises common quantities on the clean and corrupted distributions.

From (2), we see that none of $P_{\mathrm{corr}}, Q_{\mathrm{corr}}$ or π_{corr} contain any information about π in general. Thus, estimating π from $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$ is *impossible* in general. The parameters α, β are also non-identifiable, but can be estimated under some assumptions on D (Scott et al., 2013).

2.3. Special cases of MC learning

Two special cases of MC learning are notable. In learning from *class-conditional label noise* (*CCN learning*) (Angluin & Laird, 1988), positive samples have labels flipped with probability ρ_+, and negative samples with probability ρ_-. This can be shown to reduce to MC learning with

$$\alpha = \pi_{\mathrm{corr}}^{-1} \cdot (1 - \pi) \cdot \rho_- \,, \, \beta = (1 - \pi_{\mathrm{corr}})^{-1} \cdot \pi \cdot \rho_+, \tag{3}$$

and the corrupted base rate $\pi_{\mathrm{corr}} = (1 - \rho_+) \cdot \pi + \rho_- \cdot (1 - \pi)$. (See Appendix C for details.)

In learning from *positive and unlabelled data* (*PU learning*) (Denis, 1998), one has access to *unlabelled* samples in lieu of negative samples. There are two subtly different settings: in the *case-controlled* setting (Ward et al., 2009), the unlabelled samples are drawn from the marginal distribution M, corresponding to MC learning with $\alpha = 0, \beta = \pi$, and π_{corr} arbitrary. In the *censoring* setting (Elkan & Noto, 2008), observations are drawn from D followed by a *label censoring* procedure. This is in fact a special of CCN (and hence MC) learning with $\rho_- = 0$.

3. BER and AUC are immune to corruption

We first show that optimising balanced error and AUC on corrupted data is *equivalent* to doing so on clean data. Thus, with a suitably rich function class, one can optimise balanced error and AUC from corrupted data *without* knowledge of the corruption process parameters.

3.1. BER minimisation is immune to label corruption

The *balanced error* (*BER*) (Brodersen et al., 2010) of a classifier is simply the mean of the per-class error rates,

$$\mathrm{BER}^D(f) = \frac{\mathrm{FPR}^D(f) + \mathrm{FNR}^D(f)}{2}.$$

This is a popular measure in imbalanced learning problems (Cheng et al., 2002; Guyon et al., 2004) as it penalises sacrificing accuracy on the rare class in favour of accuracy on the dominant class. The negation of the BER is also known as the AM (arithmetic mean) metric (Menon et al., 2013).

The BER-optimal classifier thresholds the class-probability function at the base rate (Menon et al., 2013), so that:

$$\underset{f\colon \mathcal{X}\to\{\pm 1\}}{\operatorname{argmin}} \ \mathrm{BER}^D(f) = \mathrm{thresh}(\eta, \pi) \quad (4)$$

$$\underset{f\colon \mathcal{X}\to\{\pm 1\}}{\operatorname{argmin}} \ \mathrm{BER}^{D_{\mathrm{corr}}}(f) = \mathrm{thresh}(\eta_{\mathrm{corr}}, \pi_{\mathrm{corr}}), \quad (5)$$

where η_{corr} denotes the corrupted class-probability function. As Equation 4 depends on π, it may appear that one must know π to minimise the clean BER from corrupted data. Surprisingly, the BER-optimal classifiers in Equations 4 and 5 *coincide*. This is because of the following relationship between the clean and corrupted BER.

Proposition 1. *Pick any* D *and* $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$. *Then, for any classifier* $f\colon \mathcal{X} \to \{\pm 1\}$,

$$\mathrm{BER}^{D_{\mathrm{corr}}}(f) = (1 - \alpha - \beta) \cdot \mathrm{BER}^D(f) + \frac{\alpha + \beta}{2}, \quad (6)$$

and so the minimisers of the two are identical.

Thus, when BER is the desired performance metric, we *do not need to estimate the noise parameters, or the clean base rate*: we can (approximately) optimise the BER on the corrupted data using estimates $\hat{\eta}_{\mathrm{corr}}, \hat{\pi}_{\mathrm{corr}}$, from which we build a classifier $\mathrm{thresh}(\hat{\eta}_{\mathrm{corr}}, \hat{\pi}_{\mathrm{corr}})$. Observe that this approach effectively *treats the corrupted samples as if they were clean*, e.g. in a PU learning problem, we treat the unlabelled samples as negative, and perform CPE as usual.

With a suitably rich function class, surrogate regret bounds quantify the efficacy of thresholding approximate class-probability estimates. Suppose we know the corrupted base rate[1] π_{corr}, and suppose that s is a scorer with low ℓ-regret on the *corrupted* distribution for some proper composite loss ℓ with link ψ i.e. $\psi^{-1}(s)$ is a good estimate of η_{corr}. Then, the classifier resulting from thresholding this scorer will attain low BER on the *clean* distribution D.

Proposition 2. *Pick any* D *and* $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$. *Let* ℓ *be a strongly proper composite loss with modulus* λ *and link function* ψ. *Then, for any scorer* $s\colon \mathcal{X} \to \mathbb{R}$,

$$\mathrm{regret}^D_{\mathrm{BER}}(f) \le \frac{C(\pi_{\mathrm{corr}})}{1 - \alpha - \beta} \cdot \sqrt{\frac{2}{\lambda}} \cdot \sqrt{\mathrm{regret}^{D_{\mathrm{corr}}}_{\ell}(s)},$$

where $f = \mathrm{thresh}(s, \psi(\pi_{\mathrm{corr}}))$ *and* $C(\pi_{\mathrm{corr}}) = (2 \cdot \pi_{\mathrm{corr}} \cdot (1 - \pi_{\mathrm{corr}}))^{-1}$.

Thus, good estimates of the *corrupted* class-probabilities let us minimise the *clean* BER. Of course, learning from corrupted data comes at a price: compared to the regret bound obtained if we could minimise ℓ on the *clean* distribution D, we have an extra penalty of $(1 - \alpha - \beta)^{-1}$. This matches our intuition that for high-noise regimes (i.e. $\alpha + \beta \approx 1$), we need more corrupted samples to learn effectively with respect to the clean distribution; confer van Rooyen & Williamson (2015) for lower and upper bounds on sample complexity for a range of corruption problems.

3.2. AUC maximisation is immune to label corruption

Another popular performance measure in imbalanced learning scenarios is the *area under the ROC curve* (*AUC*). The AUC of a scorer, $\mathrm{AUC}^D(s)$, is the probability of a random positive instance scoring higher than a random negative instance (Agarwal et al., 2005):

$$\mathop{\mathbb{E}}_{\mathsf{X}\sim P, \mathsf{X}'\sim Q} \left[[\![s(\mathsf{X}) > s(\mathsf{X}')]\!] + \frac{1}{2} [\![s(\mathsf{X}) = s(\mathsf{X}')]\!] \right].$$

We have a counterpart to Proposition 1 by rewriting the AUC as an average of BER across a range of thresholds ((Flach et al., 2011); see Appendix A.5):

$$\mathrm{AUC}^D(s) = \frac{3}{2} - 2 \cdot \mathbb{E}_{\mathsf{X}\sim P}[\mathrm{BER}^D(s; s(\mathsf{X}))]. \quad (7)$$

[1] Surrogate regret bounds may also be derived for an empirically chosen threshold (Kotłowski & Dembczyński, 2015).

Corollary 3. *Pick any* $D_{P,Q,\pi}$ *and* $\operatorname{Corr}(D, \alpha, \beta, \pi_{\text{corr}})$. *Then, for any scorer* $s\colon \mathcal{X} \to \mathbb{R}$,

$$\text{AUC}^{D_{\text{corr}}}(s) = (1 - \alpha - \beta) \cdot \text{AUC}^{D}(s) + \frac{\alpha + \beta}{2}. \quad (8)$$

Thus, like the BER, optimising the AUC with respect to the corrupted distribution optimises the AUC with respect to the clean one. Further, via recent bounds on the AUC-regret (Agarwal, 2014), we can show that a good corrupted class-probability estimator will have good clean AUC.

Corollary 4. *Pick any* D *and* $\operatorname{Corr}(D, \alpha, \beta, \pi_{\text{corr}})$. *Let* ℓ *be a strongly proper composite loss with modulus* λ. *Then, for every scorer* $s\colon \mathcal{X} \to \mathbb{R}$,

$$\text{regret}^{D}_{\text{AUC}}(s) \le \frac{C(\pi_{\text{corr}})}{1 - \alpha - \beta} \cdot \sqrt{\frac{2}{\lambda}} \cdot \sqrt{\text{regret}^{D_{\text{corr}}}_{\ell}(s)},$$

where $C(\pi_{\text{corr}}) = (\pi_{\text{corr}} \cdot (1 - \pi_{\text{corr}}))^{-1}$.

What is special about the BER (and consequently the AUC) that lets us avoid estimation of the corruption parameters? To answer this, we more carefully study the structure of η_{corr} to understand why Equation 4 and 5 coincide, and whether any *other* measures have this property.

Relation to existing work For the special case of CCN learning, Proposition 1 was shown in Blum & Mitchell (1998, Section 5), and for case-controlled PU learning, in (Lee & Liu, 2003; Zhang & Lee, 2008). None of these works established surrogate regret bounds.

4. Corrupted and clean class-probabilities

The equivalence between a specific thresholding of the clean and corrupted class-probabilities (Equations 4 and 5) hints at a relationship between the two functions. We now make this relationship explicit.

Proposition 5. *For any* $D_{M,\eta}$ *and* $\operatorname{Corr}(D, \alpha, \beta, \pi_{\text{corr}})$,

$$(\forall x \in \mathcal{X})\, \eta_{\text{corr}}(x) = T(\alpha, \beta, \pi, \pi_{\text{corr}}, \eta(x)) \quad (9)$$

where, for $\phi\colon z \mapsto \frac{z}{1+z}$, $T(\alpha, \beta, \pi, \pi_{\text{corr}}, t)$ *is given by*

$$\phi\left(\frac{\pi_{\text{corr}}}{1 - \pi_{\text{corr}}} \cdot \frac{(1 - \alpha) \cdot \frac{1-\pi}{\pi} \cdot \frac{t}{1-t} + \alpha}{\beta \cdot \frac{1-\pi}{\pi} \cdot \frac{t}{1-t} + (1 - \beta)}\right). \quad (10)$$

It is evident that η_{corr} is a strictly monotone increasing transform of η. This is useful to study classifiers based on thresholding η, as per Equation 4. Suppose we want a classifier of the form $\operatorname{thresh}(\eta, t)$. The structure of η_{corr} means that this is equivalent to a *corrupted classifier* $\operatorname{thresh}(\eta_{\text{corr}}, T(\alpha, \beta, \pi, \pi_{\text{corr}}, t))$, where the function T (as per Equation 10) tells us how to modify the threshold t on corrupted data. We now make this precise.

Corollary 6. *Pick any* $D_{M,\eta}$ *and* $\operatorname{Corr}(D, \alpha, \beta, \pi_{\text{corr}})$. *Then,* $\forall x \in \mathcal{X}$ *and* $\forall t \in [0, 1]$,

$$\eta(x) > t \iff \eta_{\text{corr}}(x) > T(\alpha, \beta, \pi, \pi_{\text{corr}}, t)$$

where T *is as defined in Equation 10.*

By viewing the minimisation of a general classification measure in light of the above, we now return to the issue of why BER can avoid estimating corruption parameters.

Relation to existing work In PU learning, Proposition 5 has been shown in both the case-controlled (McCullagh & Nelder, 1989, pg. 113), (Phillips et al., 2009; Ward et al., 2009) and censoring settings (Elkan & Noto, 2008, Lemma 1). In CCN learning, Proposition 5 is used in Natarajan et al. (2013, Lemma 7). Corollary 6 is implicit in Scott et al. (2013, Proposition 1), but the explicit form for the corrupted threshold is useful for subsequent analysis.

5. Classification from corrupted data

Consider the problem of optimising a classification measure $\text{Class}^{D}_{\Psi}(f)$ for some $\Psi\colon [0, 1]^3 \to [0, 1]$. For a range of Ψ, the optimal classifier is $f = \operatorname{thresh}(\eta, t^{D}_{\Psi})$ (Koyejo et al., 2014; Narasimhan et al., 2014), for some *optimal threshold* t^{D}_{Ψ}. For example, by Equation 4, the BER-optimal classifier thresholds class-probabilities at the base rate; other examples of such Ψ are those corresponding to misclassification error, and the F-score. But by Corollary 6, $\operatorname{thresh}(\eta, t^{D}_{\Psi}) = \operatorname{thresh}(\eta_{\text{corr}}, t^{D}_{\text{corr},\Psi})$, where

$$t^{D}_{\text{corr},\Psi} = T(\alpha, \beta, \pi, \pi_{\text{corr}}, t^{D}_{\Psi}) \quad (11)$$

is the corresponding *optimal corrupted threshold*. Based on this, we now look at two approaches to minimising $\text{Class}^{D}_{\Psi}(f)$. For the purposes of description, we shall assume that α, β, π are known (or can be estimated). We then study the practically important question of when these approaches can be applied *without* knowledge of α, β, π.

5.1. Classification when t^{D}_{Ψ} is known

Suppose that t^{D}_{Ψ} has some closed-form expression; for example, for misclassification risk, $t^{D}_{\Psi} = 1/2$. Then, there is a simple strategy for minimising Class^{D}_{Ψ}: compute estimates $\hat{\eta}_{\text{corr}}$ of the corrupted class probabilities, and threshold them via $t^{D}_{\text{corr},\Psi}$ computed from Equation 11. Standard cost-sensitive regret bounds may then be invoked. For concreteness, consider the misclassification risk, where plugging in $t^{D}_{\Psi} = 1/2$ into Equation 10 gives

$$t^{D}_{\text{corr},\Psi} = \phi\left(\frac{\pi_{\text{corr}}}{1 - \pi_{\text{corr}}} \cdot \frac{(1 - \alpha) \cdot \frac{1-\pi}{\pi} + \alpha}{\beta \cdot \frac{1-\pi}{\pi} + (1 - \beta)}\right), \quad (12)$$

for $\phi\colon z \mapsto z/(1 + z)$. We have the following.

Proposition 7. *Pick any D and $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$. Let ℓ be a strongly proper composite loss with modulus λ and link function ψ. Then, for any scorer $s \colon \mathcal{X} \to \mathbb{R}$,*

$$\mathrm{regret}^D_{\mathrm{ERR}}(f) \leq \gamma \cdot \sqrt{\frac{2}{\lambda}} \cdot \sqrt{\mathrm{regret}^{D_{\mathrm{corr}}}_\ell(s)},$$

where $f = \mathrm{thresh}(s, \psi(t^D_{\mathrm{corr},\Psi}))$, $t^D_{\mathrm{corr},\Psi}$ is as per Equation 12, and γ is a constant depending on $\alpha, \beta, \pi, \pi_{\mathrm{corr}}$.

5.2. Classification when t^D_Ψ is unknown

For some Ψ, t^D_Ψ does not have a simple closed-form expression, rendering the above approach inapplicable[2]. For example, the optimal threshold for F-score does not have a closed form (Koyejo et al., 2014), and is typically computed by a grid search. In such cases, we can make progress by re-expressing $\mathrm{Class}^D_\Psi(f)$ as an equivalent measure $\mathrm{Class}^{D_{\mathrm{corr}}}_{\Psi_{\mathrm{corr}}}(f)$ on the corrupted distribution, and then tune thresholds on $\hat{\eta}_{\mathrm{corr}}$ to optimise the latter. Here, Ψ_{corr} is *not* the same as Ψ in general, but rather is the result of re-expressing the clean false positive and negative rates in terms of the corrupted ones, as per Scott et al. (2013):

$$\begin{bmatrix} \mathrm{FPR}^D(f) \\ \mathrm{FNR}^D(f) \end{bmatrix} = \begin{bmatrix} 1-\beta & -\beta \\ -\alpha & 1-\alpha \end{bmatrix}^{-1} \begin{bmatrix} \mathrm{FPR}^{D_{\mathrm{corr}}}(f) - \beta \\ \mathrm{FNR}^{D_{\mathrm{corr}}}(f) - \alpha \end{bmatrix}.$$

Thus, for example, for $\Psi \colon (u, v, p) = u$, we would have $\Psi_{\mathrm{corr}} \colon (u, v, p) \mapsto \frac{(1-\alpha)}{1-\alpha-\beta} \cdot (u - \beta) + \frac{\beta}{1-\alpha-\beta} \cdot (v - \alpha)$.

In general, both of the above approaches will require knowledge of α, β, π. For the approach in §5.1, $t^D_{\mathrm{corr},\Psi}$ may clearly depend on these parameters. For the approach in §5.2, the corrupted measure Ψ_{corr} may similarly depend on these parameters, as in the example of $\Psi(u, v, p) = u$. We now provide strong evidence that for both approaches, BER is essentially the only measure that obviates the need for estimation of the corruption parameters.

5.3. BER threshold is uniquely corruption-immune

One way of interpreting the immunity of BER is that the corrupted threshold function (Equation 10) sheds all dependence on α, β, π when instantiated with a threshold of π:

$$(\forall \alpha, \beta, \pi, \pi_{\mathrm{corr}})\, T(\alpha, \beta, \pi, \pi_{\mathrm{corr}}, \pi) = \pi_{\mathrm{corr}}.$$

Is $t \colon \pi \mapsto \pi$ the *only* threshold whose corrupted counterpart does not depend on α, β, π? As stated, the answer is trivially "no"; we can set the corrupted threshold to be any function of π_{corr}, and invert Equation 10 to get an equivalent threshold t for η. However, this t will depend on α, β, and it is unreasonable for the performance measure to depend on the exogenous corruption process. Refining the question to ask whether π is the only threshold independent of α, β such that T is independent of α, β, π, the answer is "yes". We can formalise this as follows.

Proposition 8. *Pick any Ψ. Then, there exists $F \colon (0, 1) \to (0, 1)$ such that Class^D_Ψ has a unique minimiser of the form $x \mapsto \mathrm{sign}(\eta_{\mathrm{corr}}(x) - F(\pi_{\mathrm{corr}}))$ for every D, D_{corr} if and only if $\Psi \colon (u, v, p) \mapsto (u + v)/2$ corresponds to the BER.*

Thus, for measures other than BER which are uniquely optimised by thresholding η[3], we must know one of α, β, π to find the optimal corrupted threshold. But as it is impossible in general to estimate π, it will similarly be impossible to compute this threshold to optimally classify.

While this seems disheartening, two qualifications are in order. First, in the special cases of CCN and PU learning, π *can* be estimated (see §6.2). Second, Proposition 8 is concerned with immunity to *arbitrary* corruption, where α, β, π may be chosen independently. But in special cases where these parameters are tied, other measures may have a threshold independent of these parameters; e.g., in CCN learning, the misclassification error threshold is (Natarajan et al., 2013, Theorem 9)

$$t^D_{\mathrm{corr},\Psi} = \frac{1 - \rho_+ + \rho_-}{2}. \tag{13}$$

So, when $\rho_+ = \rho_-$, $t^D_{\mathrm{corr},\Psi} = \frac{1}{2}$; i.e. *for symmetric label noise, we do not need to know the noise parameters*. Appendix G discusses this issue further.

5.4. BER is uniquely affinely related

Another way of interpreting the immunity of the BER is that, for $\Psi \colon (u, v, p) \mapsto (u + v)/2$, the corresponding corrupted performance measure Ψ_{corr} is simply an affine transformation of Ψ (Proposition 6). Thus, for this measure, $\mathrm{Class}^{D_{\mathrm{corr}}}_{\Psi_{\mathrm{corr}}}$ may be minimised without knowing α, β, π. More generally, we seek Ψ for which there exist f, g such that the corresponding Ψ_{corr} is expressible as

$$\Psi_{\mathrm{corr}}(u, v, p) = f(\alpha, \beta, \pi) \cdot \Psi(u, v, p) + g(\alpha, \beta, \pi). \tag{14}$$

While we do not have a general characterisation of all Ψ satisfying Equation 14, we can show that BER is the only *linear* combination of the false positive and negative rates with an affine relationship between Ψ and Ψ_{corr}. The key is that $(1, 1)$ is the only noise-agnostic eigenvector of the row-stochastic matrix implicit in Equation 2.

Proposition 9. *The set of Ψ of the form $\Psi \colon (u, v, p) \mapsto w_1(p) \cdot u + w_2(p) \cdot v$ where, for every D, D_{corr}, f, $\mathrm{Class}^D_\Psi(f)$ is an affine transformation of $\mathrm{Class}^{D_{\mathrm{corr}}}_\Psi(f)$ is $\{\Psi \colon (u, v, p) \mapsto w(p) \cdot (u + v) \mid w \colon [0, 1] \to \mathbb{R}\}$, corresponding to a scaled version of the BER.*

[2] Recent work has shown how for F-score, we can employ a *series* of thresholds (Parambath et al., 2014); studying this approach in our framework would be of interest.

[3] This rules out degenerate cases such $\Psi \equiv 0$, where there is a *set* of optimal classifiers (i.e. all of them).

In special cases, other Ψ may have such an affine relationship. In the censoring version of PU learning, Lee & Liu (2003) gave one example, the product of Precision and Recall; Appendix G discusses others.

Relation to existing work Scott (2015, Corollary 1) established an analogue of Proposition 7 for CCN learning. Scott et al. (2013) used the approach in §5.2 of rewriting clean in terms of corrupted rates to minimise the minimax risk on D. We are unaware of prior study on conditions where estimation of corruption parameters is unnecessary.

6. Estimating noise rates from corrupted data

We have seen that given estimates of α, β, π, a range of classification measures can be minimised by corrupted class-probability estimation. We now show that under mild assumptions on D, corrupted class-probability estimation lets us estimate α, β, and in special cases, π as well.

6.1. Estimating α, β from η_{corr}

An interesting consequence of Equation 9 is that the range of η_{corr} will be a strict subset of $[0, 1]$ in general. This is because each instance has a nonzero chance of being assigned to either the positive or negative corrupted class; thus, one cannot be *sure* as to its corrupted label.

The precise range of η_{corr} depends on $\alpha, \beta, \pi_{\mathrm{corr}}$, and the range of η. We can thus compute α, β from the range of η_{corr}, with the proviso that we impose the following *weak separability* assumption on D:

$$\inf_{x \in \mathcal{X}} \eta(x) = 0 \text{ and } \sup_{x \in \mathcal{X}} \eta(x) = 1. \tag{15}$$

This does not require D to be separable (i.e. $(\forall x)\, \eta(x) \in \{0, 1\}$), but instead stipulates that *some* instance is "perfectly positive", and another "perfectly negative". This assumption is equivalent to the "mutually irreducible" condition of Scott et al. (2013) (see Appendix H).

Equipped with this assumption, and defining

$$\eta_{\min} = \inf_{x \in \mathcal{X}} \eta_{\mathrm{corr}}(x) \text{ and } \eta_{\max} = \sup_{x \in \mathcal{X}} \eta_{\mathrm{corr}}(x),$$

we can compute the corruption parameters as follows.

Proposition 10. *Pick any $D_{M,\eta}$ satisfying Equation 15. Then, for any* $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$,

$$\begin{aligned} \alpha &= \frac{\eta_{\min} \cdot (\eta_{\max} - \pi_{\mathrm{corr}})}{\pi_{\mathrm{corr}} \cdot (\eta_{\max} - \eta_{\min})} \\ \beta &= \frac{(1 - \eta_{\max}) \cdot (\pi_{\mathrm{corr}} - \eta_{\min})}{(1 - \pi_{\mathrm{corr}}) \cdot (\eta_{\max} - \eta_{\min})}. \end{aligned} \tag{16}$$

The right hand sides above involve quantities that can be estimated given *only corrupted data*. Thus, plugging in estimates of $\hat{\eta}_{\min}, \hat{\eta}_{\max}, \hat{\pi}_{\mathrm{corr}}$ into Equation 16, we obtain estimates $\hat{\alpha}, \hat{\beta}$ of α, β. (Without the weak separability assumption, the right hand sides would depend on the unknown minimal and maximal values of η.)

The formulae for the noise rates simplify in special cases; e.g., in CCN learning (see Appendix D),

$$\rho_+ = 1 - \eta_{\max} \text{ and } \rho_- = \eta_{\min}. \tag{17}$$

Thus, corrupted class-probability estimation gives a simple means of estimating noise rates for CCN problems.

6.2. Estimating π from η_{corr} in special cases

Unlike the general case, in both CCN and PU learning, π may be estimated. This is because in each case, some information about π is present in $(P_{\mathrm{corr}}, Q_{\mathrm{corr}})$ or π_{corr}. For example, in CCN learning (see Appendix E),

$$\pi = \frac{\pi_{\mathrm{corr}} - \eta_{\min}}{\eta_{\max} - \eta_{\min}},$$

while for the case-controlled PU setting,

$$\pi = \frac{\pi_{\mathrm{corr}}}{1 - \pi_{\mathrm{corr}}} \cdot \frac{1 - \eta_{\max}}{\eta_{\max}}.$$

Estimating π may be of inherent interest beyond its use in computing classification thresholds, as e.g. in case-controlled PU learning scenarios, it lets us assess how prevalent a characteristic is in the underlying population.

6.3. Practical considerations

Equation 16 is an asymptotic identity. In practice, we typically employ estimates $\hat{\eta}_{\min}, \hat{\eta}_{\max}$ computed from a finite sample. We note several points related to this estimation.

First, it is crucial that one employs a rich model class (e.g. Gaussian kernel logistic regression, or single-layer neural network with large number of hidden units). With a misspecified model, it is impossible to determine whether the observed range reflects that of η_{corr}, or simply arises from an inability to model η_{corr}. For example, with a linear logistic regression model $\hat{\eta}_{\mathrm{corr}}(x) = \sigma(\langle w, x \rangle + b)$ applied to instances from $\mathbb{R}^d$, our estimated $\hat{\eta}_{\max}$ may be arbitrarily close to 1 *regardless* of α, β. This is because $\hat{\eta}_{\mathrm{corr}}(N \cdot \mathrm{sign}(w)) = \sigma(N||w|| + b) \to 1$ as $N \to \infty$.

Second, when constructing $\hat{\eta}_{\mathrm{corr}}$, one will often have to choose certain hyper-parameters (e.g. strength of regularisation). Motivated by our regret bounds, these can be chosen to yield the best corrupted class-probability estimates $\hat{\eta}_{\mathrm{corr}}$, as measured by some strictly proper loss. Thus, one can tune parameters by cross-validation *on the corrupted data*; clean samples are *not* required.

Third, for statistical purposes, it is ideal to compute $\hat{\eta}_{\min}, \hat{\eta}_{\max}$ from a fresh sample not used for constructing probability estimates $\hat{\eta}_{\mathrm{corr}}$. These range estimates may even be computed on *unlabelled test* instances, as they do not require ground truth labels. (This does not constitute overfitting to the test set, as the underlying model for $\hat{\eta}_{\mathrm{corr}}$ is learned purely from corrupted training data.)

Fourth, the sample maximum and minimum are clearly susceptible to outliers. Therefore, it may be preferable to employ e.g. the 99% and 1% quantiles as a robust alternative. Alternately, one may perform some form of aggregation (e.g. the bootstrap) to smooth the estimates.

Finally, to compute a suitable threshold for classification, noisy estimates of α, β may be sufficient. For example, in CCN learning, we only need the estimated difference $\hat{\rho}_+ - \hat{\rho}_-$ to be comparable to the true difference $\rho_+ - \rho_-$ (by Equation 13). du Plessis et al. (2014) performed such an analysis for the case-controlled PU learning setting.

Relation to existing work The estimator in Equation 16 may be seen as a generalisation of that proposed by Elkan & Noto (2008) for the censoring version of PU learning. For CCN learning, in independent work, Liu & Tao (2014, Theorem 4) proposed the estimators in Equation 17.

Scott et al. (2013) proposed a means of estimating the noise parameters, based on a reduction to the problem of mixture proportion estimation. By an interpretation provided by Blanchard et al. (2010), the noise parameters can be seen as arising from the derivative of the right hand side of the optimal ROC curve on $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$. Sanderson & Scott (2014); Scott (2015) explored a practical estimator along these lines. As the optimal ROC curve for D_{corr} is produced by any strictly monotone transformation of η_{corr}, class-probability estimation is implicit in this approach, and so our estimator is simply based on a different perspective. (See Appendix I.) The class-probability estimation perspective shows that a single approach can both estimate the corruption parameters and be used to classify optimally for a range of performance measures.

7. Experiments

We now present experiments that aim to validate our analysis[4] via three questions. First, can we optimise BER and AUC from corrupted data without knowledge of the noise parameters? Second, can we accurately estimate corruption parameters? Third, can we optimise other classification measures using estimates of corruption parameters?

We focus on CCN learning with label flip probabilities $\rho_+, \rho_- \in \{0, 0.1, 0.2, 0.3, 0.4, 0.49\}$; recall that $\rho_- = 0$ is the censoring version of PU learning. For this problem, a number of approaches have been proposed to answer the third question above, e.g. (Stempfel & Ralaivola, 2007; 2009; Natarajan et al., 2013). To our knowledge, all of these operate in the setting where the noise parameters are *known*. It is thus possible to use the noise estimates from class-probability estimation as inputs to these approaches, and we expect such a fusion will be beneficial. We leave such a study for future work, as our aim here is merely to illustrate that with corrupted class-probability estimation, we can answer all three questions in the affirmative.

We report results on a range of UCI datasets. For each dataset, we construct a random 80% – 20% train-test split. For fixed ρ_+, ρ_-, we inject label noise into the training set. The learner estimates class-probabilities from these noisy samples, with predictions on the clean test samples used to estimate $\hat{\eta}_{\mathrm{min}}, \hat{\eta}_{\mathrm{max}}$ if required. We summarise performance across τ independent corruptions of the training set.

Observe that if $D_{M,\eta}$ can be modelled by a linear scorer, so that $\eta \colon x \mapsto \sigma(\langle w, x \rangle + b)$, then $\eta_{\mathrm{corr}} \colon x \mapsto (1 - \rho_+ - \rho_-) \cdot \sigma(\langle w, x \rangle + b) + \rho_-$; i.e. , a neural network with a single hidden sigmoidal unit, bias term, and identity output link is well-specified. Thus, in all experiments, we use as our base model a neural network with a sigmoidal hidden layer, trained to minimise squared error[5] with ℓ_2 regularisation. The regularisation parameter for the model was tuned by cross-validation (on the *corrupted* data) based on squared error. We emphasise that both learning and parameter tuning is *solely on corrupted data*.

7.1. Are BER and AUC immune to corruption?

We first assess how effectively we can optimise BER and AUC from corrupted data *without* knowledge or estimates of the noise parameters. For a fixed setting of ρ_+, ρ_-, and each of $\tau = 100$ corruption trials, we learn a class-probability estimator from the corrupted training set. We use this to predict class-probabilities for instances on the *clean* test set. We measure the AUC of the resulting class-probabilities, as well as the BER resulting from thresholding these probabilities about the *corrupted* base rate.

Table 2 summarises the results for a selection of datasets and noise rates ρ_+, ρ_-. (Appendix J contains a full set of results.) We see that in general the BER and AUC in the noise-free case ($\rho_+ = \rho_- = 0$) and in the noisy cases are commensurate. This is in agreement with our analysis on the immunity of BER and AUC. For smaller datasets and higher levels of noise, we see a greater degradation in performance. This matches our regret bounds (Proposition 2), which indicated a penalty in high-noise regimes.

[4] Sample scripts are available at `http://users.cecs.anu.edu.au/~akmenon/papers/corrupted-labels/index.html`.

[5] Using log-loss requires explicitly constraining the range of the bias and hidden → output term, else the loss is undefined.

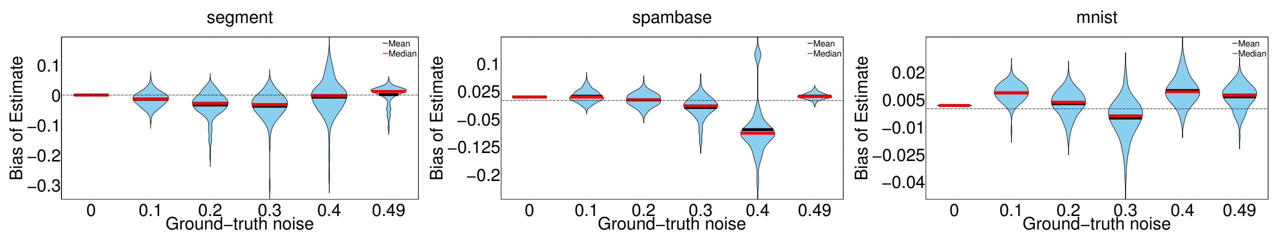

Figure 1. Violin plots of bias in estimate $\hat{\rho}_+$ over $\tau = 100$ trials on Segment (L), Spambase (M) and MNIST (R).

Dataset	**Noise**	1 - **AUC** (%)	**BER** (%)	**ERR**$_{\max}$ (%)	**ERR**$_{\text{oracle}}$ (%)
	None	0.00 ± 0.00	0.00 ± 0.00	0.00 ± 0.00	0.00 ± 0.00
segment	$(\rho_+, \rho_-) = (0.1, 0.0)$	0.00 ± 0.00	0.01 ± 0.00	0.01 ± 0.00	0.01 ± 0.00
	$(\rho_+, \rho_-) = (0.1, 0.2)$	0.02 ± 0.01	0.90 ± 0.08	0.31 ± 0.05	0.30 ± 0.05
	$(\rho_+, \rho_-) = (0.2, 0.4)$	0.03 ± 0.01	3.24 ± 0.20	0.31 ± 0.06	0.27 ± 0.06
	None	2.49 ± 0.00	6.93 ± 0.00	6.52 ± 0.00	6.52 ± 0.00
spambase	$(\rho_+, \rho_-) = (0.1, 0.0)$	2.67 ± 0.02	7.10 ± 0.03	6.88 ± 0.03	6.89 ± 0.03
	$(\rho_+, \rho_-) = (0.1, 0.2)$	3.01 ± 0.03	7.66 ± 0.05	7.51 ± 0.05	7.48 ± 0.05
	$(\rho_+, \rho_-) = (0.2, 0.4)$	4.91 ± 0.09	10.52 ± 0.13	10.82 ± 0.31	10.26 ± 0.12
	None	0.92 ± 0.00	3.63 ± 0.00	3.63 ± 0.00	3.63 ± 0.00
mnist	$(\rho_+, \rho_-) = (0.1, 0.0)$	0.95 ± 0.01	3.56 ± 0.01	3.55 ± 0.01	3.55 ± 0.01
	$(\rho_+, \rho_-) = (0.1, 0.2)$	0.97 ± 0.01	3.63 ± 0.02	3.62 ± 0.02	3.62 ± 0.02
	$(\rho_+, \rho_-) = (0.2, 0.4)$	1.17 ± 0.02	4.06 ± 0.03	4.06 ± 0.03	4.05 ± 0.03

Table 2. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on UCI datasets injected with random label noise $\tau = 100$ times. The case $\rho_- = 0$ corresponds to the censoring version of PU learning. $\text{ERR}_{\max}$ and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

7.2. Can we reliably estimate noise rates?

We now study the viability of learning label flip probabilities ρ_+, ρ_-. As above, we compute corrupted class-probability estimates, and use these to compute label flip probability estimates $\hat{\rho}_+, \hat{\rho}_-$ as per the approach in §6.

Figure 1 presents violin plots (Hintze & Nelson, 1998) of the signed errors in the estimate $\hat{\rho}_+$, for symmetric ground-truth ρ_+, ρ_-, on three of the UCI datasets. (For plots of $\hat{\rho}_-$, see Appendix J.) These plots show the distribution of signed errors across the noise trials; concentration about zero is ideal. For lower noise rates, the estimates are generally only mildly biased, and possess low mean squared error. As previously, we see a greater spread in the error distribution for higher ground-truth noise rates.

7.3. Can other classification measures be minimised?

We finally study the misclassification error[6] of a classifier learned from noisy data. As above, we learn a corrupted class-probability estimator, and compute noise estimates ρ_+, ρ_- as per §6. We then threshold predictions based on Equation 13 to form a classifier. We also include the results of an oracle that has exact knowledge of ρ_+, ρ_-, but only access to the noisy data. The performance of this method illustrates whether increased classification error is due to inexact estimates of ρ_+, ρ_-, or inexact estimates of η_{corr}.

[6]While BER is more apposite on imbalanced data, we simply aim to assess the feasibility of minimising misclassification risk.

Table 2 illustrates that while compared to BER and AUC, we see slightly higher levels of degradation, in general the misclassification rate can be effectively minimised even in high noise regimes. As previously, we find that under higher levels of ground-truth noise, there is in general a slight decrease in accuracy. Interestingly, this is so *even for the oracle estimator*, again corroborating our regret bounds which indicate a penalty in high-noise regimes.

In summary, class-probability estimation lets us both estimate the parameters of the contamination process, as well as minimise a range of classification measures.

8. Conclusion

We have used class-probability estimation to study learning from corrupted binary labels. In particular, we have shown that for optimising the balanced error and AUC, the corruption process may be ignored; given estimates of the corruption parameters, several classification measures can be minimised; and that such estimates may be obtained by the range of the class-probabilities.

In future work, we aim to study the impact of corruption on estimation rates of class-probabilities; study ranking risks beyond the AUC; and study potential extensions of our results to more general corruption problems.

Acknowledgments. NICTA is funded by the Australian Government through the Department of Communications and the Australian Research Council through the ICT Centre of Excellence Program.

References

Agarwal, Shivani. Surrogate regret bounds for bipartite ranking via strongly proper losses. *Journal of Machine Learning Research*, 15:1653–1674, 2014.

Agarwal, Shivani, Graepel, Thore, Herbrich, Ralf, Har-Peled, Sariel, and Roth, Dan. Generalization bounds for the area under the ROC curve. *Journal of Machine Learning Research*, 6:393–425, December 2005.

Angluin, Dana and Laird, Philip. Learning from noisy examples. *Machine Learning*, 2(4):343–370, 1988.

Blanchard, Gilles, Lee, Gyemin, and Scott, Clayton. Semi-supervised novelty detection. *Journal of Machine Learning Research*, 11:2973–3009, December 2010.

Blum, Avrim and Mitchell, Tom. Combining labeled and unlabeled data with co-training. In *Conference on Computational Learning Theory (COLT)*, pp. 92–100, New York, NY, USA, 1998. ACM. ISBN 1-58113-057-0.

Brodersen, Kay H., Ong, Cheng Soon, Stephan, Klaas E., and Buhmann, Joachim M. The balanced accuracy and its posterior distribution. In *Proceedings of the International Conference on Pattern Recognition (ICPR)*, pp. 3121–3124, 2010.

Cheng, Jie, Hatzis, Christos, Hayashi, Hisashi, Krogel, Mark-A., Morishita, Shinchi, Page, David, and Sese, Jun. KDD Cup 2001 report. *ACM SIGKDD Explorations Newsletter*, 3(2):47–64, 2002.

Clémençon, Stéphan, Lugosi, Gábor, and Vayatis, Nicolas. Ranking and Empirical Minimization of U-statistics. *The Annals of Statistics*, 36(2):844–874, April 2008.

Denis, François. PAC learning from positive statistical queries. In *Algorithmic Learning Theory (ALT)*, volume 1501 of *Lecture Notes in Computer Science*, pp. 112–126. Springer Berlin Heidelberg, 1998. ISBN 978-3-540-65013-3.

du Plessis, Marthinus C, Niu, Gang, and Sugiyama, Masashi. Analysis of learning from positive and unlabeled data. In *Advances in Neural Information Processing Systems (NIPS)*, pp. 703–711. Curran Associates, Inc., 2014.

du Plessis, Marthinus Christoffel and Sugiyama, Masashi. Class prior estimation from positive and unlabeled data. *IEICE Transactions*, 97-D(5):1358–1362, 2014.

Elkan, Charles and Noto, Keith. Learning classifiers from only positive and unlabeled data. In *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, pp. 213–220, New York, NY, USA, 2008. ACM. ISBN 978-1-60558-193-4.

Flach, Peter, Hernândez-Orallo, Josè, and Ferri, Cësar. A coherent interpretation of AUC as a measure of aggregated classification performance. In *International Conference on Machine Learning (ICML)*, 2011.

Guyon, Isabelle, Hur, Asa Ben, Gunn, Steve, and Dror, Gideon. Result analysis of the NIPS 2003 feature selection challenge. In *Advances in Neural Information Processing Systems (NIPS)*, pp. 545–552. MIT Press, 2004.

Hintze, Jerry L. and Nelson, Ray D. Violin plots: A box plot-density trace synergism. *The American Statistician*, 52(2):181–184, 1998.

Kotłowski, Wojciech and Dembczyński, Krzysztof. Surrogate regret bounds for generalized classification performance metrics. In *Conference on Learning Theory (COLT)*, 2015.

Koyejo, Oluwasanmi O, Natarajan, Nagarajan, Ravikumar, Pradeep K, and Dhillon, Inderjit S. Consistent binary classification with generalized performance metrics. In *Advances in Neural Information Processing Systems (NIPS)*, pp. 2744–2752. Curran Associates, Inc., 2014.

Krzanowski, Wojtek J. and Hand, David J. *ROC Curves for Continuous Data*. Chapman & Hall/CRC, 1st edition, 2009. ISBN 1439800219, 9781439800218.

Lee, Wee Sun and Liu, Bing. Learning with Positive and Unlabeled Examples Using Weighted Logistic Regression. In *International Conference on Machine Learning (ICML)*, 2003.

Liu, T. and Tao, D. Classification with Noisy Labels by Importance Reweighting. *ArXiv e-prints*, November 2014. URL `http://arxiv.org/abs/1411.7718`.

McCullagh, Peter and Nelder, John Ashworth. *Generalized linear models (Second edition)*. London: Chapman & Hall, 1989.

Menon, Aditya Krishna, Narasimhan, Harikrishna, Agarwal, Shivani, and Chawla, Sanjay. On the statistical consistency of algorithms for binary classification under class imbalance. In *International Conference on Machine Learning (ICML)*, pp. 603–611, 2013.

Narasimhan, Harikrishna, Vaish, Rohit, and Agarwal, Shivani. On the statistical consistency of plug-in classifiers for non-decomposable performance measures. In *Advances in Neural Information Processing Systems (NIPS)*, pp. 1493–1501. Curran Associates, Inc., 2014.

Natarajan, Nagarajan, Dhillon, Inderjit S., Ravikumar, Pradeep D., and Tewari, Ambuj. Learning with noisy labels. In *Advances in Neural Information Processing Systems (NIPS)*, pp. 1196–1204, 2013.

Parambath, Shameem A. Puthiya, Usunier, Nicolas, and Grandvalet, Yves. Optimizing F-measures by cost-sensitive classification. In *Advances in Neural Information Processing Systems (NIPS)*, pp. 2123–2131, 2014.

Phillips, Steven J., Dudik, Miroslav, Elith, Jane, Graham, Catherine H., Lehmann, Anthony, Leathwick, John, and Ferrier, Simon. Sample selection bias and presence-only distribution models: implications for background and pseudo-absence data. *Ecological Applications*, 19 (1):181–197, 2009.

Reid, Mark D. and Williamson, Robert C. Composite binary losses. *Journal of Machine Learning Research*, 11: 2387–2422, December 2010.

Sanderson, Tyler and Scott, Clayton. Class proportion estimation with application to multiclass anomaly rejection. In *AISTATS*, pp. 850–858, 2014.

Scott, Clayton. A rate of convergence for mixture proportion estimation, with application to learning from noisy labels. In *To appear in International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2015.

Scott, Clayton, Blanchard, Gilles, and Handy, Gregory. Classification with asymmetric label noise: Consistency and maximal denoising. In *Conference on Learning Theory (COLT)*, volume 30 of *JMLR Proceedings*, pp. 489–511, 2013.

Stempfel, Guillaume and Ralaivola, Liva. Learning kernel perceptrons on noisy data using random projections. In Hutter, Marcus, Servedio, Rocco., and Takimoto, Eiji (eds.), *Algorithmic Learning Theory*, volume 4754 of *Lecture Notes in Computer Science*, pp. 328–342. Springer Berlin Heidelberg, 2007. ISBN 978-3-540-75224-0.

Stempfel, Guillaume and Ralaivola, Liva. Learning SVMs from sloppily labeled data. In Alippi, Cesare, Polycarpou, Marios, Panayiotou, Christos, and Ellinas, Georgios (eds.), *Artificial Neural Networks (ICANN)*, volume 5768 of *Lecture Notes in Computer Science*, pp. 884–893. Springer Berlin Heidelberg, 2009. ISBN 978-3-642-04273-7.

van Rooyen, Brendan and Williamson, Robert C. Learning in the Presence of Corruption. *ArXiv e-prints*, March 2015. URL http://arxiv.org/abs/1504.00091.

Ward, Gill, Hastie, Trevor, Barry, Simon, Elith, Jane, and Leathwick, John R. Presence-only data and the EM algorithm. *Biometrics*, 65(2):554–563, 2009.

Zhang, Dell and Lee, Wee Sun. Learning classifiers without negative examples: A reduction approach. In *Third International Conference on Digital Information Management (ICDIM)*, pp. 638–643, 2008.

Proofs for "Learning from Corrupted Binary Labels via Class-Probability Estimation"

A. Additional helper results

We collect here some results that are useful for the proofs of results in the main body.

A.1. Basic properties of η_{corr}

Corollary 11. *Pick any $D_{M,\eta}$ and $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$. Then, η_{corr} is a strictly monotone increasing transform of η.*

Proof of Corollary 11. Pick any $f\colon \mathbb{R} \to \mathbb{R}$, and define the function $g : x \mapsto \frac{a \cdot f(x) + b}{c \cdot f(x) + d}$ for $a, b, c, d \geq 0$. If $c = 0$, g is an affine transformation of f, and since $a \geq 0$ it is a strictly monotone increasing transformation of f. If $c \neq 0$, we can rewrite g as

$$\begin{aligned} g\colon x &\mapsto \frac{\frac{a}{c} \cdot c \cdot f(x) + \frac{bc}{a} \cdot \frac{a}{c}}{c \cdot f(x) + d} \\ &= x \mapsto \frac{a}{c} \cdot \frac{c \cdot f(x) + \frac{bc}{a}}{c \cdot f(x) + d} \\ &= x \mapsto \frac{a}{c} \cdot \left(1 + \frac{\frac{bc}{a} - d}{c \cdot f(x) + d} \right) \\ &= x \mapsto \frac{a}{c} + \frac{bc - ad}{ac \cdot f(x) + ad}. \end{aligned}$$

Since $ac \geq 0$, g is a strictly monotone increasing transformation of f when $ad > bc$.

We now apply this to $f(x) = \frac{1-\pi}{\pi} \cdot \frac{\eta(x)}{1-\eta(x)}$, which is in turn a strictly monotone increasing transformation of η. Then, $g = \eta_{\mathrm{corr}}$, where from Equation 9,

$$\begin{aligned} a &= (1 - \alpha) \\ b &= \alpha \\ c &= \beta \\ d &= 1 - \beta. \end{aligned}$$

Thus, $ad - bc = 1 - \alpha - \beta$, which by our assumption that $\alpha + \beta < 1$ is positive. Hence η_{corr} is a strictly monotone increasing transformation of η. □

Corollary 12. *Pick any $D_{M,\eta}$ satisfying Equation 15. Then, for every $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$,*

$$\eta_{\min} = \frac{\pi_{\mathrm{corr}} \cdot \alpha}{1 - \rho} \text{ and } \eta_{\max} = \frac{\pi_{\mathrm{corr}} \cdot (1 - \alpha)}{\rho},$$

where $\rho = \pi_{\mathrm{corr}} \cdot (1 - \alpha) + (1 - \pi_{\mathrm{corr}}) \cdot \beta$.

Proof of Corollary 12. For the ρ as defined, it is easy to check that

$$1 - \rho = \pi_{\mathrm{corr}} \cdot \alpha + (1 - \pi_{\mathrm{corr}}) \cdot (1 - \beta).$$

Plug in $\eta(x) = 0$ into Equation 9, and we get

$$\frac{\eta_{\mathrm{corr}}(x)}{1 - \eta_{\mathrm{corr}}(x)} = \frac{\pi_{\mathrm{corr}}}{1 - \pi_{\mathrm{corr}}} \cdot \frac{\alpha}{1 - \beta},$$

which has solution

$$\eta_{\text{corr}}(x) = \frac{\pi_{\text{corr}} \cdot \alpha}{\pi_{\text{corr}} \cdot \alpha + (1 - \pi_{\text{corr}}) \cdot (1 - \beta)}.$$

Clearly such an x corresponds to the minimum of η, and since η_{corr} is a strictly monotone transformation of η by Corollary 11, it must correspond to the minimum of η_{corr} as well.

Similarly, plug in $\eta(x) = 1$ into Equation 9, and we get

$$\frac{\eta_{\text{corr}}(x)}{1 - \eta_{\text{corr}}(x)} = \frac{\pi_{\text{corr}}}{1 - \pi_{\text{corr}}} \cdot \frac{1 - \alpha}{\beta},$$

which has solution

$$\eta_{\text{corr}}(x) = \frac{\pi_{\text{corr}} \cdot (1 - \alpha)}{\pi_{\text{corr}} \cdot (1 - \alpha) + (1 - \pi_{\text{corr}}) \cdot \beta}.$$

□

Proposition 13. *Let $T \colon [0,1]^5 \to [0,1]$ be as per Equation 10. Suppose $\Delta_{\mathcal{X} \times \{\pm 1\}}$ is the set of all distributions on $\mathcal{X} \times \{\pm 1\}$. The only function $t \colon \Delta_{\mathcal{X} \times \{\pm 1\}} \to [0,1]$ for which*

$$(\exists F \colon [0,1] \to [0,1]) \, (\forall D, D_{\text{corr}}) \, T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(D)) = F(\pi_{\text{corr}})$$

is $t \colon D_{P,Q,\pi} \mapsto \pi$.

Proof of Proposition 13. Let $t(D)$ be some candidate clean threshold function, independent of $\alpha, \beta, \pi_{\text{corr}}$. For convenience, let $\bar{t}(D) = \frac{t(D)}{1 - t(D)}$ and $g(\pi) = \frac{1-\pi}{\pi}$. Recall from Equation 10 that

$$(\forall D, D_{\text{corr}}) \, \frac{T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(D))}{1 - T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(D))} = \frac{\pi_{\text{corr}}}{1 - \pi_{\text{corr}}} \cdot \frac{(1 - \alpha) \cdot g(\pi) \cdot \bar{t}(D) + \alpha}{\beta \cdot g(\pi) \cdot \bar{t}(D) + (1 - \beta)}.$$

We require $T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(D))$ to be equal to $F(\pi_{\text{corr}})$ for some function F, or equivalently, to be independent of α, β, π (as well as any other parameters derived from D). Now, as the left hand side of the above equation is a strictly monotone transformation of $T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(D))$, we equivalently need the right hand side of the above to be independent of α, β, π. As the first term, $\frac{\pi_{\text{corr}}}{1 - \pi_{\text{corr}}}$, depends solely on π_{corr}, we need the second term to be independent of α, β, π. Say the second term equals some function $G(\pi_{\text{corr}})$. Then, we require

$$(\forall D, D_{\text{corr}}) \, (1 - \alpha) \cdot g(\pi) \cdot \bar{t}(D) + \alpha = G(\pi_{\text{corr}}) \cdot (\beta \cdot g(\pi) \cdot \bar{t}(D) + (1 - \beta)).$$

But then, differentiating this with respect to α, we need

$$(\forall D, D_{\text{corr}}) \, - g(\pi) \cdot \bar{t}(D) + 1 = 0,$$

meaning that the only possible solution for $\bar{t}(D)$ is

$$\bar{t}(D) = \frac{1}{g(\pi)},$$

or $t(D) = \pi$.

Suppose we require $T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(D))$ to merely be independent of π, but possibly dependent on α, β. For simplicity, suppose t only depends on π. Then, we equivalently need

$$(\forall \alpha, \beta, \pi) \, (1 - \alpha) \cdot g(\pi) \cdot \bar{t}(\pi) + \alpha = G(\pi_{\text{corr}}, \alpha, \beta) \cdot (\beta \cdot g(\pi) \cdot \bar{t}(\pi) + (1 - \beta))$$

for some function G. Differentiating with respect to π, we get that either $g(\pi) \cdot \bar{t}(\pi)$ is a constant (independent of π), or $G(\pi_{\text{corr}}, \alpha, \beta) = \frac{1-\alpha}{\beta}$. The latter can be ruled out by plugging back into the original equation, and so we find that the admissible threshold functions are

$$\left\{ t \colon \pi \mapsto \frac{c_0 \cdot \pi}{(1 - \pi) + c_0 \cdot \pi} \mid c_0 \in \mathbb{R} \right\}.$$

Clearly $c_0 = 1$ corresponds to $t(\pi) = \pi$, but other thresholds (corresponding to non-standard performance measures) are also possible in this case, e.g. $\frac{2\pi}{1+\pi}$. □

A.2. Contaminated BER and AUC

Corollary 14. *Pick any D and $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$. Then, for any classifier $f \colon \mathcal{X} \to \{\pm 1\}$,*

$$\underset{f \colon \mathcal{X} \to \{\pm 1\}}{\mathrm{Argmin}} \ \mathrm{BER}^{D_{\mathrm{corr}}}(f) = \underset{f \colon \mathcal{X} \to \{\pm 1\}}{\mathrm{Argmin}} \ \mathrm{BER}^{D}(f)$$

and

$$\mathrm{regret}^{D}_{\mathrm{BER}}(f) = \frac{1}{1 - \alpha - \beta} \cdot \mathrm{regret}^{D_{\mathrm{corr}}}_{\mathrm{BER}}(f).$$

Proof of Corollary 14. As the corrupted BER is a positive scaling and translation of the clean BER (Equation 6), the equivalence of minimisers is immediate.

For the regret relation, observe that

$$\begin{aligned}
\mathrm{regret}^{D}_{\mathrm{BER}}(f) &= \mathrm{BER}^{D}(f) - \inf_{g \colon \mathcal{X} \to \{\pm 1\}} \mathrm{BER}^{D}(g) \\
&= \frac{1}{1 - \alpha - \beta} \cdot \left(\mathrm{BER}^{D_{\mathrm{corr}}}(f) - \frac{1}{2} \right) - \inf_{g \colon \mathcal{X} \to \{\pm 1\}} \frac{1}{1 - \alpha - \beta} \cdot \left(\mathrm{BER}^{D_{\mathrm{corr}}}(g) - \frac{1}{2} \right) \\
&= \frac{1}{1 - \alpha - \beta} \cdot \left(\mathrm{BER}^{D_{\mathrm{corr}}}(f) - \inf_{g \colon \mathcal{X} \to \{\pm 1\}} \mathrm{BER}^{D_{\mathrm{corr}}}(g) \right) \\
&= \frac{1}{1 - \alpha - \beta} \cdot \mathrm{regret}^{D_{\mathrm{corr}}}_{\mathrm{BER}}(f).
\end{aligned}$$

□

Corollary 15. *For any D and $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$,*

$$\underset{s \colon \mathcal{X} \to \mathbb{R}}{\mathrm{Argmin}} \, \mathrm{AUC}^{D_{\mathrm{corr}}}(s) = \underset{s \colon \mathcal{X} \to \mathbb{R}}{\mathrm{Argmin}} \, \mathrm{AUC}^{D}(s)$$

and

$$\mathrm{regret}^{D}_{\mathrm{AUC}}(s) = \frac{1}{1 - \alpha - \beta} \cdot \mathrm{regret}^{D_{\mathrm{corr}}}_{\mathrm{AUC}}(s).$$

Proof of Corollary 15. Building on Corollary 3, this follows analogously to the proof of Corollary 14. □

A.3. Contaminated false positive and negative rates

Proposition 16 ((Scott et al., 2013))**.** *Pick any D and $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$. Then, for any classifier $f \colon \mathcal{X} \to \{\pm 1\}$,*

$$\begin{aligned}
\mathrm{FPR}^{D_{\mathrm{corr}}}(f) &= (1 - \beta) \cdot \mathrm{FPR}^{D}(f) - \beta \cdot \mathrm{FNR}^{D}(f) + \beta \\
\mathrm{FNR}^{D_{\mathrm{corr}}}(f) &= -\alpha \cdot \mathrm{FPR}^{D}(f) + (1 - \alpha) \cdot \mathrm{FNR}^{D}(f) + \alpha,
\end{aligned}$$

or equivalently,

$$\begin{aligned}
\mathrm{FPR}^{D}(f) &= \frac{1}{1 - \alpha - \beta} \cdot \left((1 - \alpha) \cdot \mathrm{FPR}^{D_{\mathrm{corr}}}(f) + \beta \cdot \mathrm{FNR}^{D_{\mathrm{corr}}}(f) - \beta \right) \\
\mathrm{FNR}^{D}(f) &= \frac{1}{1 - \alpha - \beta} \cdot \left(\alpha \cdot \mathrm{FPR}^{D_{\mathrm{corr}}}(f) + (1 - \beta) \cdot \mathrm{FNR}^{D_{\mathrm{corr}}}(f) - \alpha \right).
\end{aligned}$$

Proof of Proposition 16. This result essentially appears in Scott et al. (2013), but we find it useful to slightly re-express it here, and so present a rederivation. Observe that

$$\begin{aligned}
\mathrm{FPR}^{D_{\mathrm{corr}}}(f) &= \mathop{\mathbb{E}}_{\mathsf{X} \sim Q_{\mathrm{corr}}} [\![f(\mathsf{X}) = 1]\!] \\
&= \mathop{\mathbb{E}}_{\mathsf{X} \sim \beta P + (1-\beta) Q} [\![f(\mathsf{X}) = 1]\!] \\
&= \beta \cdot \mathop{\mathbb{E}}_{\mathsf{X} \sim P} [\![f(\mathsf{X}) = 1]\!] + (1-\beta) \cdot \mathop{\mathbb{E}}_{\mathsf{X} \sim Q} [\![f(\mathsf{X}) = 1]\!] \\
&= \beta \cdot \mathrm{TPR}^{D}(f) + (1-\beta) \cdot \mathrm{FPR}^{D}(f) \\
&= \beta - \beta \cdot \mathrm{FNR}^{D}(f) + (1-\beta) \cdot \mathrm{FPR}^{D}(f),
\end{aligned}$$

and similarly,

$$\begin{aligned}
\mathrm{FNR}^{D_{\mathrm{corr}}}(f) &= \mathop{\mathbb{E}}_{\mathsf{X} \sim P_{\mathrm{corr}}} [\![f(\mathsf{X}) = -1]\!] \\
&= \mathop{\mathbb{E}}_{\mathsf{X} \sim (1-\alpha) P + \alpha Q} [\![f(\mathsf{X}) = -1]\!] \\
&= (1-\alpha) \cdot \mathop{\mathbb{E}}_{\mathsf{X} \sim P} [\![f(\mathsf{X}) = -1]\!] + \alpha \cdot \mathop{\mathbb{E}}_{\mathsf{X} \sim Q} [\![f(\mathsf{X}) = -1]\!] \\
&= (1-\alpha) \cdot \mathrm{FNR}^{D}(f) + \alpha \cdot \mathrm{TNR}^{D}(f) \\
&= (1-\alpha) \cdot \mathrm{FNR}^{D}(f) + \alpha - \alpha \cdot \mathrm{FPR}^{D}(f).
\end{aligned}$$

This gives the first part of the result. For the second part, write the above as

$$\begin{bmatrix} \mathrm{FPR}^{D_{\mathrm{corr}}}(f) \\ \mathrm{FNR}^{D_{\mathrm{corr}}}(f) \end{bmatrix} = \begin{bmatrix} 1-\beta & -\beta \\ -\alpha & 1-\alpha \end{bmatrix} \begin{bmatrix} \mathrm{FPR}^{D}(f) \\ \mathrm{FNR}^{D}(f) \end{bmatrix} + \begin{bmatrix} \beta \\ \alpha \end{bmatrix}.$$

Inverting this matrix equation gives the second part result. □

Lemma 17. *Pick any D and $\mathrm{Corr}(D, \alpha, \beta, \pi_{\mathrm{corr}})$. Then, for any classifier $f \colon \mathcal{X} \to \{\pm 1\}$,*

$$\mathrm{ERR}^{D}(f) = \gamma \cdot \mathrm{CS}^{D_{\mathrm{corr}}}(f; c) - \frac{\pi \cdot \alpha + (1-\pi) \cdot \beta}{1 - \alpha - \beta},$$

where

$$\begin{aligned}
c &= \phi\left(\frac{\pi_{\mathrm{corr}}}{1 - \pi_{\mathrm{corr}}} \cdot \frac{\pi \cdot \alpha + (1-\pi) \cdot (1-\alpha)}{\pi \cdot (1-\beta) + (1-\pi) \cdot \beta} \right) \\
\gamma &= \frac{1}{1-\alpha-\beta} \cdot \frac{\pi \cdot (1-\rho) + \rho \cdot (1-\pi)}{\pi_{\mathrm{corr}} \cdot (1 - \pi_{\mathrm{corr}})} \\
\rho &= \pi_{\mathrm{corr}} \cdot (1-\alpha) + (1-\pi_{\mathrm{corr}}) \cdot \beta \\
\phi &\colon z \mapsto \frac{z}{1+z}.
\end{aligned}$$

Proof of Lemma 17. From Proposition 16,

$$\begin{aligned}
\pi \cdot \mathrm{FNR}^{D}(f) &= \frac{\pi}{1-\alpha-\beta} \cdot (\alpha \cdot \mathrm{FPR}^{D_{\mathrm{corr}}}(f) + (1-\beta) \cdot \mathrm{FNR}^{D_{\mathrm{corr}}}(f) - \alpha) \\
(1-\pi) \cdot \mathrm{FPR}^{D}(f) &= \frac{1-\pi}{1-\alpha-\beta} \cdot ((1-\alpha) \cdot \mathrm{FPR}^{D_{\mathrm{corr}}}(f) + \beta \cdot \mathrm{FNR}^{D_{\mathrm{corr}}}(f) - \beta),
\end{aligned}$$

and so

$$\mathrm{ERR}^{D}(f) = \frac{\pi \cdot (1-\beta) + (1-\pi) \cdot \beta}{1-\alpha-\beta} \cdot \mathrm{FNR}^{D_{\mathrm{corr}}}(f) + \frac{\pi \cdot \alpha + (1-\pi) \cdot (1-\alpha)}{1-\alpha-\beta} \cdot \mathrm{FPR}^{D_{\mathrm{corr}}}(f) + C,$$

where $C = -\frac{\pi \cdot \alpha + (1-\pi) \cdot \beta}{1-\alpha-\beta}$.

But a performance measure of the form

$$\begin{aligned}
a \cdot \mathrm{FNR}^{D_{\mathrm{corr}}}(f) + b \cdot \mathrm{FPR}^{D_{\mathrm{corr}}}(f) &= \pi_{\mathrm{corr}} \cdot \frac{a}{\pi_{\mathrm{corr}}} \cdot \mathrm{FNR}^{D_{\mathrm{corr}}}(f) + (1 - \pi_{\mathrm{corr}}) \cdot \frac{b}{1 - \pi_{\mathrm{corr}}} \cdot \mathrm{FPR}^{D_{\mathrm{corr}}}(f) \\
&= \left(\frac{a}{\pi_{\mathrm{corr}}} + \frac{b}{1 - \pi_{\mathrm{corr}}} \right) \cdot \mathrm{CS}^{D_{\mathrm{corr}}}(f; c),
\end{aligned}$$

where $c = \frac{b}{1-\pi_{\mathrm{corr}}} \cdot \left(\frac{a}{\pi_{\mathrm{corr}}} + \frac{b}{1-\pi_{\mathrm{corr}}} \right)^{-1}$, and

$$\phi^{-1}(c) = \frac{c}{1-c} = \frac{\pi_{\mathrm{corr}}}{1 - \pi_{\mathrm{corr}}} \cdot \frac{b}{a}.$$

In our case,

$$\begin{aligned}
\gamma &= \frac{a}{\pi_{\mathrm{corr}}} + \frac{b}{1 - \pi_{\mathrm{corr}}} \\
&= \frac{\pi_{\mathrm{corr}} \cdot (b - a) + a}{\pi_{\mathrm{corr}} \cdot (1 - \pi_{\mathrm{corr}})} \\
&= \frac{\pi_{\mathrm{corr}} \cdot (1 - 2\pi) \cdot (1 - \alpha - \beta) + \pi \cdot (1 - \beta) + (1 - \pi) \cdot \beta}{\pi_{\mathrm{corr}} \cdot (1 - \pi_{\mathrm{corr}})} \\
&= \frac{(1 - \pi) \cdot \rho + \pi \cdot (1 - \rho)}{\pi_{\mathrm{corr}} \cdot (1 - \pi_{\mathrm{corr}})}
\end{aligned}$$

and

$$\begin{aligned}
\frac{c}{1-c} &= \frac{\pi_{\mathrm{corr}}}{1 - \pi_{\mathrm{corr}}} \cdot \frac{b}{a} \\
&= \frac{\pi_{\mathrm{corr}}}{1 - \pi_{\mathrm{corr}}} \cdot \frac{\pi \cdot \alpha + (1 - \pi) \cdot (1 - \alpha)}{\pi \cdot (1 - \beta) + (1 - \pi) \cdot \beta}.
\end{aligned}$$

□

A.4. Strongly proper losses

Proposition 18. *Pick any $D_{M,\eta}$. Let ℓ be a strongly proper composite loss with modulus λ. Then, for any $s \colon \mathcal{X} \to \mathbb{R}$,*

$$\mathbb{E}_{\mathsf{X} \sim M} \left[(\eta(\mathsf{X}) - \psi^{-1}(s(\mathsf{X})))^2 \right] \leq \frac{2}{\lambda} \cdot \mathrm{regret}_{\ell}^{D}(s).$$

Proof of Proposition 18. An equivalent definition of ℓ being strongly proper composite with modulus λ is (Agarwal, 2014, Definition 7)

$$(\forall \eta, \hat{\eta} \in [0, 1])\, \mathrm{regret}_{\ell}(\eta, \hat{\eta}) \geq \frac{\lambda}{2} \cdot (\eta - \hat{\eta})^2,$$

where $\mathrm{regret}_{\ell}(\eta, \hat{\eta})$ denotes the conditional regret with respect to loss ℓ, so that

$$\mathrm{regret}_{\ell}^{D}(s) = \mathbb{E}_{\mathsf{X} \sim M} \left[\mathrm{regret}_{\ell}(\eta(\mathsf{X}), \psi^{-1}(s(\mathsf{X})) \right].$$

Therefore,

$$\mathbb{E}_{\mathsf{X} \sim M} \left[(\eta(\mathsf{X}) - \psi^{-1}(s(\mathsf{X})))^2 \right] \leq \frac{2}{\lambda} \cdot \mathrm{regret}_{\ell}^{D}(s).$$

□

A.5. Properties of the AUC and BER

We first show the following simple property of the AUC.

Proposition 19. *Pick any distribution P over $\mathcal{X}$ and scorer $s\colon \mathcal{X} \to \mathbb{R}$. Then,*

$$\mathop{\mathbb{E}}_{\mathsf{X}\sim P, \mathsf{X}'\sim P}\left[[\![s(\mathsf{X}) > s(\mathsf{X}')]\!] + \frac{1}{2} [\![s(\mathsf{X}) = s(\mathsf{X}')]\!] \right] = \frac{1}{2}.$$

Proof. Define a distribution $D = (P, P, \pi)$ over $\mathcal{X} \times \{\pm 1\}$ for some $\pi \in (0, 1)$. Then,

$$\mathrm{AUC}^D(s) = \mathop{\mathbb{E}}_{\mathsf{X}\sim P, \mathsf{X}'\sim P}\left[[\![s(\mathsf{X}) > s(\mathsf{X}')]\!] + \frac{1}{2} [\![s(\mathsf{X}) = s(\mathsf{X}')]\!] \right].$$

By the Neyman-Pearson lemma (Clémençon et al., 2008),

$$\mathop{\mathrm{Argmin}}_{s\colon \mathcal{X}\to\mathbb{R}} 1 - \mathrm{AUC}^D(s) = \{ \phi \circ \eta \mid \phi \text{ strictly monotone increasing } \}.$$

But for two identical class-conditionals, η is just a constant, since

$$(\forall x \in \mathcal{X})\ \frac{\eta(x)}{1 - \eta(x)} = \frac{\pi}{1 - \pi} \cdot \frac{P(x)}{P(x)},$$

or $\eta \equiv \pi$. Therefore,

$$\max_{s\colon \mathcal{X}\to\mathbb{R}} \mathrm{AUC}^D(s) = \mathrm{AUC}^D(\pi) = \frac{1}{2}.$$

Now consider any other scorer $s\colon \mathcal{X} \to \mathbb{R}$. Suppose $\mathrm{AUC}^D(s) < \frac{1}{2}$. Then, define the scorer $\bar{s}\colon x \mapsto -s(x)$. Clearly, $\mathrm{AUC}^D(\bar{s}) = 1 - \mathrm{AUC}^D(s)$. But if $\mathrm{AUC}^D(s) < \frac{1}{2}$, then $\mathrm{AUC}^D(\bar{s}) > \frac{1}{2}$. This contradicts the fact that the maximal achievable AUC is $\frac{1}{2}$. Thus, *every* scorer must attain $\mathrm{AUC}^D(s) = \frac{1}{2}$. ☐

Using the above, we show how the AUC can be seen as the average BER for a specific distribution over classification thresholds. This is implicit in Flach et al. (2011, Theorems 4, 5), but we show the result here for completeness.

Proposition 20. *Pick any $D_{P,Q,\pi}$. Then,*

$$\begin{aligned}\mathrm{AUC}^D(s) &= \frac{3}{2} - 2 \cdot \mathop{\mathbb{E}}_{\mathsf{X}\sim P}\left[\mathrm{BER}^D(s; s(\mathsf{X})) \right] \\ &= \frac{3}{2} - 2 \cdot \mathop{\mathbb{E}}_{\mathsf{X}\sim Q}\left[\mathrm{BER}^D(s; s(\mathsf{X})) \right].\end{aligned}$$

Proof. We use as our starting point the following definition of the AUC (Agarwal et al., 2005):

$$\mathrm{AUC}^D(s) = \mathop{\mathbb{E}}_{\mathsf{X}\sim P, \mathsf{X}'\sim Q}\left[[\![s(\mathsf{X}) > s(\mathsf{X}')]\!] + \frac{1}{2} [\![s(\mathsf{X}) = s(\mathsf{X}')]\!] \right].$$

This can be re-expressed as

$$\mathrm{AUC}^D(s) = \mathop{\mathbb{E}}_{\mathsf{X}\sim P}\left[1 - \mathrm{FPR}^D(s; s(\mathsf{X})) \right],$$

where

$$\mathrm{FPR}^D(s; t) = \mathop{\mathbb{P}}_{\mathsf{X}'\sim Q}\left(s(\mathsf{X}') > t \right) + \frac{1}{2} \cdot \mathop{\mathbb{P}}_{\mathsf{X}\sim Q}\left(s(\mathsf{X}') = t \right),$$

which is equivalent to the false positive rate of a *randomised* classifier that outputs $\mathrm{thresh}(s, t)$ when $s(x) \neq t$, and $\{\pm 1\}$ uniformly at random when $s(x) = t$.

Further, by Proposition 19,

$$\begin{aligned}\mathbb{E}_{\mathsf{X}\sim P}\left[\mathrm{FNR}^D(s;s(\mathsf{X}))\right] &= \mathbb{E}_{\mathsf{X}\sim P,\mathsf{X}'\sim P}\left[[\![s(\mathsf{X}) > s(\mathsf{X}')]\!] + \frac{1}{2}[\![s(\mathsf{X}) = s(\mathsf{X}')]\!]\right] \\ &= \frac{1}{2}.\end{aligned}$$

Thus,

$$\mathbb{E}_{\mathsf{X}\sim P}\left[\frac{\mathrm{FPR}^D(s;s(\mathsf{X})) + \mathrm{FNR}^D(s;s(\mathsf{X}))}{2}\right] = \frac{1 - \mathrm{AUC}^D(s) + \frac{1}{2}}{2},$$

or

$$\mathrm{AUC}^D(s) = \frac{3}{2} - 2\cdot \mathbb{E}_{\mathsf{X}\sim P}\left[\mathrm{BER}^D(s;s(\mathsf{X}))\right].$$

Equivalently, we have

$$\mathrm{AUC}^D(s) = \mathbb{E}_{\mathsf{X}\sim Q}\left[1 - \mathrm{FNR}^D(s;s(\mathsf{X}))\right]$$

and by Proposition 19,

$$\begin{aligned}\mathbb{E}_{\mathsf{X}\sim Q}\left[\mathrm{FPR}^D(s;s(\mathsf{X}))\right] &= \mathbb{E}_{\mathsf{X}\sim Q,\mathsf{X}'\sim Q}\left[[\![s(\mathsf{X}') > s(\mathsf{X})]\!] + \frac{1}{2}[\![s(\mathsf{X}') = s(\mathsf{X})]\!]\right] \\ &= \frac{1}{2}.\end{aligned}$$

Thus,

$$\mathbb{E}_{\mathsf{X}\sim Q}\left[\frac{\mathrm{FPR}^D(s;s(\mathsf{X})) + \mathrm{FNR}^D(s;s(\mathsf{X}))}{2}\right] = \frac{1 - \mathrm{AUC}^D(s) + \frac{1}{2}}{2},$$

or

$$\mathrm{AUC}^D(s) = \frac{3}{2} - 2\cdot \mathbb{E}_{\mathsf{X}\sim Q}\left[\mathrm{BER}^D(s;s(\mathsf{X}))\right].$$

□

Observe that the above implies a special property of the BER.

Corollary 21. *Pick any $D_{P,Q,\pi}$ and scorer $s\colon \mathcal{X} \to \mathbb{R}$. Then,*

$$\mathbb{E}_{\mathsf{X}\sim P}\left[\mathrm{BER}^D(s;s(\mathsf{X}))\right] = \mathbb{E}_{\mathsf{X}\sim Q}\left[\mathrm{BER}^D(s;s(\mathsf{X}))\right].$$

B. Proofs of results in main body

We now present proofs of all results in the main body.

B.1. BER and AUC are immune to corruption

Proof of Proposition 1. Recalling from Proposition 16 that for any classifier $f\colon \mathcal{X} \to \{\pm 1\}$,

$$\begin{aligned}\mathrm{FPR}^D(f) &= \frac{1}{1-\alpha-\beta}\cdot\left((1-\alpha)\cdot\mathrm{FPR}^{D_{\mathrm{corr}}}(f) + \beta\cdot\mathrm{FNR}^{D_{\mathrm{corr}}}(f) - \beta\right)\\ \mathrm{FNR}^D(f) &= \frac{1}{1-\alpha-\beta}\cdot\left(\alpha\cdot\mathrm{FPR}^{D_{\mathrm{corr}}}(f) + (1-\beta)\cdot\mathrm{FNR}^{D_{\mathrm{corr}}}(f) - \alpha\right),\end{aligned}$$

the result follows immediately by definition of the BER as the mean of the false positive and negative rates. □

Proof of Proposition 2. Define $\hat{\eta}_{\mathrm{corr}} \colon x \mapsto \psi^{-1}(s(x))$. For some fixed $c \in (0,1)$, let $f = \mathrm{thresh}(s, \psi(c)) = \mathrm{thresh}(\hat{\eta}_{\mathrm{corr}}, c)$. By Menon et al. (2013, Lemma 4),

$$\mathrm{regret}^{D_{\mathrm{corr}}}_{\mathrm{CS}(c)}(f) \leq \min_{r \geq 1} \left(\mathop{\mathbb{E}}_{\mathsf{X} \sim M_{\mathrm{corr}}} [|\eta_{\mathrm{corr}}(\mathsf{X}) - \hat{\eta}_{\mathrm{corr}}(\mathsf{X})|^r] \right)^{1/r},$$

where $\mathrm{regret}^{D_{\mathrm{corr}}}_{\mathrm{CS}(c)}(f)$ denotes the regret with respect to the cost-sensitive loss with parameter c,

$$\mathrm{CS}(f; c) = \pi \cdot (1 - c) \cdot \mathrm{FNR}^D(f) + (1 - \pi) \cdot c \cdot \mathrm{FPR}^D(f).$$

The BER of f with respect to distribution D_{corr} can be viewed as a scaled version cost-sensitive loss with cost parameter $c = \pi_{\mathrm{corr}}$:

$$\mathrm{BER}^{D_{\mathrm{corr}}}(f) = \frac{1}{2 \cdot \pi_{\mathrm{corr}} \cdot (1 - \pi_{\mathrm{corr}})} \cdot \mathrm{CS}(f; \pi_{\mathrm{corr}}).$$

So, by Corollary 14,

$$\begin{aligned}
\mathrm{regret}^{D}_{\mathrm{BER}}(f) &= \frac{1}{1 - \alpha - \beta} \cdot \mathrm{regret}^{D_{\mathrm{corr}}}_{\mathrm{BER}}(f) \\
&= \frac{1}{1 - \alpha - \beta} \cdot \frac{1}{2 \cdot \pi_{\mathrm{corr}} \cdot (1 - \pi_{\mathrm{corr}})} \cdot \mathrm{regret}^{D_{\mathrm{corr}}}_{\mathrm{CS}(c)}(f) \\
&\leq \frac{1}{1 - \alpha - \beta} \cdot \frac{1}{2 \cdot \pi_{\mathrm{corr}} \cdot (1 - \pi_{\mathrm{corr}})} \cdot \min_{r \geq 1} \left(\mathop{\mathbb{E}}_{\mathsf{X} \sim M_{\mathrm{corr}}} [|\eta_{\mathrm{corr}}(\mathsf{X}) - \hat{\eta}_{\mathrm{corr}}(\mathsf{X})|^r] \right)^{1/r}.
\end{aligned}$$

If ℓ is strongly proper composite with modulus λ, then by Proposition 18,

$$\sqrt{\mathop{\mathbb{E}}_{\mathsf{X} \sim M_{\mathrm{corr}}} [(\eta_{\mathrm{corr}}(\mathsf{X}) - \hat{\eta}_{\mathrm{corr}}(\mathsf{X}))^2]} \leq \sqrt{\frac{2}{\lambda}} \cdot \sqrt{\mathrm{regret}^{D_{\mathrm{corr}}}_{\ell}(s)}.$$

But the left hand side corresponds to the case of $r = 2$ in the above bound, meaning

$$\mathrm{regret}^{D}_{\mathrm{BER}}(f) \leq \frac{C(\pi_{\mathrm{corr}})}{1 - \alpha - \beta} \cdot \sqrt{\frac{2}{\lambda}} \cdot \sqrt{\mathrm{regret}^{D_{\mathrm{corr}}}_{\ell}(s)}.$$

□

Proof of Corollary 3. Using the results of Appendix A.5, we have

$$\begin{aligned}
\mathrm{AUC}^{D_{\mathrm{corr}}}(s) &= \frac{3}{2} - 2 \cdot \mathop{\mathbb{E}}_{\mathsf{X} \sim P_{\mathrm{corr}}} \left[\mathrm{BER}^{D_{\mathrm{corr}}}(s; s(\mathsf{X})) \right] \\
&= \frac{3}{2} - 2 \cdot \mathop{\mathbb{E}}_{\mathsf{X} \sim P_{\mathrm{corr}}} \left[\frac{1}{2} + (1 - \alpha - \beta) \cdot \left(\mathrm{BER}^{D}(s; s(\mathsf{X})) - \frac{1}{2} \right) \right] \\
&= \frac{3}{2} - (\alpha + \beta) - 2 \cdot (1 - \alpha - \beta) \cdot \mathop{\mathbb{E}}_{\mathsf{X} \sim P_{\mathrm{corr}}} \left[\mathrm{BER}^{D}(s; s(\mathsf{X})) \right] \\
&= \frac{1}{2} + (1 - \alpha - \beta) - 2 \cdot (1 - \alpha - \beta) \cdot \left((1 - \alpha) \cdot \mathop{\mathbb{E}}_{\mathsf{X} \sim P} \left[\mathrm{BER}^{D}(s; s(\mathsf{X})) \right] + \alpha \cdot \mathop{\mathbb{E}}_{\mathsf{X} \sim Q} \left[\mathrm{BER}^{D}(s; s(\mathsf{X})) \right] \right) \\
&= \frac{1}{2} + (1 - \alpha - \beta) - 2 \cdot (1 - \alpha - \beta) \cdot \mathop{\mathbb{E}}_{\mathsf{X} \sim P} \left[\mathrm{BER}^{D}(s; s(\mathsf{X})) \right] \\
&= \frac{1}{2} + (1 - \alpha - \beta) + (1 - \alpha - \beta) \cdot \mathrm{AUC}^{D}(s) - \frac{3}{2} \cdot (1 - \alpha - \beta) \\
&= \frac{1}{2} + (1 - \alpha - \beta) \cdot \left(\mathrm{AUC}^{D}(s) - \frac{1}{2} \right).
\end{aligned}$$

□

Proof of Corollary 4. From Corollary 15, we know that

$$\text{regret}^{D}_{\text{AUC}}(s) = \frac{1}{1-\alpha-\beta} \cdot \text{regret}^{D_{\text{corr}}}_{\text{AUC}}(s).$$

Now apply Agarwal (2014, Theorem 13) to the right hand side. ☐

B.2. The corrupted class-probabilities

Proof of Proposition 5. Let p, q denotes the densities of P, Q, and $p_{\text{corr}}, q_{\text{corr}}$ the densities of $P_{\text{corr}}, Q_{\text{corr}}$. By the definition of conditional probability, we have

$$\frac{p(x)}{q(x)} = \frac{1-\pi}{\pi} \cdot \frac{\eta(x)}{1-\eta(x)}.$$

and, on the corrupted distribution,

$$\frac{\eta_{\text{corr}}(x)}{1-\eta_{\text{corr}}(x)} = \frac{\pi_{\text{corr}}}{1-\pi_{\text{corr}}} \cdot \frac{p_{\text{corr}}(x)}{q_{\text{corr}}(x)}.$$

Thus, from Equation 2,

$$\begin{aligned}
(\forall x \in \mathcal{X})\ \frac{\eta_{\text{corr}}(x)}{1-\eta_{\text{corr}}(x)} &= \frac{\pi_{\text{corr}}}{1-\pi_{\text{corr}}} \cdot \frac{(1-\alpha)\cdot p(x) + \alpha \cdot q(x)}{\beta \cdot p(x) + (1-\beta)\cdot q(x)} \\
&= \frac{\pi_{\text{corr}}}{1-\pi_{\text{corr}}} \cdot \frac{(1-\alpha)\cdot \frac{p(x)}{q(x)} + \alpha}{\beta \cdot \frac{p(x)}{q(x)} + (1-\beta)} \\
&= \frac{\pi_{\text{corr}}}{1-\pi_{\text{corr}}} \cdot \frac{(1-\alpha)\cdot \frac{1-\pi}{\pi} \cdot \frac{\eta(x)}{1-\eta(x)} + \alpha}{\beta \cdot \frac{1-\pi}{\pi} \cdot \frac{\eta(x)}{1-\eta(x)} + (1-\beta)}.
\end{aligned}$$

☐

Proof of Corollary 6. This follows from the fact that η_{corr} is a strictly monotone increasing transformation of η (Corollary 11), and plugging in $\eta(x) = t$ into Equation 9. ☐

B.3. Classification from corrupted data

Proof of Proposition 7. Define $\hat{\eta}_{\text{corr}} \colon x \mapsto \psi^{-1}(s(x))$, and let $f = \text{thresh}(\hat{\eta}_{\text{corr}}, t^{D}_{\text{corr},\Psi})$. Now, recall from Lemma 17 that

$$\text{ERR}^{D}(f) = \gamma \cdot \text{CS}^{D_{\text{corr}}}(f; c) - \frac{\pi \cdot \alpha + (1-\pi)\cdot \beta}{1-\alpha-\beta}$$

where the cost parameter $c = t^{D}_{\text{corr},\Psi}$. Thus,

$$\text{regret}^{D}_{\text{ERR}}(f) = \gamma \cdot \text{regret}^{D_{\text{corr}}}_{\text{CS}(c)}(f).$$

The rest of the proof proceeds identically to that of Proposition 2. ☐

Proof of Proposition 8. ($\Longleftarrow$). For Ψ corresponding to the BER, we know from Proposition 1 that this holds for the identity function $F \colon \pi_{\text{corr}} \mapsto \pi_{\text{corr}}$.

($\Longrightarrow$). Suppose Ψ satisfies the desired statement. Since Ψ has a unique minimiser which is a thresholding of η_{corr}, and since η and η_{corr} are strict monotone transformations of each other, we can conclude that for every D, Ψ has a unique minimiser of the form $\text{sign}(\eta(x) - t^{D}_{\Psi})$ for some t^{D}_{Ψ}. By Corollary 6, we have that

$$(\forall D, D_{\text{corr}})\ (\forall x \in \mathcal{X})\ \text{sign}(\eta(x) - t^{D}_{\Psi}) = \text{sign}(\eta_{\text{corr}}(x) - T(\alpha, \beta, \pi, \pi_{\text{corr}}, t^{D}_{\Psi})).$$

Thus, by assumption on the minimiser of Ψ,

$$(\exists F)\ (\forall D, D_{\text{corr}})\ (\forall x \in \mathcal{X})\ \text{sign}(\eta_{\text{corr}}(x) - T(\alpha, \beta, \pi, \pi_{\text{corr}}, t^{D}_{\Psi})) = \text{sign}(\eta_{\text{corr}}(x) - F(\pi_{\text{corr}})).$$

Thus, it must be true that

$$(\exists F)\,(\forall D, D_{\mathrm{corr}})\,F(\pi_{\mathrm{corr}}) = T(\alpha, \beta, \pi, \pi_{\mathrm{corr}}, t^D_\Psi).$$

Now, by Proposition 13, we must have that $t^D_\Psi = \pi$. But this corresponds to the unique optimal threshold for the BER. Hence, Ψ must correspond to the BER. $\square$

Proof of Proposition 9. Given some $w\colon [0,1] \to \mathbb{R}^2_+$, we restrict attention to functions of the form[7]

$$\Psi_w\colon (u, v, p) \mapsto \left\langle w(p), \begin{bmatrix} u \\ v \end{bmatrix} \right\rangle,$$

with corresponding performance measures of the form

$$\mathrm{Class}^D_{\Psi_w}(f) = w_1(\pi) \cdot \mathrm{FPR}^D(f) + w_2(\pi) \cdot \mathrm{FNR}^D(f).$$

We are interested in *admissible* weights w, for which the performance measures on the clean and corrupted distributions are some affine transformation on each other:

$$\begin{aligned} \mathcal{W} &= \{w\colon [0,1] \to \mathbb{R}^2_+ \mid (\forall D)\,(\forall \alpha, \beta, \pi_{\mathrm{corr}})(\exists a, b \in \mathbb{R})\,(\forall f)\,\mathrm{Class}^D_{\Psi_w}(f) = a \cdot \mathrm{Class}^{D_{\mathrm{corr}}}_{\Psi_w}(f) + b\} \\ &= \{w\colon [0,1] \to \mathbb{R}^2_+ \mid (\forall D)\,(\forall \alpha, \beta, \pi_{\mathrm{corr}})(\exists a, b \in \mathbb{R})\,(\forall f)\,\langle w(\pi), x\rangle = a \cdot \langle w(\pi_{\mathrm{corr}}), \bar{x}\rangle + b\}, \end{aligned}$$

where we let $x = \begin{bmatrix} \mathrm{FPR}^D(f) \\ \mathrm{FNR}^D(f) \end{bmatrix}$, and $\bar{x} = \begin{bmatrix} \mathrm{FPR}^{D_{\mathrm{corr}}}(f) \\ \mathrm{FNR}^{D_{\mathrm{corr}}}(f) \end{bmatrix}$. Observe that a, b are allowed to depend on the distribution D, and the corruption process parameters. What is relevant is that they do *not* depend on the classifier f, so that for the purposes of minimising Ψ on D, we can equivalently minimise Ψ on D_{corr}.

Recall from Proposition 16 that, for any D, D_{corr}, f,

$$\begin{bmatrix} \mathrm{FPR}^{D_{\mathrm{corr}}}(f) \\ \mathrm{FNR}^{D_{\mathrm{corr}}}(f) \end{bmatrix} = \begin{bmatrix} 1-\beta & -\beta \\ -\alpha & 1-\alpha \end{bmatrix} \begin{bmatrix} \mathrm{FPR}^D(f) \\ \mathrm{FNR}^D(f) \end{bmatrix} + \begin{bmatrix} \beta \\ \alpha \end{bmatrix},$$

or, in the preceding notation,

$$\bar{x} = Ax + c$$

where

$$\begin{aligned} A &= \begin{bmatrix} 1-\beta & -\beta \\ -\alpha & 1-\alpha \end{bmatrix} \\ c &= \begin{bmatrix} \beta \\ \alpha \end{bmatrix}. \end{aligned}$$

Pick any $w \in {\mathbb{R}^2_+}^{[0,1]}$. Then, we have

$$w \in \mathcal{W} \iff (\forall D_{P,Q,\pi})\,(\forall \alpha, \beta, \pi_{\mathrm{corr}})\,(\exists a, b)\,(\forall f)\,\langle w(\pi), x\rangle = a \cdot \langle w(\pi_{\mathrm{corr}}), Ax + c\rangle + b.$$

As this must hold for every choice of π_{corr}, it must hold for the case $\pi_{\mathrm{corr}} = \pi$, i.e.

$$w \in \mathcal{W} \implies (\forall D_{P,Q,\pi})\,(\forall \alpha, \beta)\,(\exists a, b)\,(\forall f)\,\langle w(\pi), x\rangle = a \cdot \langle w(\pi), Ax + c\rangle + b.$$

For any $\pi \in (0,1)$, we can pick (P, Q) such that D is separable. For a separable D, we can pick a classifier so as to attain *any* combination of false-positive and negative rates (possibly by allowing for randomised classifiers). For $x = \begin{bmatrix} 0 & 0 \end{bmatrix}$, we see that $b = -a \cdot \langle w(\pi), c\rangle$. So,

$$\begin{aligned} w \in \mathcal{W} &\implies (\forall \pi)\,(\forall \alpha, \beta)\,(\exists a)\,(\forall x \in [0,1]^2)\,\langle w(\pi), x\rangle = a \cdot \langle A^T w(\pi), x\rangle \\ &\implies (\forall \pi)\,(\forall \alpha, \beta)\,(\exists a)\,(\forall x \in [0,1]^2)\,\left\langle \left(\frac{1}{a} I - A^T\right) w(\pi), x \right\rangle = 0. \end{aligned}$$

[7]We assume here for simplicity that the performance measure is such that $\Psi(0, 0, p) = 0$; adding any constant to Ψ will trivially leave the following unchanged.

As this must hold for every $x \in [0,1]^2$, this is satisfiable iff the first term is zero, i.e.

$$w \in \mathcal{W} \implies (\forall \pi)\,(\forall \alpha, \beta)\,(\exists a)\, A^T w(\pi) = \frac{1}{a} I w(\pi).$$

This is possible only if $w(\pi)$ is some scaling of an eigenvector of A^T, or is in the nullspace of A^T. But

$$A^T = \begin{bmatrix} 1-\beta & -\alpha \\ -\beta & 1-\alpha \end{bmatrix},$$

which is a scaled row-stochastic matrix. Since $\alpha + \beta \neq 1$, it is invertible and hence has empty nullspace. Its eigenvectors are $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ -\beta/\alpha \end{bmatrix}$. The latter depends on α, β, which is not possible since w does not depend on these parameters. So,

$$\mathcal{W} \subseteq \left\{ w \colon \pi \mapsto \begin{bmatrix} \lambda(\pi) \\ \lambda(\pi) \end{bmatrix} \mid \lambda \colon [0,1] \to \mathbb{R} \right\}.$$

The above is in fact an equality. Pick any $w \colon \pi \mapsto \begin{bmatrix} \lambda(\pi) & \lambda(\pi) \end{bmatrix}^T$. Then, for any D, D_{corr}, and classifier f,

$$\begin{aligned}
\langle w(\pi_{\mathrm{corr}}), Ax + c \rangle &= \lambda(\pi_{\mathrm{corr}}) \cdot \left\langle \begin{bmatrix} 1 \\ 1 \end{bmatrix}, Ax + c \right\rangle \\
&= \lambda(\pi_{\mathrm{corr}}) \cdot \left\langle A^T \begin{bmatrix} 1 \\ 1 \end{bmatrix}, x \right\rangle + \lambda(\pi_{\mathrm{corr}}) \cdot \left\langle \begin{bmatrix} 1 \\ 1 \end{bmatrix}, c \right\rangle \\
&= \lambda(\pi_{\mathrm{corr}}) \cdot (1 - \alpha - \beta) \cdot \left\langle \begin{bmatrix} 1 \\ 1 \end{bmatrix}, x \right\rangle + \lambda(\pi_{\mathrm{corr}}) \cdot \left\langle \begin{bmatrix} 1 \\ 1 \end{bmatrix}, c \right\rangle \\
&= \frac{\lambda(\pi_{\mathrm{corr}})}{\lambda(\pi)} \cdot (1 - \alpha - \beta) \cdot \left\langle \lambda(\pi) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}, x \right\rangle + \lambda(\pi_{\mathrm{corr}}) \cdot \left\langle \begin{bmatrix} 1 \\ 1 \end{bmatrix}, c \right\rangle \\
&= a \cdot \langle w(\pi), x \rangle + b
\end{aligned}$$

for appropriate a, b, so that $w \in \mathcal{W}$. Thus,

$$\mathcal{W} = \left\{ w \colon \pi \mapsto \begin{bmatrix} \lambda(\pi) \\ \lambda(\pi) \end{bmatrix} \mid \lambda \colon [0,1] \to \mathbb{R} \right\}.$$

These correspond to the performance measures

$$\mathrm{Class}_w^D(f) = \lambda(\pi) \cdot (\mathrm{FPR}^D(f) + \mathrm{FNR}^D(f)) = 2\lambda(\pi) \cdot \mathrm{BER}^D(f),$$

meaning that the set of admissible functionals is the set of scalings and translations of balanced error. □

B.4. Learning noise rates

Proof of Proposition 10. From Corollary 12,

$$\begin{aligned}
\eta_{\min} &= \frac{\pi_{\mathrm{corr}} \cdot \alpha}{\pi_{\mathrm{corr}} \cdot \alpha + (1 - \pi_{\mathrm{corr}}) \cdot (1 - \beta)} \\
\eta_{\max} &= \frac{\pi_{\mathrm{corr}} \cdot (1 - \alpha)}{\pi_{\mathrm{corr}} \cdot (1 - \alpha) + (1 - \pi_{\mathrm{corr}}) \cdot \beta}.
\end{aligned}$$

Rearranging,

$$\begin{aligned}
\pi_{\mathrm{corr}} \cdot (1 - \eta_{\min}) \cdot \alpha + (1 - \pi_{\mathrm{corr}}) \cdot \eta_{\min} \cdot \beta &= (1 - \pi_{\mathrm{corr}}) \cdot \eta_{\min} \\
\pi_{\mathrm{corr}} \cdot (1 - \eta_{\max}) \cdot \alpha + (1 - \pi_{\mathrm{corr}}) \cdot \eta_{\max} \cdot \beta &= \pi_{\mathrm{corr}} \cdot (1 - \eta_{\max}).
\end{aligned}$$

In matrix form,

$$A \cdot \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} (1 - \pi_{\mathrm{corr}}) \cdot \eta_{\min} \\ \pi_{\mathrm{corr}} \cdot (1 - \eta_{\max}) \end{bmatrix}$$

where

$$\begin{aligned} A &= \begin{bmatrix} \pi_{\text{corr}} \cdot (1 - \eta_{\text{min}}) & (1 - \pi_{\text{corr}}) \cdot \eta_{\text{min}} \\ \pi_{\text{corr}} \cdot (1 - \eta_{\text{max}}) & (1 - \pi_{\text{corr}}) \cdot \eta_{\text{max}} \end{bmatrix} \\ &= \begin{bmatrix} 1 - \eta_{\text{min}} & \eta_{\text{min}} \\ 1 - \eta_{\text{max}} & \eta_{\text{max}} \end{bmatrix} \cdot \begin{bmatrix} \pi_{\text{corr}} & 0 \\ 0 & 1 - \pi_{\text{corr}} \end{bmatrix}. \end{aligned}$$

It is apparent that

$$A^{-1} = \begin{bmatrix} \pi_{\text{corr}}^{-1} & 0 \\ 0 & (1 - \pi_{\text{corr}})^{-1} \end{bmatrix} \cdot \frac{1}{\eta_{\text{max}} - \eta_{\text{min}}} \cdot \begin{bmatrix} \eta_{\text{max}} & -\eta_{\text{min}} \\ -(1 - \eta_{\text{max}}) & 1 - \eta_{\text{min}} \end{bmatrix}$$

Hence,

$$\begin{aligned} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} &= A^{-1} \cdot \begin{bmatrix} (1 - \pi_{\text{corr}}) \cdot \eta_{\text{min}} \\ \pi_{\text{corr}} \cdot (1 - \eta_{\text{max}}) \end{bmatrix} \\ &= \frac{1}{\eta_{\text{max}} - \eta_{\text{min}}} \cdot \begin{bmatrix} \pi_{\text{corr}}^{-1} & 0 \\ 0 & (1 - \pi_{\text{corr}})^{-1} \end{bmatrix} \cdot \begin{bmatrix} \eta_{\text{max}} & -\eta_{\text{min}} \\ -(1 - \eta_{\text{max}}) & 1 - \eta_{\text{min}} \end{bmatrix} \cdot \begin{bmatrix} (1 - \pi_{\text{corr}}) \cdot \eta_{\text{min}} \\ \pi_{\text{corr}} \cdot (1 - \eta_{\text{max}}) \end{bmatrix} \\ &= \frac{1}{\eta_{\text{max}} - \eta_{\text{min}}} \cdot \begin{bmatrix} \pi_{\text{corr}}^{-1} & 0 \\ 0 & (1 - \pi_{\text{corr}})^{-1} \end{bmatrix} \cdot \begin{bmatrix} (1 - \pi_{\text{corr}}) \cdot \eta_{\text{max}} \cdot \eta_{\text{min}} - \pi_{\text{corr}} \cdot \eta_{\text{min}} \cdot (1 - \eta_{\text{max}}) \\ -(1 - \pi_{\text{corr}}) \cdot \eta_{\text{min}} \cdot (1 - \eta_{\text{max}}) + \pi_{\text{corr}} \cdot (1 - \eta_{\text{min}}) \cdot (1 - \eta_{\text{max}}) \end{bmatrix} \\ &= \frac{1}{\eta_{\text{max}} - \eta_{\text{min}}} \cdot \begin{bmatrix} \pi_{\text{corr}}^{-1} & 0 \\ 0 & (1 - \pi_{\text{corr}})^{-1} \end{bmatrix} \cdot \begin{bmatrix} \eta_{\text{min}} \cdot (\eta_{\text{max}} - \pi_{\text{corr}}) \\ (1 - \eta_{\text{max}}) \cdot (\pi_{\text{corr}} - \eta_{\text{min}}) \end{bmatrix}. \end{aligned}$$

Thus,

$$\begin{aligned} \alpha &= \frac{\eta_{\text{min}} \cdot (\eta_{\text{max}} - \pi_{\text{corr}})}{\pi_{\text{corr}} \cdot (\eta_{\text{max}} - \eta_{\text{min}})} \\ \beta &= \frac{(1 - \eta_{\text{max}}) \cdot (\pi_{\text{corr}} - \eta_{\text{min}})}{(1 - \pi_{\text{corr}}) \cdot (\eta_{\text{max}} - \eta_{\text{min}})}. \end{aligned}$$

$\square$

Additional Discussion for "Learning from Corrupted Binary Labels via Class-Probability Estimation"

C. Derivation of special cases of MC learning

We now show the precise settings of $\alpha, \beta, \pi_{\mathrm{corr}}$ that recover CCN and PU learning as special cases of MC learning.

C.1. CCN learning

The problem of learning with class-conditional label noise is the following (Blum & Mitchell, 1998; Natarajan et al., 2013). We imagine drawing $(\mathsf{X}, \mathsf{Y}) \sim D$. The instance X is unchanged: however, the label is altered such that positive samples have labels flipped with probability ρ_+, while negative samples have labels flipped with probability ρ_-. We will refer to the resulting distribution by $\mathrm{CCN}(D, \rho_+, \rho_-)$. It is apparent that the noise process leaves the marginal distribution of instances, M, unchanged. However, all other quantities are distinct from their counterparts in D. From the definition of CCN learning, the form of the class-probability function is apparent. This result appears in the proof of Natarajan et al. (2013, Lemma 7).

Proposition 22. *Pick any $D_{P,Q,\pi}$. Denote the class-probability function of $\mathrm{CCN}(D, \rho_+, \rho_-)$ by*

$$\eta_{\mathrm{corr}} : x \mapsto \mathbb{P}(\mathsf{Z} = 1 | \mathsf{X} = x).$$

Then,

$$(\forall x \in \mathcal{X})\, \eta_{\mathrm{corr}}(x) = (1 - \rho_+ - \rho_-) \cdot \eta(x) + \rho_-. \tag{18}$$

Proof of Proposition 22. Let (X, Y) denote random variables distributed according to D. Let Z denote the noisy label. By definition of the noise process,

$$\begin{aligned}(\forall x \in \mathcal{X})\, \mathbb{P}(\mathsf{Z} = 1 | \mathsf{X} = x) &= \mathbb{P}(\mathsf{Z} = 1 | \mathsf{Y} = 1) \cdot \mathbb{P}(\mathsf{Y} = 1 | \mathsf{X} = x) + \mathbb{P}(\mathsf{Z} = 1 | \mathsf{Y} = -1) \cdot \mathbb{P}(\mathsf{Y} = -1 | \mathsf{X} = x) \\ &= (1 - \rho_+) \cdot \eta(x) + \rho_- \cdot (1 - \eta(x)) \\ &= (1 - \rho_+ - \rho_-) \cdot \eta(x) + \rho_-.\end{aligned}$$

□

From this, one can also relate the base rate π_{corr} to the noise parameters ρ_+, ρ_-.

Corollary 23. *Pick any $D_{P,Q,\pi}$. Then, $\mathrm{CCN}(D, \rho_+, \rho_-)$ has base rate*

$$\pi_{\mathrm{corr}} = \pi \cdot (1 - \rho_+ - \rho_-) + \rho_-.$$

Proof of Corollary 23. Take the expectation of Equation 18 over $\mathsf{X} \sim M$, and use the fact that $\mathbb{E}_{\mathsf{X} \sim M}[\eta(\mathsf{X})] = \pi$. □

Now observe that

$$\begin{aligned}(\forall x \in \mathcal{X})\, P_{\mathrm{corr}}(x) &= \frac{M(x) \cdot \eta_{\mathrm{corr}}(x)}{\pi_{\mathrm{corr}}} \\ &= \frac{M(x) \cdot ((1 - \rho_+ - \rho_-) \cdot \eta(x) + \rho_-)}{\pi \cdot (1 - \rho_+ - \rho_-) + \rho_-} \\ &= \frac{M(x) \cdot (1 - \rho_+ - \rho_-) \cdot \eta(x) + M(x) \cdot \rho_-}{\pi \cdot (1 - \rho_+ - \rho_-) + \rho_-} \\ &= \frac{\pi \cdot (1 - \rho_+ - \rho_-) \cdot P(x) + \pi \cdot \rho_- \cdot P(x) + (1 - \pi) \cdot \rho_- \cdot Q(x)}{\pi \cdot (1 - \rho_+ - \rho_-) + \rho_-} \\ &= \frac{\pi \cdot (1 - \rho_+ - \rho_-) + \pi \cdot \rho_-}{\pi \cdot (1 - \rho_+ - \rho_-) + \rho_-} \cdot P(x) + \frac{(1 - \pi) \cdot \rho_-}{\pi \cdot (1 - \rho_+ - \rho_-) + \rho_-} \cdot Q(x),\end{aligned}$$

Quantity	CCN Learning
$\mathbb{P}(\mathsf{Z}=1)$	$\pi \cdot (1-\rho_+ - \rho_-) + \rho_-$
P_{corr}	$(1-\alpha) \cdot P + \alpha \cdot Q$
Q_{corr}	$\beta \cdot P + (1-\beta) \cdot Q$
M_{corr}	M
$\eta_{\mathrm{corr}}(x)$	$(1-\rho_+ - \rho_-) \cdot \eta(x) + \rho_-$

Table 3. Summary of marginal and condition densities for CCN learning. Here, α, β are as defined in Equation 19.

so that the noisy class-conditional is a mixture of the clean class-conditionals. A similar calculation for Q_{corr} reveals that the distribution $\mathrm{CCN}(D, \rho_+, \rho_-)$ is, unsurprisingly, a special case of an MC learning distribution, with noise parameters

$$\begin{aligned} \alpha &= \frac{(1-\pi) \cdot \rho_-}{\pi \cdot (1-\rho_+) + (1-\pi) \cdot \rho_-} \\ \beta &= \frac{\pi \cdot \rho_+}{\pi \cdot \rho_+ + (1-\pi) \cdot (1-\rho_-)}. \end{aligned} \tag{19}$$

That is,

$$\mathrm{CCN}(D, \rho_+, \rho_-) = \mathrm{Corr}(D, \alpha, \beta, \pi \cdot (1-\rho_+ - \rho_-) + \rho_-).$$

Table 3 summarises some properties of this distribution.

C.2. PU learning

There are two variants of the PU learning problem, both of which are special cases of MC learning.

In *case-controlled PU learning* (Ward et al., 2009), we see samples from a distribution $\mathrm{PU}_{\mathrm{case}}(D, \pi_{\mathrm{corr}})$, for some base rate $\pi_{\mathrm{corr}} \in (0,1)$. Here, positive instances are drawn from the true class-conditional P, and unlabelled instances are drawn from the true marginal M. The base rate π_{corr} specifies the fraction of positive to unlabelled samples, which is in general unrelated to the clean base rate π. Since our observed samples have class-conditionals (P, M), drawn with base rate π, it is evident that

$$\mathrm{PU}_{\mathrm{case}}(D, \pi_{\mathrm{corr}}) = \mathrm{Corr}(D, 0, \pi, \pi_{\mathrm{corr}}).$$

The class-probability function may thus be written as

$$\begin{aligned} (\forall x \in \mathcal{X})\, \eta_{\mathrm{corr}}(x) &= \frac{\pi_{\mathrm{corr}} \cdot \eta(x)}{\pi \cdot (1-\pi_{\mathrm{corr}}) + \pi_{\mathrm{corr}} \cdot \eta(x)} \\ &= \sigma\left(\log(\eta(x)) + \sigma^{-1}(\pi_{\mathrm{corr}}) - \log \pi\right), \end{aligned}$$

where $\sigma \colon x \mapsto 1/(1+\exp(-x))$ is the sigmoid function.

In *censored PU learning* (Denis, 1998; Lee & Liu, 2003; Elkan & Noto, 2008), we see samples from a distribution $\mathrm{PU}_{\mathrm{cen}}(D, c)$, for some censoring parameter $c \in (0,1)$. Here, positive instances are drawn from the true class-conditional P, while unlabelled distances are drawn from a distribution defined by a censoring process, wherein one (conceptually) draws a sample from the true D, but then conceals the labels of any negative samples with certainty, and conceals the label of an positive sample with probability $1-c$. The censoring process may be understood as a special case of CCN learning, where there is no noise on the negatives (i.e. no negative is accidentally labelled as positive), but there is noise rate $1-c$ on the positives (so that some positives are accidentally labelled as negative). That is,

$$\begin{aligned} \mathrm{PU}_{\mathrm{cen}}(D, c) &= \mathrm{CCN}(D, 1-c, 0) \\ &= \mathrm{Corr}\left(D, 0, \frac{\pi \cdot (1-c)}{1-c \cdot \pi}, c \cdot \pi\right). \end{aligned}$$

Quantity	Case controlled	Censoring
$\mathbb{P}(\mathsf{Z}=1)$	π_{corr}	$c \cdot \pi$
P_{corr}	P	P
Q_{corr}	M	$\frac{\pi \cdot (1-c)}{1-c\cdot\pi} \cdot P + \frac{1-\pi}{1-c\cdot\pi} \cdot Q$
M_{corr}	$\rho \cdot P + (1-\rho) \cdot Q$	M
$\eta_{\mathrm{corr}}(x)$	$\sigma(\log(\eta(x)) + \sigma^{-1}(\pi_{\mathrm{corr}}) - \log \pi)$	$c \cdot \eta(x)$

Table 4. Summary of marginal and condition densities for $\mathrm{PU}_{\mathrm{case}}(D, \pi_{\mathrm{corr}})$ and $\mathrm{PU}_{\mathrm{cen}}\,(D, c)$. Here, $\rho = \pi_{\mathrm{corr}} \cdot (1-\pi) + \pi$.

The connection to CCN learning means that, for example,

$$(\forall x \in \mathcal{X})\, \eta_{\mathrm{corr}}(x) = c \cdot \eta(x).$$

We see that both settings are special cases of MC learning where the positive class contamination rate $\alpha = 0$. However, the censoring setting involves a choice of corrupted base rate that depends on the noise parameter β. (This is just a consequence of this setting being a special case of CCN learning.) Interestingly, the case controlled setting is *not* a special case of CCN learning in general, because it involves an arbitrary corrupted base rate π_{corr}.

Table 4 summarises the properties of the distributions for each setting.

D. Estimates for noise rates special cases

We have seen how corruption parameters can be estimated in general. We now see how these simplify for the special cases discussed earlier. While these all can be derived directly from Equation 16, it is simpler (and illustrative) to build on our earlier expressions for η_{corr} in each case.

D.1. CCN learning

Recall that

$$\eta_{\mathrm{corr}} \colon x \mapsto (1 - \rho_+ - \rho_-) \cdot \eta(x) + \rho_-.$$

Thus, any x for which $\eta(x) = 0$ will have $\eta_{\mathrm{corr}}(x) = \rho_-$, and if $\eta(x) = 1$, $\eta_{\mathrm{corr}}(x) = 1 - \rho_+$. Since these correspond to the minimum and maximum of η, and thus η_{corr}, we have

$$\rho_+ = 1 - \eta_{\mathrm{max}} \text{ and } \rho_- = \eta_{\mathrm{min}}.$$

D.2. PU learning

In PU learning, we know that $\alpha = 0$. Therefore, we only need an estimate for the contamination rate β. In the case-controlled setting, recall that $\beta = \pi$. But we have

$$\begin{aligned}\eta_{\mathrm{max}} &= \frac{\pi_{\mathrm{corr}}}{\pi_{\mathrm{corr}} + (1 - \pi_{\mathrm{corr}}) \cdot \pi} \\ &= \frac{\pi_{\mathrm{corr}}}{\pi_{\mathrm{corr}} + (1 - \pi_{\mathrm{corr}}) \cdot \beta}.\end{aligned}$$

which may be inverted to give

$$\beta = \frac{\pi_{\mathrm{corr}}}{1 - \pi_{\mathrm{corr}}} \cdot \frac{1 - \eta_{\mathrm{max}}}{\eta_{\mathrm{max}}}.$$

In the censoring setting, building on the result for CCN learning,

$$1 - c = 1 - \eta_{\mathrm{max}},$$

or

$$c = \eta_{\max}.$$

This is precisely one of the estimators proposed by Elkan & Noto (2008).

E. Estimates for π in special cases

We show how π can be estimated in each of the special cases discussed earlier.

E.1. CCN learning

In the CCN learning scenario, we have

$$\pi = \frac{\pi_{\text{corr}} - \rho_-}{1 - \rho_+ - \rho_-}.$$

That is, the base rate contains information about π, unlike the general MC learning problem. Using the estimates for ρ_+, ρ_- from earlier, we can thus estimate π from η_{corr} as

$$\pi = \frac{\pi_{\text{corr}} - \eta_{\min}}{\eta_{\max} - \eta_{\min}}.$$

E.2. PU learning

In the case-controlled scenario, we have $\alpha = 0$ and $\beta = \pi$. Therefore, estimating β is equivalent to estimating π. Recalling our earlier estimate for β, we have

$$\pi = \frac{\pi_{\text{corr}}}{1 - \pi_{\text{corr}}} \cdot \frac{1 - \eta_{\max}}{\eta_{\max}}.$$

This does not contradict Ward et al. (2009, Proposition 7), which states that π is unidentifiable when using linear logistic regression to model an arbitrary η (i.e. when using a misspecified model). This reiterates the importance of our assumption of a suitably rich function class, as well as the weak separability assumption D.

In the censoring scenario, using the result for CCN learning, we have the following, which is mentioned in Elkan & Noto (2008, Section 3):

$$\pi = \frac{\pi_{\text{corr}}}{\eta_{\max}}.$$

F. Thresholds for misclassification error in special cases

The optimal corrupted threshold for the misclassification error simplifies in the special cases discussed earlier.

F.1. CCN learning

From the definition of η_{corr}, it is apparent that

$$(\forall x \in \mathcal{X})\, \eta(x) > t \iff \eta_{\text{corr}}(x) > (1 - \rho_+ - \rho_-) \cdot t + \rho_-.$$

Setting $t = \frac{1}{2}$,

$$(\forall x \in \mathcal{X})\, \eta(x) > \frac{1}{2} \iff \eta_{\text{corr}}(x) > \frac{1 - \rho_+ + \rho_-}{2}.$$

It is apparent that the only choice of noise rates for which the contaminated threshold is a constant is $\rho_+ = \rho_-$, i.e. the symmetric noise case.

F.2. PU learning

In the case-controlled setting, from the definition of η_{corr}, it is apparent that

$$(\forall x \in \mathcal{X})\, \eta(x) > t \iff \eta_{\text{corr}}(x) > \frac{\pi_{\text{corr}} \cdot t}{\pi_{\text{corr}} \cdot t + (1 - \pi_{\text{corr}}) \cdot \pi}.$$

Setting $t = \frac{1}{2}$,

$$(\forall x \in \mathcal{X})\, \eta(x) > \frac{1}{2} \iff \eta_{\text{corr}}(x) > \frac{\pi_{\text{corr}}}{\pi_{\text{corr}} + 2 \cdot (1 - \pi_{\text{corr}}) \cdot \pi}.$$

Recall that π can be expressed in terms of π_{corr} and $\eta_{\max}$. Plugging this in, we find

$$(\forall x \in \mathcal{X})\, \eta(x) > \frac{1}{2} \iff \eta_{\text{corr}}(x) > \frac{\eta_{\max}}{2 - \eta_{\max}}.$$

In general this is not a constant, and we cannot avoid the estimation of $\eta_{\max}$.

In the censoring setting, plugging in $\rho_+ = 1 - c$ and $\rho_- = 0$ into the CCN formula,

$$(\forall x \in \mathcal{X})\, \eta(x) > \frac{1}{2} \iff \eta_{\text{corr}}(x) > \frac{c}{2}.$$

It is apparent that we thus *always* need to estimate the censoring rate in order to optimally threshold. This also follows from the fact that the problem is a form of asymmetric label noise, which we saw above yields a non-constant corrupted threshold.

G. Noise immunity in special cases

We study whether in special cases, there are performance measures other than BER that are immune to corruption.

G.1. CCN learning

For CCN learning with arbitrary label noise, as before, we consider a clean threshold function $t(\pi)$ on η such that the corresponding contaminated threshold $T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(\pi))$ depends only on π_{corr} (i.e. is independent of ρ_+, ρ_-, π). As in the general case, the only such threshold is $t(\pi) = \pi$.

Proposition 24. *For CCN learning with arbitrary label noise, the only function $t(\pi)$ for which $T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(\pi))$ is independent of ρ_+, ρ_-, π is $t(\pi) = \pi$, i.e. the optimal threshold for BER.*

Proof. From the definition of η_{corr}, it is apparent that

$$T(\alpha, \beta, \pi, \pi_{\text{corr}}, t) = (1 - \rho_+ - \rho_-) \cdot t + \rho_-.$$

For noise-immunity, we want the corrupted threshold to be some function of π_{corr} (and thus independent of ρ_+, ρ_-, π) when given a clean threshold $t(\pi)$. Recall that $\pi_{\text{corr}} = (1 - \rho_+ - \rho_-) \cdot \pi + \rho_-$ is itself a function of ρ_+, ρ_-, π. So, we are interested in all choices of clean threshold $t(\pi)$ such that

$$(\forall \rho_+, \rho_-, \pi)\, (1 - \rho_+ - \rho_-) \cdot t(\pi) + \rho_- = F((1 - \rho_+ - \rho_-) \cdot \pi + \rho_-)$$

for some function F.

Plug in $\pi = 0$ in the above and we get

$$(\forall \rho_+, \rho_-)\, \rho_- = F(\rho_-).$$

That is, the only feasible choice of F is the identity function. Thus,

$$(\forall \rho_+, \rho_-, \pi)\, (1 - \rho_+ - \rho_-) \cdot t(\pi) + \rho_- = (1 - \rho_+ - \rho_-) \cdot \pi + \rho_-,$$

or

$$(\forall \rho_+, \rho_-, \pi)\, (1 - \rho_+ - \rho_-) \cdot (t(\pi) - \pi) = 0.$$

Fix any ρ_+, ρ_- such that $\rho_+ + \rho_- \neq 1$, and we need

$$(\forall \pi)\, t(\pi) - \pi = 0.$$

$\square$

In the symmetric label noise case, however, there is a broader class of functions $t(\pi)$ such that the corresponding contaminated threshold sheds dependence on ρ_+, ρ_-, π.

Proposition 25. *For CCN learning with symmetric label noise, the set of functions $t(\pi)$ for which $T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(\pi))$ is independent of ρ_+, ρ_-, π is*

$$\{t \colon \pi \mapsto (1 - c_0) \cdot \pi + c_0 \cdot (1 - \pi) \mid c_0 \in [0, 1]\}.$$

Proof. Here, we have

$$T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(\pi)) = (1 - 2\rho_+) \cdot t(\pi) + \rho_+$$

and $\pi_{\text{corr}} = (1 - 2\rho_+) \cdot \pi + \rho_+$. As before, we want there to exist some function F such that

$$(\forall \rho_+, \pi)\, (1 - 2\rho_+) \cdot t(\pi) + \rho_+ = F((1 - 2\rho_+) \cdot \pi + \rho_+)$$

Plug in $\pi = 0$ as before, and we get

$$(\forall \rho_+)\, F(\rho_+) = (1 - 2t(0)) \cdot \rho_+ + t(0).$$

Therefore, we need

$$(\forall \rho_+, \pi)\, (1 - 2\rho_+) \cdot t(\pi) + \rho_+ = (1 - 2t(0)) \cdot ((1 - 2\rho_+) \cdot \pi + \rho_+) + t(0)$$

or

$$(\forall \rho_+, \pi)\, (1 - 2\rho_+) \cdot (t(\pi) - (1 - 2t(0)) \cdot \pi - t(0)) = 0.$$

As before, pick any $\rho_+ \neq \frac{1}{2}$ and we find

$$(\forall \pi)\, t(\pi) = (1 - 2t(0)) \cdot \pi + t(0).$$

Let $c_0 := t(0)$ and we get

$$(\forall \pi)\, t(\pi) = (1 - c_0) \cdot \pi + c_0 \cdot (1 - \pi).$$

Clearly $c_0 = 0$ corresponds to $t(\pi) = \pi$, as before. However, we can also set $c_0 = \frac{1}{2}$ and get $t(\pi) = \frac{1}{2}$, corresponding to the optimal threshold for misclassification risk. For other choices of c_0 we get less obviously interpretable, but still immune thresholds e.g. $t(\pi) = \frac{2\pi+1}{4}$. □

G.2. PU learning

For case-controlled PU learning, recall that $\alpha = 0$, while $\beta = \pi$. Thus, there is no restriction per se on the clean threshold t, which may freely depend on π and hence β. It turns out that, like the symmetric label noise setting, there are a range of clean thresholds for which the corresponding contaminated threshold is independent of π.

Proposition 26. *For case-controlled PU learning, the set of functions $t(\pi)$ for which $T(\alpha, \beta, \pi, \pi_{\text{corr}}, t(\pi))$ is independent of π is*

$$\{t \colon \pi \mapsto c_0 \cdot \pi \mid c_0 \in \mathbb{R} - \{0\}\}.$$

Proof. In the case-controlled setting, from the definition of η_{corr}, it is apparent that

$$\begin{aligned} T(\alpha, \beta, \pi, \pi_{\text{corr}}, t) &= \frac{\pi_{\text{corr}} \cdot t}{\pi_{\text{corr}} \cdot t + (1 - \pi_{\text{corr}}) \cdot \pi} \\ &= \frac{1}{1 + \frac{(1 - \pi_{\text{corr}}) \cdot \pi}{\pi_{\text{corr}} \cdot t}}. \end{aligned}$$

Let $\bar{T}(\pi, \pi_{\text{corr}}) = \frac{1 - \pi_{\text{corr}}}{\pi_{\text{corr}}} \cdot \frac{\pi}{t(\pi)}$. Recall that π_{corr} is chosen independent of π in this setting. Thus, we simply need

$$(\forall \pi, \pi_{\text{corr}})\, \bar{T}(\pi_{\text{corr}}, \pi) = F(\pi_{\text{corr}})$$

for some function F. Since $\bar{T}$ decomposes into a product of one function of π_{corr} and another function of π, we clearly need the second function to evaluate to a constant. This requires $t(\pi) = c_0 \cdot \pi$ for some constant $c_0 \neq 0$. Setting $c_0 = 1$, we get the BER-optimal threshold $t(\pi) = \pi$. For other choices of the constant, we get thresholds corresponding to functionals of the form

$$\pi \cdot (1 - c_0 \cdot \pi) \cdot \mathrm{FPR}^D(f) + (1 - \pi) \cdot c_0 \cdot \pi \cdot \mathrm{FNR}^D(f).$$

$\square$

Recall that the censoring setting is a special case of CCN learning with asymmetric label noise. Thus, from the previous results, we see that the only clean threshold that does not require estimating the censoring parameter is $t(\pi) = \pi$. As noted in the body, a qualification is in order, which we now discuss.

G.3. When do performance measure equivalences hold in the censoring setting?

We show that for the purposes of minimising a performance measure on the clean distribution, it is possible to have a corrupted threshold that depends on the corruption parameters, *but* that we can nonetheless estimate this threshold without having to estimate the corruption parameters. We do this by operating in the censoring version of PU learning, which simplifies a lot of the analysis. Consider

$$\Psi \colon (u, v, p) \mapsto \frac{(1 - y)^2}{p \cdot (1 - y) + (1 - p) \cdot x}, \tag{20}$$

so that

$$\mathrm{Class}_\Psi^D(f) = \frac{(\mathrm{TPR}^D(f))^2}{\pi \cdot \mathrm{TPR}^D(f) + (1 - \pi) \cdot \mathrm{FPR}^D(f)}.$$

The denominator is subtly different from the misclassification risk, and in fact is simply $\mathbb{P}_{\mathsf{X} \sim M}(f(\mathsf{X}) = 1)$. Lee & Liu (2003) showed that, in the censoring setting,

$$\mathrm{Class}_\Psi^D(f) = \mathrm{Class}_\Psi^{\mathrm{PU}_{\mathrm{cen}}(D,c)}(f). \tag{21}$$

This is apparent since the marginal distributions of instances is unchanged in the censoring setting, so that the denominators coincide; further, the numerators also coincide in the censoring setting, since $P_{\mathrm{corr}} = P$. Of interest is that the left hand side is independent of c; this implies that the performance measure on the corrupted distribution *can be evaluated without knowledge of the corruption parameters*.

Let t_Ψ^D denote the optimal clean threshold for $\mathrm{Class}_\Psi^D(f)$. Now, we know that the optimal corrupted threshold is

$$t_{\mathrm{corr},\Psi}^D = c \cdot t_\Psi^D,$$

which clearly depends on the corruption parameter c. Ostensibly, then, thresholding η_{corr} requires that we estimate this parameter. But this is not true: we can simply define

$$t_{\mathrm{corr},\Psi}^D = \operatorname*{argmin}_{t \in [0,1]} \mathrm{Class}_\Psi^{\mathrm{PU}_{\mathrm{cen}}(D,c)}(\mathrm{thresh}(\eta_{\mathrm{corr}}, t)),$$

where the performance measure, as we saw earlier, does not depend on the corruption parameter. While the *result* of the minimisation will depend on c, *performing* the minimisation does not require knowledge of this parameter.

In the censoring setting, we can characterise all smooth functions Ψ that satisfy Equation 21. Observe that

$$\mathrm{Class}^{\mathrm{PU}_{\mathrm{cen}}(D,c)}(f) = \Psi\left(\frac{1 - p}{1 - c \cdot p}\mathrm{FPR}^D(f) + \left(1 - \frac{1 - p}{1 - c \cdot p}\right)(1 - \mathrm{FNR}^D(f)), \mathrm{FNR}^D(f), c \cdot \pi\right).$$

Thus, we need all solutions to the functional equation

$$\Psi(x, y, p) = \Psi\left(\frac{1 - p}{1 - c \cdot p}x + \left(1 - \frac{1 - p}{1 - c \cdot p}\right)y, y, c \cdot p\right),$$

where we will instantiate $x = \mathrm{FPR}^D(f), y = \mathrm{TPR}^D(f), p = \pi$.

For brevity, denote $\bar{x} = \frac{1-p}{1-c \cdot p} x + \left(1 - \frac{1-p}{1-c \cdot p}\right) y$. Differentiating the above with respect to c, we find

$$\begin{aligned} 0 &= \frac{\partial \Psi}{\partial x}(\bar{x}, y, p) \cdot \frac{\partial \bar{x}}{\partial c} + \frac{\partial \Psi}{\partial p}(\bar{x}, y, p) \cdot p \\ &= \frac{\partial \Psi}{\partial x}(\bar{x}, y, p) \cdot \frac{p(1-p)}{(1 - c \cdot p)^2} \cdot (x - y) + \frac{\partial \Psi}{\partial p}(\bar{x}, y, p) \cdot p. \end{aligned}$$

Let $c = 1$. Then, we need

$$0 = \frac{\partial \Psi}{\partial x}(x, y, p) \cdot \frac{p}{1-p} \cdot (x - y) + \frac{\partial \Psi}{\partial p}(x, y, p) \cdot p.$$

This can be shown (via MATHEMATICA) to have the solutions of the form

$$\{\Psi \colon (x, y, p) \mapsto f(y, (1-p) \cdot x + p \cdot y) \mid f \colon \mathbb{R}^2 \to \mathbb{R}\},$$

i.e. the only possible solutions are functions of $\mathrm{TPR}^D(f)$ and $\mathbb{P}_{\mathsf{X} \sim M}(f(\mathsf{X}) = 1)$. This includes the performance measure of Equation 20, as expected. The family includes the following scaled version of balanced error,

$$\mathrm{Class}_\Psi^D(f) = (1 - \pi) \cdot \mathrm{BER}^D(f),$$

but this does not satisfy the equation as stated, due to the presence of an additional translation term. In general, we need to solve

$$\mathrm{Class}^{\mathrm{PU}_{\mathrm{cen}}(D,c)}(f) = A(c) \cdot \Psi\left(\frac{1-p}{1-c \cdot p}\mathrm{FPR}^D(f) + \left(1 - \frac{1-p}{1-c \cdot p}\right)(1 - \mathrm{FNR}^D(f)), \mathrm{FNR}^D(f), c \cdot \pi\right) + B(c),$$

which can again be shown (via MATHEMATICA) to have the solutions of the form

$$\{\Psi \colon (x, y, p) \mapsto p^{-A'(1)/A(1)} \cdot f(y, (1-p) \cdot x + p \cdot y) - B'(1) \mid f \colon \mathbb{R}^2 \to \mathbb{R}\}.$$

That is, scaling by π is permitted: this is because we can always write $c = \frac{\pi_{\mathrm{corr}}}{\pi}$, and use this to define a suitable A.

H. Mutually irreducible and weakly separable distributions

Scott et al. (2013) assumed that the clean distribution $D_{P,Q,\pi}$ had class-conditionals P, Q mutually irreducible in the sense that, if they have densities p, q

$$\inf_{x \in \mathcal{X}} \frac{p(x)}{q(x)} = \inf_{x \in \mathcal{X}} \frac{q(x)}{p(x)} = 0.$$

This is equivalent to our weak separability assumption (Equation 15). By Bayes' rule,

$$(\forall x \in \mathcal{X})\, \frac{p(x)}{q(x)} = \frac{\pi}{1-\pi} \cdot \frac{\eta(x)}{1 - \eta(x)}.$$

Thus, if $\pi \in (0, 1)$,

$$\begin{aligned} \inf_{x \in \mathcal{X}} \frac{p(x)}{q(x)} = 0 &\iff \inf_{x \in \mathcal{X}} \eta(x) = 0, \\ \inf_{x \in \mathcal{X}} \frac{q(x)}{p(x)} = 0 &\iff \inf_{x \in \mathcal{X}} (1 - \eta(x)) = 0 \iff \sup_{x \in \mathcal{X}} \eta(x) = 1. \end{aligned}$$

I. Relating the ROC and class-probability estimators

For brevity, let $\bar{P} = P_{\mathrm{corr}}, \bar{Q} = Q_{\mathrm{corr}}$, and denote the corresponding densities by $\bar{p}, \bar{q}$. Scott et al. (2013, Proposition 3) established the following identities for the noise rates:

$$\begin{aligned} \alpha &= \frac{\nu^*(\bar{P}, \bar{Q}) \cdot (1 - \nu^*(\bar{Q}, \bar{P}))}{1 - \nu^*(\bar{P}, \bar{Q}) \cdot \nu^*(\bar{Q}, \bar{P})} \\ \beta &= \frac{\nu^*(\bar{Q}, \bar{P}) \cdot (1 - \nu^*(\bar{P}, \bar{Q}))}{1 - \nu^*(\bar{P}, \bar{Q}) \cdot \nu^*(\bar{Q}, \bar{P})}, \end{aligned}$$

where

$$\nu^*(\bar{P}, \bar{Q}) = \inf_{x \in \mathcal{X}} \frac{\bar{p}(x)}{\bar{q}(x)}.$$

Scott et al. (2013) then proposed to use plugin estimates of $\nu^*(\bar{P}, \bar{Q})$ and $\nu^*(\bar{Q}, \bar{P})$ to estimate α, β from a finite sample.

Now, by (Blanchard et al., 2010, 6.2), we can interpret $\nu^*(\bar{P}, \bar{Q})$ as the left-derivative of the optimal ROC curve for $(\bar{P}, \bar{Q})$ at the right endpoint. By Krzanowski & Hand (2009, pg. 22), the derivative of this optimal ROC curve at the right endpoint is

$$\nu^*(\bar{P}, \bar{Q}) = \frac{1 - \pi_{\text{corr}}}{\pi_{\text{corr}}} \cdot \frac{(\text{FPR}^{D_{\text{corr}}}_{\eta_{\text{corr}}})^{-1}(1)}{1 - (\text{FPR}^{D_{\text{corr}}}_{\eta_{\text{corr}}})^{-1}(1)}.$$

Now,

$$\text{FPR}^{D_{\text{corr}}}_{\eta_{\text{corr}}}(t) = \mathbb{P}_{\mathsf{X} \sim \bar{Q}}(\eta_{\text{corr}}(\mathsf{X}) > t),$$

and so $(\text{FPR}^{D_{\text{corr}}}_{\eta_{\text{corr}}})^{-1}(1) = \eta_{\min}$. Thus,

$$\nu^*(\bar{P}, \bar{Q}) = \frac{1 - \pi_{\text{corr}}}{\pi_{\text{corr}}} \cdot \frac{\eta_{\min}}{1 - \eta_{\min}}.$$

Similarly, for $\nu^*(\bar{Q}, \bar{P})$, we have the same as the above except the roles of the two classes are swapped. Thus, we just swap the base rates and work with $1 - \eta_{\text{corr}}$, giving

$$\nu^*(\bar{P}, \bar{Q}) = \frac{\pi_{\text{corr}}}{1 - \pi_{\text{corr}}} \cdot \frac{1 - \eta_{\max}}{\eta_{\max}}.$$

We then have

$$\begin{aligned} 1 - \nu^*(\bar{P}, \bar{Q})) &= 1 - \frac{1 - \pi_{\text{corr}}}{\pi_{\text{corr}}} \cdot \frac{\eta_{\min}}{1 - \eta_{\min}} \\ &= \frac{\pi_{\text{corr}} - \eta_{\min}}{\pi_{\text{corr}} \cdot (1 - \eta_{\min})}, \end{aligned}$$

and

$$\begin{aligned} 1 - \nu^*(\bar{P}, \bar{Q})) \cdot \nu^*(\bar{Q}, \bar{P}) &= 1 - \frac{\eta_{\min} \cdot (1 - \eta_{\max})}{\eta_{\max} \cdot (1 - \eta_{\min})} \\ &= \frac{\eta_{\max} - \eta_{\min}}{\eta_{\max} \cdot (1 - \eta_{\min})}. \end{aligned}$$

Thus,

$$\begin{aligned} \beta &= \frac{\nu^*(\bar{Q}, \bar{P}) \cdot (1 - \nu^*(\bar{P}, \bar{Q}))}{1 - \nu^*(\bar{P}, \bar{Q}) \cdot \nu^*(\bar{Q}, \bar{P})} \\ &= \nu^*(\bar{Q}, \bar{P}) \cdot \frac{\pi_{\text{corr}} - \eta_{\min}}{\pi_{\text{corr}}} \cdot \frac{\eta_{\max}}{\eta_{\max} - \eta_{\min}} \\ &= \frac{(1 - \eta_{\max}) \cdot (\pi_{\text{corr}} - \eta_{\min})}{(1 - \pi_{\text{corr}}) \cdot (\eta_{\max} - \eta_{\min})}, \end{aligned}$$

and similarly for α. Thus, the two estimators rely on the same identities for the noise rates.

Observe that to estimate the derivative of the right-hand side of the optimal ROC curve, a natural strategy is to produce this curve first. This optimal ROC curve is produced by a scorer that is any strictly monotone transformation of η_{corr}, by the Neyman-Pearson lemma (Clémençon et al., 2008). Therefore, class-probability estimation is one way by which to use the ROC-based estimator.

Additional Experiments for "Learning from Corrupted Binary Labels via Class-Probability Estimation"

J. Additional experimental results

We present results assessing the quality of our noise estimates, and the performance of the resulting classifier, on a range of UCI datasets (Table 5). For the MNIST 3v8 data, we perform PCA to reduce the feature space to $D = 50$ dimensions.

Dataset	N	D	$\mathbb{P}(\mathsf{Y} = 1)$
Housing	506	13	0.0692
Car	1,728	8	0.0376
Image	2,086	18	0.5695
Segment	2,310	19	0.1429
Splice	3,190	61	0.2404
Spambase	4,601	57	0.3940
Optdigits	5,620	64	0.0986
Thyroid	7,200	21	0.0231
Pendigits	10,992	16	0.0960
MNIST 3v8	13,966	784	0.4887
Letter	20,000	16	0.0367
Covtype-Binary	38,501	54	0.0713
KDDCup98	191,779	15	0.0507

Table 5. Summary of UCI datasets. Here, N denotes the total number of samples, and D the dimensionality of the feature space. Many of these datasets are seen to be imbalanced.

J.1. Results of noise estimation on synthetic data

It is illustrative to study the results of our noise estimator on synthetic data. Following Natarajan et al. (2013) we consider a linearly separable 2D distribution where instances $x = (x_1, x_2) \in \mathbb{R}^2$ are drawn uniformly from the subset of $[0, 1]^2$ that is the complement of $\{(x_1, x_2) \in [0, 1]^2 \mid |x_1 - x_2| < 0.5\}$. Further, the class-probability function is $\eta(x) = [\![x_2 > x_1 + 0.5]\!]$. Figure 2 illustrates a draw from this distribution.

We know that the weak (indeed, full) separability assumption holds on the synthetic distribution, so it serves as a suitable sanity check. We consider the CCN learning setting with label flip probabilities $\rho_+, \rho_- \in \{0, 0.1, 0.2, 0.3, 0.4\}$. Recall that in CCN learning, our estimators for the label flip probabilities are

$$\rho_+ = 1 - \eta_{\max} \text{ and } \rho_- = \eta_{\min}.$$

As previously, we consider a fixed 80% – 20% train–test split of the data. We assess the performance of our noise estimators across $\tau = 500$ corruption trials. We consider draws of N training samples from this distribution, where $N \in \{500, 1000, 2000, 3000\}$. For each such N, and each random corruption trial, we compute label flip probability estimates $\hat{\rho}_+, \hat{\rho}_-$. For learning, we used a capped sigmoid model of the form $\hat{\eta}_{\text{corr}} : x \mapsto u + v \cdot \sigma(\langle w, x \rangle + b)$.

To evaluate our noise estimates, we present histograms across all τ trials, and also consider the mean squared error (MSE) to the ground truth values. For the histograms, we would like to observe a unimodal distribution that is not badly biased, with concentration about the mode. Our use of MSE is simply in keeping with prior work on evaluating estimates of

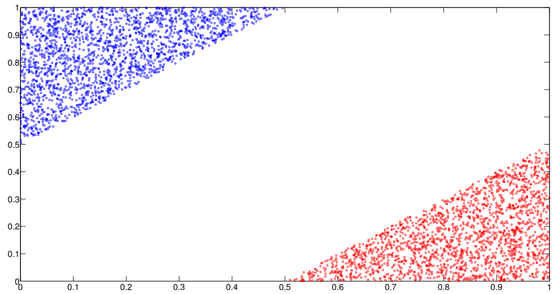

Figure 2. Synthetic 2D dataset. Blue (red) coloured points indicate positive (negative) examples.

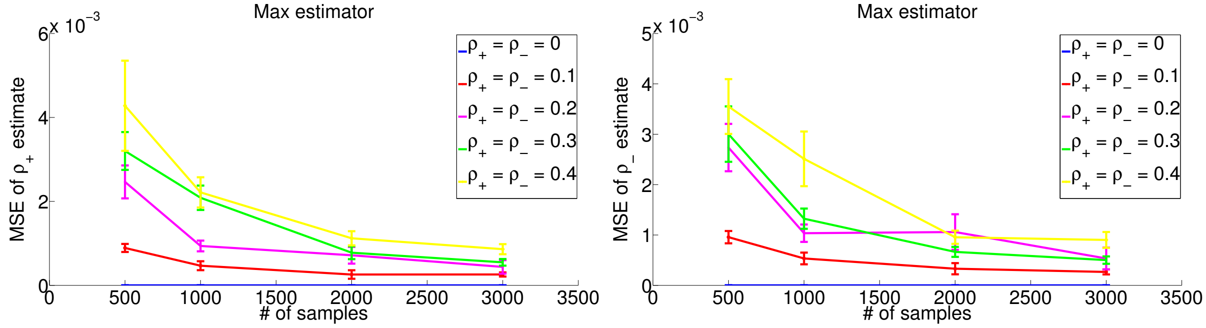

Figure 3. MSE in estimates of ρ_+ (L) and ρ_- (R), synthetic dataset.

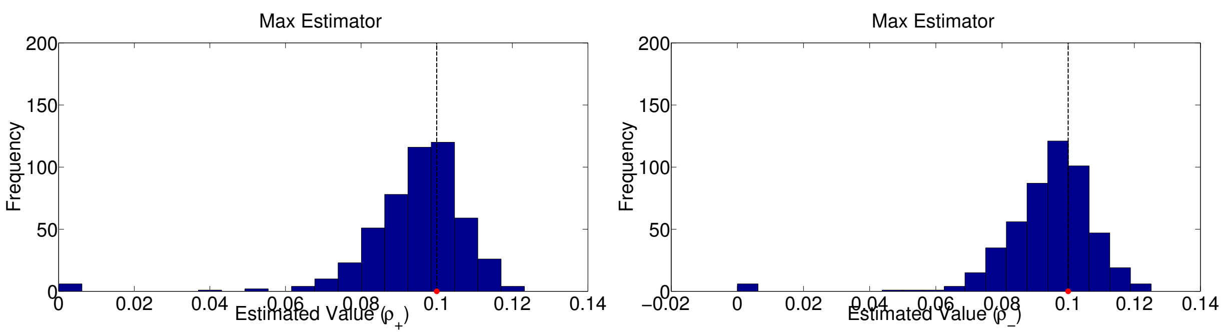

Figure 4. Histogram of estimates for ρ_+ (L) and ρ_- (R) over $\tau = 500$ trials, synthetic dataset with $N = 3000$ examples.

corruption parameters, e.g. du Plessis & Sugiyama (2014) in the PU learning setting.

Figure 3 summarises the MSE in the estimates $\hat{\rho}_+, \hat{\rho}_-$ as the number of training samples N varies, and for various choices of ground-truth ρ_+, ρ_-. We find that for all choices of ground-truth ρ_+, ρ_-, the MSE decreases given more samples. We also find that for higher noise rates, there is higher MSE given fewer number of samples. In all cases the MSE of the estimates is low, indicating accurate recovery of the noise rates. Figure 4 shows the histogram of estimates of ρ_+, ρ_- for the setting $\rho_+ = \rho_- = 0.1$ and $N = 3000$. We see that the distribution is unimodal, with concentration about the mode.

J.2. Violin plots of noise estimates

We present violin plots of the estimates $\hat{\rho}_+, \hat{\rho}_-$ for all datasets and symmetric ground-truth in Figures 5 – 17. We see that the trend for the two quantities is largely similar. Generally, poor estimation can be attributed to either the dataset having too few training examples (e.g. Car), and (or) not satisfying the weak separability assumption, as evidenced by a bias in the estimates even in the noise-free case (e.g. Letter).

With very high noise rate ($\rho_+ = \rho_- = 0.49$), generally the bias in the estimate is low. This can be attributed to the fact that in such regimes, it is difficult to learn a discriminative classifier except with a very large number of samples.

We find that on some datasets, while there is concentration of the estimates close to the expected value, there are occasional outliers (e.g. Splice). These can potentially be smoothened out by some form of training set averaging, such as the bootstrap; we plan to explore this in future work.

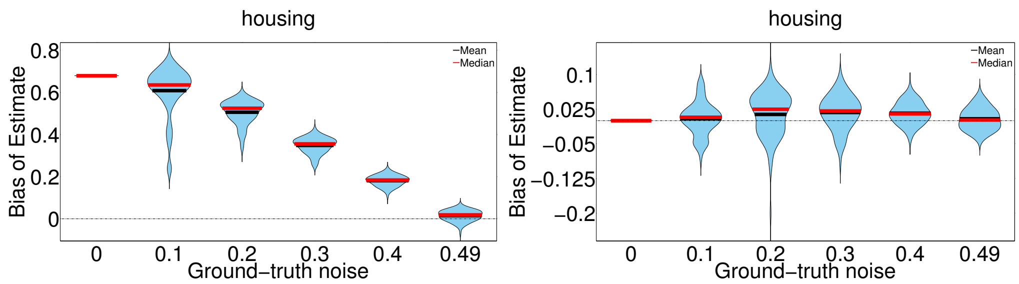

Figure 5. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `housing`. (Note the different axes on the plots.)

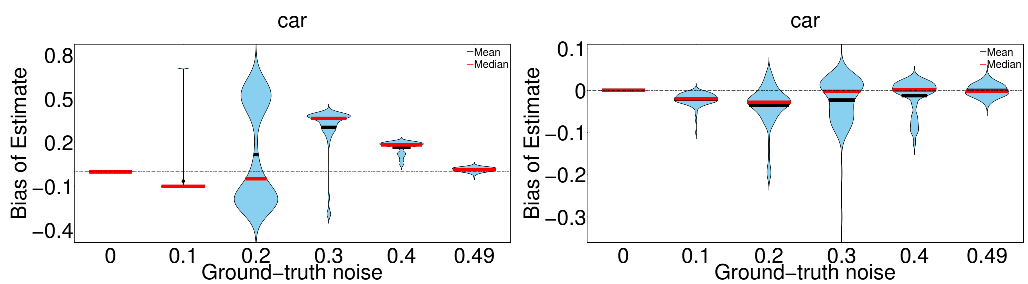

Figure 6. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `car`. (Note the different axes on the plots.)

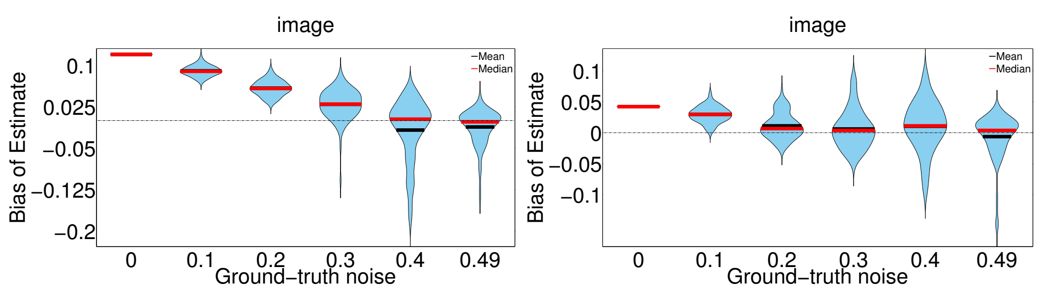

Figure 7. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `image`. (Note the different axes on the plots.)

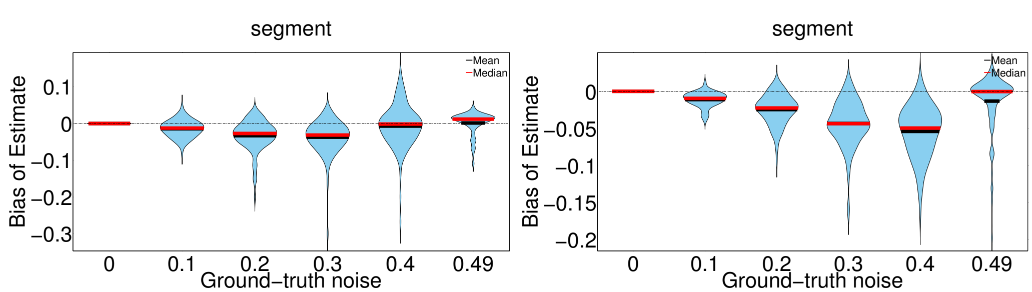

Figure 8. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `segment`. (Note the different axes on the plots.)

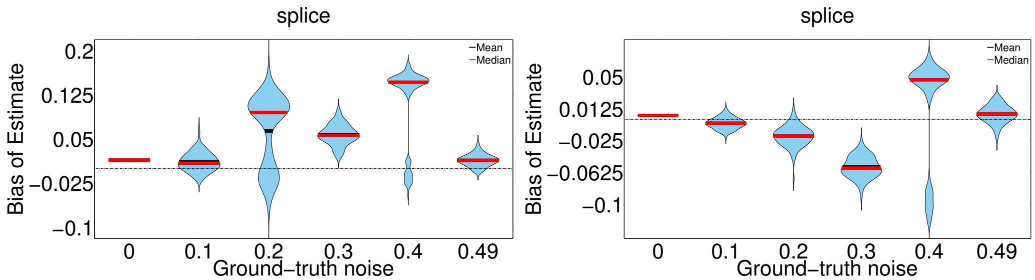

Figure 9. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `splice`. (Note the different axes on the plots.)

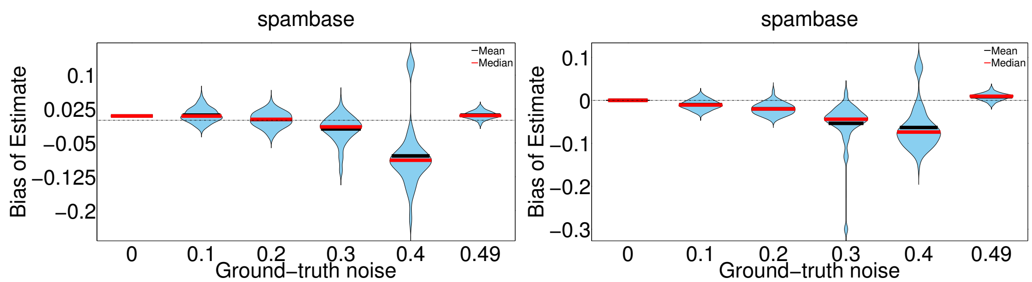

Figure 10. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `spambase`. (Note the different axes on the plots.)

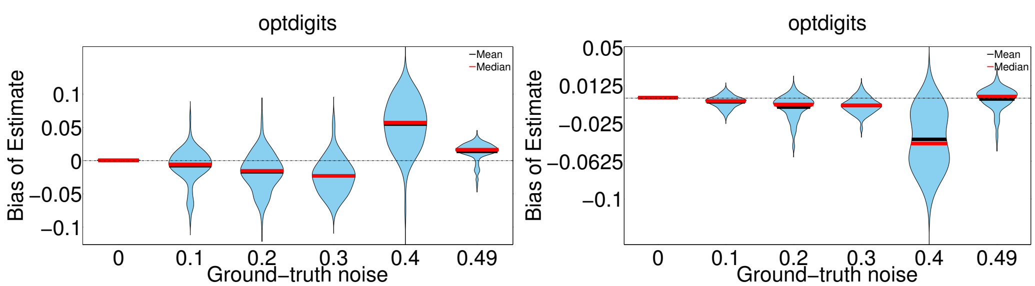

Figure 11. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `optdigits`. (Note the different axes on the plots.)

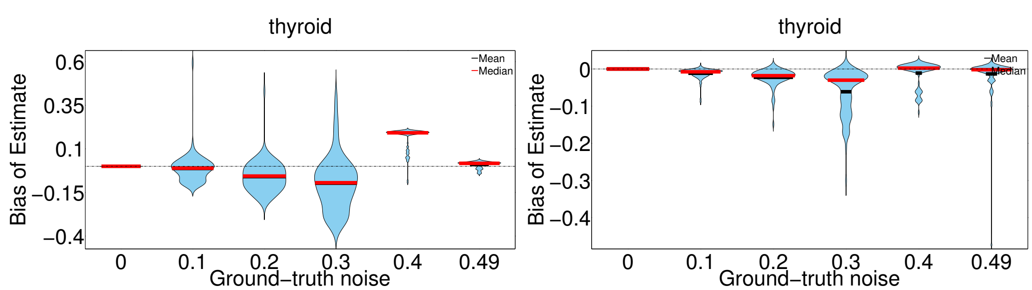

Figure 12. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `thyroid`. (Note the different axes on the plots.)

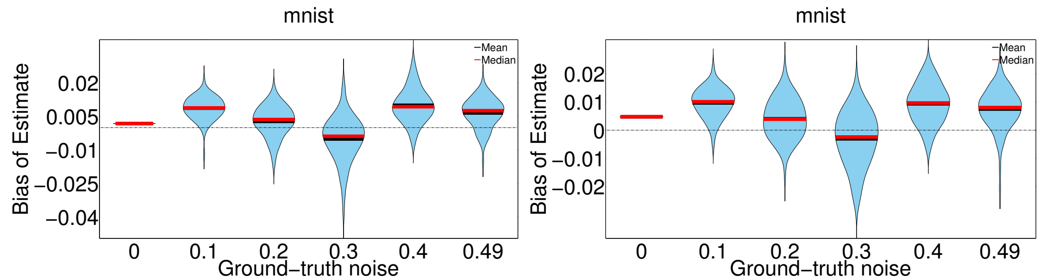

Figure 13. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `mnist3v8`. (Note the different axes on the plots.)

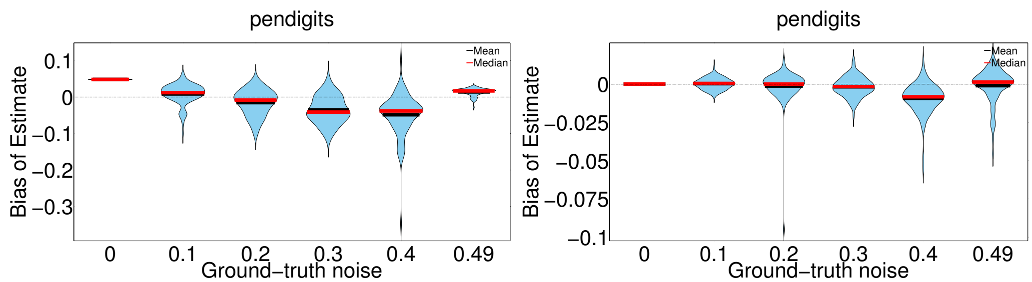

Figure 14. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `pendigits`. (Note the different axes on the plots.)

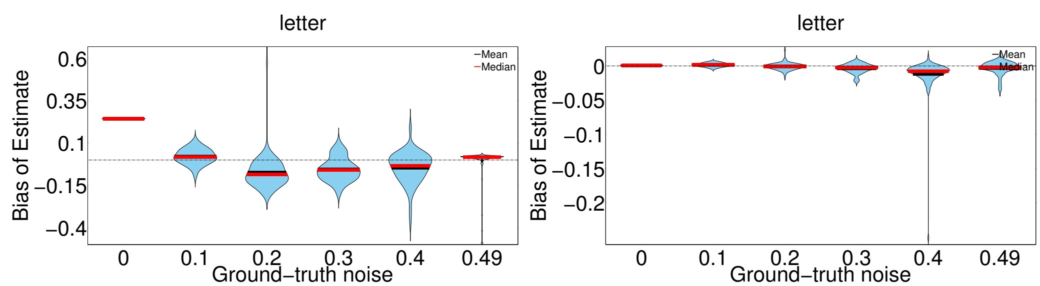

Figure 15. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `letter`. (Note the different axes on the plots.)

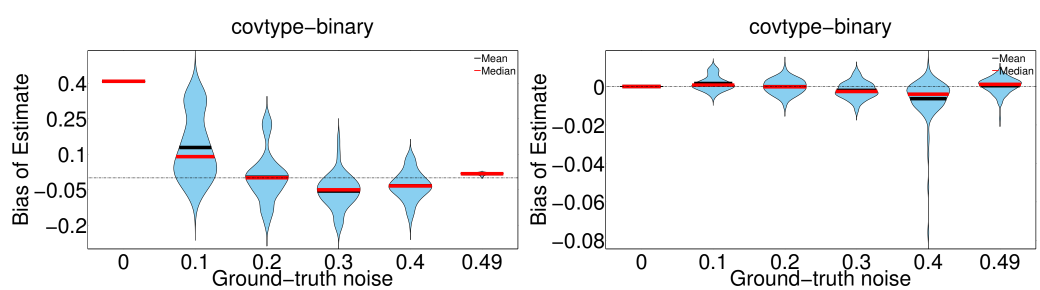

Figure 16. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `covtype-binary`. (Note the different axes on the plots.)

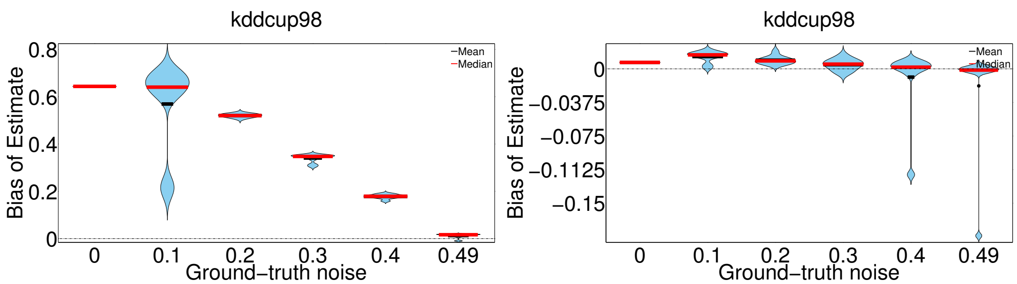

Figure 17. Violin plots of bias in estimate $\hat{\rho}_+, \hat{\rho}_-$ over $\tau = 100$ trials on `kddcup98`. (Note the different axes on the plots.)

J.3. Classification performance

We present results showing clean test set AUC, BER, and misclassification error for a range of noise settings in Tables 7 – 16. (Recall from §7.3 that $\mathrm{ERR}_{\mathrm{max}}$ denotes the misclassification error of the classification formed by thresholding based on the estimated noise rates, while $\mathrm{ERR}_{\mathrm{oracle}}$ is that of the classifier formed by thresholding based on the true noise rates.) We find that generally, even with inexact estimates of ρ_+, ρ_-, we can attain reasonable classification performance.

Recall that the immunity of AUC and BER does *not* rely on the weak separability assumption. Therefore, even with imperfect performance in the noise-free case, we expect only mild degradation in general. Nonetheless, on some datasets (e.g. `housing`, `car`), there is significant degradation in the AUC and BER with moderate to high noise rates. These are generally accompanied by a corresponding degradation in performance of the oracle classifier. This again indicates that there is difficulty in accurately estimating the noisy class-conditional. One explanation for these results is that the required sample size at moderate noise rates is not met by some of the smaller datasets. By contrast, on larger datasets, like `kddcup98`, we observe robustness even at high noise rates.

Noise	1 - **AUC** (%)	**BER** (%)	$\mathbf{ERR}_{\text{max}}$(%)	$\mathbf{ERR}_{\text{oracle}}$(%)
None	14.48 ± 0.00	10.94 ± 0.00	19.80 ± 0.00	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	26.23 ± 0.71	29.99 ± 0.79	19.25 ± 0.96	5.11 ± 0.06
$(\rho_+, \rho_-) = (0.0, 0.2)$	33.91 ± 1.28	37.94 ± 1.04	37.30 ± 1.96	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.3)$	38.56 ± 1.45	43.84 ± 0.95	41.50 ± 1.84	4.96 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.4)$	40.30 ± 1.50	44.59 ± 0.84	49.83 ± 1.79	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.49)$	42.85 ± 1.55	47.14 ± 0.86	55.84 ± 1.81	5.00 ± 0.04
$(\rho_+, \rho_-) = (0.1, 0.0)$	17.04 ± 0.34	18.69 ± 0.70	16.39 ± 0.25	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.1, 0.1)$	29.84 ± 1.20	33.45 ± 1.06	23.99 ± 1.63	5.10 ± 0.06
$(\rho_+, \rho_-) = (0.1, 0.2)$	36.89 ± 1.35	40.40 ± 1.04	40.71 ± 2.02	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.1, 0.3)$	39.51 ± 1.40	44.74 ± 0.93	43.53 ± 1.85	5.15 ± 0.17
$(\rho_+, \rho_-) = (0.1, 0.4)$	41.67 ± 1.53	46.56 ± 0.73	51.38 ± 1.70	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.1, 0.49)$	44.55 ± 1.57	47.86 ± 0.69	59.59 ± 1.86	5.07 ± 0.07
$(\rho_+, \rho_-) = (0.2, 0.0)$	18.88 ± 0.53	21.46 ± 0.76	15.99 ± 0.30	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.2, 0.1)$	33.84 ± 1.32	36.71 ± 1.07	32.22 ± 1.99	5.16 ± 0.07
$(\rho_+, \rho_-) = (0.2, 0.2)$	39.50 ± 1.44	43.36 ± 1.01	43.57 ± 1.99	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.2, 0.3)$	44.39 ± 1.48	46.37 ± 0.82	49.42 ± 1.96	4.97 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.4)$	44.06 ± 1.57	47.86 ± 0.76	54.72 ± 1.75	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.2, 0.49)$	46.71 ± 1.52	48.75 ± 0.73	53.67 ± 1.92	5.29 ± 0.18
$(\rho_+, \rho_-) = (0.3, 0.0)$	21.09 ± 0.70	23.76 ± 0.93	16.59 ± 0.62	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.3, 0.1)$	37.38 ± 1.36	39.89 ± 1.10	35.83 ± 2.08	5.14 ± 0.07
$(\rho_+, \rho_-) = (0.3, 0.2)$	43.15 ± 1.40	45.82 ± 0.90	49.48 ± 1.85	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.3, 0.3)$	45.75 ± 1.41	48.52 ± 0.67	50.66 ± 1.91	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.3, 0.4)$	44.14 ± 1.54	48.74 ± 0.60	51.22 ± 1.95	5.19 ± 0.14
$(\rho_+, \rho_-) = (0.3, 0.49)$	47.16 ± 1.51	49.46 ± 0.70	58.56 ± 1.77	6.05 ± 0.46
$(\rho_+, \rho_-) = (0.4, 0.0)$	23.01 ± 0.93	27.63 ± 1.01	17.58 ± 0.92	4.96 ± 0.01
$(\rho_+, \rho_-) = (0.4, 0.1)$	40.74 ± 1.41	43.32 ± 1.01	42.83 ± 2.19	5.14 ± 0.08
$(\rho_+, \rho_-) = (0.4, 0.2)$	45.08 ± 1.52	47.03 ± 0.82	47.74 ± 2.00	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.4, 0.3)$	48.73 ± 1.53	49.79 ± 0.21	52.50 ± 1.92	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.4, 0.4)$	46.95 ± 1.51	50.62 ± 0.28	55.10 ± 1.83	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.4, 0.49)$	48.24 ± 1.63	49.45 ± 0.63	53.63 ± 1.82	11.78 ± 1.90
$(\rho_+, \rho_-) = (0.49, 0.0)$	25.44 ± 1.10	29.94 ± 0.99	18.77 ± 1.29	5.15 ± 0.10
$(\rho_+, \rho_-) = (0.49, 0.1)$	42.48 ± 1.47	44.39 ± 0.94	42.88 ± 2.14	5.04 ± 0.04
$(\rho_+, \rho_-) = (0.49, 0.2)$	47.16 ± 1.45	48.31 ± 0.85	48.43 ± 1.91	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.49, 0.3)$	49.74 ± 1.55	49.79 ± 0.21	51.80 ± 1.93	4.95 ± 0.00
$(\rho_+, \rho_-) = (0.49, 0.4)$	46.19 ± 1.53	50.58 ± 0.37	52.74 ± 2.07	7.73 ± 1.40
$(\rho_+, \rho_-) = (0.49, 0.49)$	51.74 ± 1.60	50.24 ± 0.27	54.41 ± 1.97	44.92 ± 4.46

Table 6. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `housing` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. ERR_{max} and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	$\mathbf{ERR}_{\text{max}}(\%)$	$\mathbf{ERR}_{\text{oracle}}(\%)$
None	0.42 ± 0.00	0.61 ± 0.00	1.16 ± 0.00	1.16 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	0.87 ± 0.24	8.73 ± 0.26	3.34 ± 0.60	2.57 ± 0.08
$(\rho_+, \rho_-) = (0.0, 0.2)$	0.93 ± 0.27	10.57 ± 0.27	3.28 ± 0.84	2.28 ± 0.08
$(\rho_+, \rho_-) = (0.0, 0.3)$	4.22 ± 0.87	14.72 ± 0.75	13.87 ± 2.69	2.84 ± 0.13
$(\rho_+, \rho_-) = (0.0, 0.4)$	11.38 ± 1.39	23.30 ± 1.34	28.46 ± 2.96	3.98 ± 0.15
$(\rho_+, \rho_-) = (0.0, 0.49)$	16.38 ± 1.11	32.02 ± 1.35	40.53 ± 1.91	4.97 ± 0.08
$(\rho_+, \rho_-) = (0.1, 0.0)$	0.84 ± 0.16	2.80 ± 0.32	1.90 ± 0.05	1.81 ± 0.04
$(\rho_+, \rho_-) = (0.1, 0.1)$	1.17 ± 0.29	9.65 ± 0.33	4.35 ± 0.91	2.74 ± 0.08
$(\rho_+, \rho_-) = (0.1, 0.2)$	2.48 ± 0.57	12.81 ± 0.69	8.71 ± 1.99	2.74 ± 0.11
$(\rho_+, \rho_-) = (0.1, 0.3)$	8.58 ± 1.05	21.56 ± 1.21	24.95 ± 2.67	4.01 ± 0.14
$(\rho_+, \rho_-) = (0.1, 0.4)$	18.32 ± 1.50	31.75 ± 1.36	39.19 ± 2.15	5.04 ± 0.07
$(\rho_+, \rho_-) = (0.1, 0.49)$	22.32 ± 1.33	37.29 ± 1.24	44.11 ± 1.07	5.22 ± 0.00
$(\rho_+, \rho_-) = (0.2, 0.0)$	1.26 ± 0.19	3.82 ± 0.39	2.11 ± 0.07	1.97 ± 0.06
$(\rho_+, \rho_-) = (0.2, 0.1)$	1.75 ± 0.35	11.14 ± 0.42	6.12 ± 1.28	2.99 ± 0.10
$(\rho_+, \rho_-) = (0.2, 0.2)$	5.68 ± 0.78	20.04 ± 1.29	19.48 ± 2.33	3.76 ± 0.14
$(\rho_+, \rho_-) = (0.2, 0.3)$	19.26 ± 1.97	31.01 ± 1.43	36.36 ± 2.12	4.82 ± 0.09
$(\rho_+, \rho_-) = (0.2, 0.4)$	20.53 ± 1.39	37.52 ± 1.34	43.18 ± 1.47	5.18 ± 0.05
$(\rho_+, \rho_-) = (0.2, 0.49)$	26.11 ± 1.37	42.37 ± 1.12	47.59 ± 1.00	5.22 ± 0.00
$(\rho_+, \rho_-) = (0.3, 0.0)$	2.15 ± 0.27	5.00 ± 0.37	2.09 ± 0.07	1.90 ± 0.05
$(\rho_+, \rho_-) = (0.3, 0.1)$	4.65 ± 0.62	14.78 ± 0.64	13.23 ± 1.72	3.82 ± 0.13
$(\rho_+, \rho_-) = (0.3, 0.2)$	13.72 ± 1.73	29.87 ± 1.63	30.45 ± 2.13	4.61 ± 0.11
$(\rho_+, \rho_-) = (0.3, 0.3)$	23.36 ± 1.64	36.79 ± 1.43	43.75 ± 1.70	5.19 ± 0.03
$(\rho_+, \rho_-) = (0.3, 0.4)$	31.20 ± 1.83	41.84 ± 1.13	46.15 ± 1.15	5.22 ± 0.01
$(\rho_+, \rho_-) = (0.3, 0.49)$	33.83 ± 1.53	44.41 ± 0.99	46.68 ± 0.88	5.22 ± 0.00
$(\rho_+, \rho_-) = (0.4, 0.0)$	2.93 ± 0.33	6.21 ± 0.55	2.49 ± 0.08	2.21 ± 0.07
$(\rho_+, \rho_-) = (0.4, 0.1)$	8.63 ± 1.29	22.43 ± 1.38	20.05 ± 1.82	4.59 ± 0.10
$(\rho_+, \rho_-) = (0.4, 0.2)$	20.44 ± 1.77	37.13 ± 1.49	38.81 ± 1.71	5.15 ± 0.04
$(\rho_+, \rho_-) = (0.4, 0.3)$	27.42 ± 1.68	40.70 ± 1.29	43.96 ± 1.36	5.26 ± 0.03
$(\rho_+, \rho_-) = (0.4, 0.4)$	34.88 ± 1.82	43.90 ± 1.02	47.76 ± 1.02	5.42 ± 0.08
$(\rho_+, \rho_-) = (0.4, 0.49)$	38.73 ± 1.78	46.73 ± 0.84	48.86 ± 0.85	5.28 ± 0.04
$(\rho_+, \rho_-) = (0.49, 0.0)$	2.89 ± 0.40	5.41 ± 0.56	3.16 ± 0.10	2.76 ± 0.09
$(\rho_+, \rho_-) = (0.49, 0.1)$	15.13 ± 1.81	28.55 ± 1.43	29.03 ± 1.58	5.09 ± 0.06
$(\rho_+, \rho_-) = (0.49, 0.2)$	26.36 ± 1.75	40.94 ± 1.30	42.40 ± 1.56	5.36 ± 0.07
$(\rho_+, \rho_-) = (0.49, 0.3)$	38.35 ± 2.04	44.18 ± 1.09	47.99 ± 1.42	5.44 ± 0.11
$(\rho_+, \rho_-) = (0.49, 0.4)$	40.95 ± 1.71	47.22 ± 0.82	49.22 ± 0.92	6.42 ± 0.36
$(\rho_+, \rho_-) = (0.49, 0.49)$	45.08 ± 1.84	48.82 ± 0.62	48.47 ± 0.87	35.54 ± 4.13

Table 7. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `car` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. ERR_{max} and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	**ERR**$_{\text{max}}$(%)	**ERR**$_{\text{oracle}}$(%)
None	11.47 $\pm$ 0.00	14.98 $\pm$ 0.00	13.67 $\pm$ 0.00	13.91 $\pm$ 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	11.60 $\pm$ 0.01	14.56 $\pm$ 0.03	13.87 $\pm$ 0.04	13.94 $\pm$ 0.03
$(\rho_+, \rho_-) = (0.0, 0.2)$	11.62 $\pm$ 0.02	14.58 $\pm$ 0.03	13.87 $\pm$ 0.04	13.89 $\pm$ 0.04
$(\rho_+, \rho_-) = (0.0, 0.3)$	11.67 $\pm$ 0.03	14.55 $\pm$ 0.04	13.84 $\pm$ 0.05	13.84 $\pm$ 0.05
$(\rho_+, \rho_-) = (0.0, 0.4)$	11.71 $\pm$ 0.03	14.69 $\pm$ 0.05	13.98 $\pm$ 0.06	13.95 $\pm$ 0.05
$(\rho_+, \rho_-) = (0.0, 0.49)$	11.86 $\pm$ 0.07	14.82 $\pm$ 0.09	14.24 $\pm$ 0.08	14.18 $\pm$ 0.08
$(\rho_+, \rho_-) = (0.1, 0.0)$	11.55 $\pm$ 0.01	14.64 $\pm$ 0.03	13.81 $\pm$ 0.03	13.85 $\pm$ 0.03
$(\rho_+, \rho_-) = (0.1, 0.1)$	11.64 $\pm$ 0.02	14.61 $\pm$ 0.03	13.93 $\pm$ 0.04	13.97 $\pm$ 0.05
$(\rho_+, \rho_-) = (0.1, 0.2)$	11.68 $\pm$ 0.04	14.61 $\pm$ 0.05	14.02 $\pm$ 0.06	13.93 $\pm$ 0.06
$(\rho_+, \rho_-) = (0.1, 0.3)$	11.93 $\pm$ 0.05	14.89 $\pm$ 0.07	14.30 $\pm$ 0.07	14.21 $\pm$ 0.07
$(\rho_+, \rho_-) = (0.1, 0.4)$	12.12 $\pm$ 0.07	15.13 $\pm$ 0.09	14.65 $\pm$ 0.10	14.56 $\pm$ 0.09
$(\rho_+, \rho_-) = (0.1, 0.49)$	12.70 $\pm$ 0.14	16.34 $\pm$ 0.23	15.92 $\pm$ 0.25	15.63 $\pm$ 0.21
$(\rho_+, \rho_-) = (0.2, 0.0)$	11.62 $\pm$ 0.02	14.66 $\pm$ 0.03	13.92 $\pm$ 0.05	13.97 $\pm$ 0.04
$(\rho_+, \rho_-) = (0.2, 0.1)$	11.75 $\pm$ 0.05	14.65 $\pm$ 0.05	14.06 $\pm$ 0.06	13.98 $\pm$ 0.06
$(\rho_+, \rho_-) = (0.2, 0.2)$	11.91 $\pm$ 0.05	14.82 $\pm$ 0.08	14.25 $\pm$ 0.08	14.18 $\pm$ 0.08
$(\rho_+, \rho_-) = (0.2, 0.3)$	12.13 $\pm$ 0.07	15.14 $\pm$ 0.09	14.83 $\pm$ 0.09	14.74 $\pm$ 0.09
$(\rho_+, \rho_-) = (0.2, 0.4)$	12.95 $\pm$ 0.15	16.80 $\pm$ 0.25	16.66 $\pm$ 0.23	16.32 $\pm$ 0.22
$(\rho_+, \rho_-) = (0.2, 0.49)$	14.45 $\pm$ 0.24	19.38 $\pm$ 0.35	19.11 $\pm$ 0.34	18.81 $\pm$ 0.33
$(\rho_+, \rho_-) = (0.3, 0.0)$	11.68 $\pm$ 0.04	14.62 $\pm$ 0.05	13.96 $\pm$ 0.05	14.02 $\pm$ 0.05
$(\rho_+, \rho_-) = (0.3, 0.1)$	12.03 $\pm$ 0.10	14.88 $\pm$ 0.09	14.24 $\pm$ 0.10	14.23 $\pm$ 0.10
$(\rho_+, \rho_-) = (0.3, 0.2)$	12.45 $\pm$ 0.12	15.43 $\pm$ 0.12	14.89 $\pm$ 0.12	14.84 $\pm$ 0.13
$(\rho_+, \rho_-) = (0.3, 0.3)$	13.09 $\pm$ 0.15	17.07 $\pm$ 0.27	16.51 $\pm$ 0.27	16.27 $\pm$ 0.23
$(\rho_+, \rho_-) = (0.3, 0.4)$	15.23 $\pm$ 0.29	20.64 $\pm$ 0.43	20.40 $\pm$ 0.52	19.70 $\pm$ 0.40
$(\rho_+, \rho_-) = (0.3, 0.49)$	19.30 $\pm$ 0.41	26.27 $\pm$ 0.50	26.68 $\pm$ 0.68	25.44 $\pm$ 0.43
$(\rho_+, \rho_-) = (0.4, 0.0)$	11.76 $\pm$ 0.04	14.71 $\pm$ 0.07	14.06 $\pm$ 0.07	14.03 $\pm$ 0.07
$(\rho_+, \rho_-) = (0.4, 0.1)$	12.27 $\pm$ 0.09	15.22 $\pm$ 0.12	14.59 $\pm$ 0.11	14.57 $\pm$ 0.11
$(\rho_+, \rho_-) = (0.4, 0.2)$	12.95 $\pm$ 0.13	16.73 $\pm$ 0.22	16.12 $\pm$ 0.21	15.94 $\pm$ 0.18
$(\rho_+, \rho_-) = (0.4, 0.3)$	14.86 $\pm$ 0.29	20.05 $\pm$ 0.42	19.57 $\pm$ 0.46	19.13 $\pm$ 0.38
$(\rho_+, \rho_-) = (0.4, 0.4)$	20.28 $\pm$ 0.48	27.47 $\pm$ 0.57	27.90 $\pm$ 0.71	26.62 $\pm$ 0.57
$(\rho_+, \rho_-) = (0.4, 0.49)$	29.96 $\pm$ 0.78	38.96 $\pm$ 0.86	38.87 $\pm$ 0.77	37.84 $\pm$ 0.77
$(\rho_+, \rho_-) = (0.49, 0.0)$	11.94 $\pm$ 0.09	14.96 $\pm$ 0.10	14.25 $\pm$ 0.12	14.26 $\pm$ 0.11
$(\rho_+, \rho_-) = (0.49, 0.1)$	12.73 $\pm$ 0.12	16.10 $\pm$ 0.18	15.50 $\pm$ 0.22	15.38 $\pm$ 0.17
$(\rho_+, \rho_-) = (0.49, 0.2)$	14.30 $\pm$ 0.19	19.73 $\pm$ 0.36	19.17 $\pm$ 0.43	18.58 $\pm$ 0.29
$(\rho_+, \rho_-) = (0.49, 0.3)$	19.62 $\pm$ 0.51	26.42 $\pm$ 0.51	28.28 $\pm$ 0.84	25.41 $\pm$ 0.53
$(\rho_+, \rho_-) = (0.49, 0.4)$	30.28 $\pm$ 0.94	38.17 $\pm$ 0.85	38.36 $\pm$ 0.87	37.49 $\pm$ 0.79
$(\rho_+, \rho_-) = (0.49, 0.49)$	43.80 $\pm$ 1.37	47.79 $\pm$ 0.58	47.18 $\pm$ 0.77	47.59 $\pm$ 0.56

Table 8. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `image` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. ERR$_{\text{max}}$ and ERR$_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	$\mathbf{ERR}_{\max}$(%)	$\mathbf{ERR}_{\text{oracle}}$(%)
None	0.00 ± 0.00	0.00 ± 0.00	0.00 ± 0.00	0.00 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	0.02 ± 0.01	0.38 ± 0.04	0.18 ± 0.03	0.18 ± 0.03
$(\rho_+, \rho_-) = (0.0, 0.2)$	0.01 ± 0.01	0.71 ± 0.07	0.23 ± 0.04	0.22 ± 0.04
$(\rho_+, \rho_-) = (0.0, 0.3)$	0.01 ± 0.01	1.08 ± 0.07	0.23 ± 0.04	0.22 ± 0.04
$(\rho_+, \rho_-) = (0.0, 0.4)$	0.02 ± 0.01	1.56 ± 0.10	0.39 ± 0.08	0.39 ± 0.08
$(\rho_+, \rho_-) = (0.0, 0.49)$	0.04 ± 0.01	2.16 ± 0.15	0.54 ± 0.08	0.50 ± 0.08
$(\rho_+, \rho_-) = (0.1, 0.0)$	0.00 ± 0.00	0.01 ± 0.00	0.01 ± 0.00	0.01 ± 0.00
$(\rho_+, \rho_-) = (0.1, 0.1)$	0.01 ± 0.00	0.46 ± 0.04	0.19 ± 0.03	0.19 ± 0.03
$(\rho_+, \rho_-) = (0.1, 0.2)$	0.02 ± 0.01	0.90 ± 0.08	0.31 ± 0.05	0.30 ± 0.05
$(\rho_+, \rho_-) = (0.1, 0.3)$	0.00 ± 0.00	1.51 ± 0.10	0.16 ± 0.04	0.16 ± 0.04
$(\rho_+, \rho_-) = (0.1, 0.4)$	0.03 ± 0.01	2.31 ± 0.16	0.47 ± 0.07	0.45 ± 0.07
$(\rho_+, \rho_-) = (0.1, 0.49)$	0.05 ± 0.01	3.15 ± 0.20	1.03 ± 0.26	0.66 ± 0.11
$(\rho_+, \rho_-) = (0.2, 0.0)$	0.00 ± 0.00	0.02 ± 0.01	0.02 ± 0.01	0.02 ± 0.01
$(\rho_+, \rho_-) = (0.2, 0.1)$	0.00 ± 0.00	0.51 ± 0.05	0.09 ± 0.02	0.10 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.2)$	0.02 ± 0.02	1.00 ± 0.08	0.18 ± 0.05	0.17 ± 0.05
$(\rho_+, \rho_-) = (0.2, 0.3)$	0.03 ± 0.01	2.00 ± 0.14	0.23 ± 0.05	0.23 ± 0.05
$(\rho_+, \rho_-) = (0.2, 0.4)$	0.03 ± 0.01	3.24 ± 0.20	0.31 ± 0.06	0.27 ± 0.06
$(\rho_+, \rho_-) = (0.2, 0.49)$	0.13 ± 0.04	5.00 ± 0.28	1.47 ± 0.25	0.94 ± 0.21
$(\rho_+, \rho_-) = (0.3, 0.0)$	0.00 ± 0.00	0.06 ± 0.02	0.06 ± 0.01	0.06 ± 0.01
$(\rho_+, \rho_-) = (0.3, 0.1)$	0.02 ± 0.01	0.60 ± 0.06	0.20 ± 0.04	0.19 ± 0.04
$(\rho_+, \rho_-) = (0.3, 0.2)$	0.03 ± 0.01	1.59 ± 0.11	0.45 ± 0.09	0.43 ± 0.08
$(\rho_+, \rho_-) = (0.3, 0.3)$	0.05 ± 0.02	2.85 ± 0.18	0.49 ± 0.09	0.45 ± 0.09
$(\rho_+, \rho_-) = (0.3, 0.4)$	0.03 ± 0.01	5.09 ± 0.27	0.62 ± 0.12	0.31 ± 0.06
$(\rho_+, \rho_-) = (0.3, 0.49)$	0.03 ± 0.01	8.41 ± 0.37	3.10 ± 0.49	1.45 ± 0.32
$(\rho_+, \rho_-) = (0.4, 0.0)$	0.01 ± 0.01	0.10 ± 0.03	0.08 ± 0.02	0.07 ± 0.02
$(\rho_+, \rho_-) = (0.4, 0.1)$	0.03 ± 0.02	0.78 ± 0.08	0.26 ± 0.07	0.24 ± 0.07
$(\rho_+, \rho_-) = (0.4, 0.2)$	0.02 ± 0.01	1.98 ± 0.15	0.23 ± 0.06	0.20 ± 0.06
$(\rho_+, \rho_-) = (0.4, 0.3)$	0.02 ± 0.01	4.24 ± 0.24	0.46 ± 0.12	0.26 ± 0.07
$(\rho_+, \rho_-) = (0.4, 0.4)$	0.07 ± 0.02	8.21 ± 0.39	3.19 ± 0.83	1.53 ± 0.33
$(\rho_+, \rho_-) = (0.4, 0.49)$	1.28 ± 0.55	16.72 ± 1.04	18.16 ± 1.87	6.80 ± 0.68
$(\rho_+, \rho_-) = (0.49, 0.0)$	0.02 ± 0.01	0.19 ± 0.06	0.17 ± 0.06	0.11 ± 0.02
$(\rho_+, \rho_-) = (0.49, 0.1)$	0.02 ± 0.01	1.00 ± 0.09	0.24 ± 0.07	0.18 ± 0.05
$(\rho_+, \rho_-) = (0.49, 0.2)$	0.05 ± 0.02	2.98 ± 0.19	0.55 ± 0.17	0.32 ± 0.08
$(\rho_+, \rho_-) = (0.49, 0.3)$	0.07 ± 0.04	6.71 ± 0.33	1.48 ± 0.43	0.48 ± 0.11
$(\rho_+, \rho_-) = (0.49, 0.4)$	5.27 ± 1.30	20.19 ± 1.51	18.16 ± 1.75	7.31 ± 0.63
$(\rho_+, \rho_-) = (0.49, 0.49)$	32.23 ± 3.17	42.82 ± 1.39	44.23 ± 1.91	31.76 ± 2.86

Table 9. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `segment` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. $\text{ERR}_{\max}$ and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	$\textbf{ERR}_{\max}$(%)	$\textbf{ERR}_{\text{oracle}}$(%)
None	0.28 ± 0.00	3.40 ± 0.00	2.35 ± 0.00	2.35 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	0.76 ± 0.03	4.20 ± 0.07	3.27 ± 0.05	3.27 ± 0.05
$(\rho_+, \rho_-) = (0.0, 0.2)$	1.22 ± 0.06	4.70 ± 0.10	4.23 ± 0.09	4.23 ± 0.09
$(\rho_+, \rho_-) = (0.0, 0.3)$	1.32 ± 0.06	6.12 ± 0.12	5.04 ± 0.09	4.62 ± 0.11
$(\rho_+, \rho_-) = (0.0, 0.4)$	1.10 ± 0.04	8.85 ± 0.11	6.67 ± 0.13	4.50 ± 0.09
$(\rho_+, \rho_-) = (0.0, 0.49)$	1.46 ± 0.04	10.76 ± 0.12	9.31 ± 0.17	5.38 ± 0.10
$(\rho_+, \rho_-) = (0.1, 0.0)$	0.55 ± 0.03	4.07 ± 0.08	2.83 ± 0.06	2.79 ± 0.05
$(\rho_+, \rho_-) = (0.1, 0.1)$	1.12 ± 0.04	4.84 ± 0.09	3.75 ± 0.07	3.75 ± 0.07
$(\rho_+, \rho_-) = (0.1, 0.2)$	1.70 ± 0.07	5.79 ± 0.11	5.00 ± 0.11	4.99 ± 0.11
$(\rho_+, \rho_-) = (0.1, 0.3)$	1.48 ± 0.06	7.96 ± 0.11	6.04 ± 0.11	5.08 ± 0.10
$(\rho_+, \rho_-) = (0.1, 0.4)$	2.01 ± 0.07	10.72 ± 0.12	9.08 ± 0.18	6.19 ± 0.11
$(\rho_+, \rho_-) = (0.1, 0.49)$	3.06 ± 0.09	13.35 ± 0.14	13.53 ± 0.24	7.92 ± 0.13
$(\rho_+, \rho_-) = (0.2, 0.0)$	0.75 ± 0.03	4.95 ± 0.12	3.54 ± 0.11	3.36 ± 0.06
$(\rho_+, \rho_-) = (0.2, 0.1)$	1.60 ± 0.06	6.05 ± 0.12	4.59 ± 0.09	4.53 ± 0.08
$(\rho_+, \rho_-) = (0.2, 0.2)$	1.79 ± 0.10	7.02 ± 0.10	5.39 ± 0.16	5.56 ± 0.15
$(\rho_+, \rho_-) = (0.2, 0.3)$	2.17 ± 0.07	9.93 ± 0.14	7.75 ± 0.13	6.63 ± 0.11
$(\rho_+, \rho_-) = (0.2, 0.4)$	3.64 ± 0.13	13.29 ± 0.17	12.73 ± 0.26	9.63 ± 0.37
$(\rho_+, \rho_-) = (0.2, 0.49)$	5.09 ± 0.24	16.01 ± 0.23	18.17 ± 0.40	15.70 ± 0.59
$(\rho_+, \rho_-) = (0.3, 0.0)$	1.07 ± 0.05	5.99 ± 0.16	4.69 ± 0.22	4.09 ± 0.08
$(\rho_+, \rho_-) = (0.3, 0.1)$	1.68 ± 0.08	6.54 ± 0.12	6.37 ± 0.26	5.53 ± 0.12
$(\rho_+, \rho_-) = (0.3, 0.2)$	1.95 ± 0.06	8.75 ± 0.13	6.55 ± 0.13	6.71 ± 0.13
$(\rho_+, \rho_-) = (0.3, 0.3)$	3.68 ± 0.11	12.25 ± 0.16	10.87 ± 0.20	8.79 ± 0.16
$(\rho_+, \rho_-) = (0.3, 0.4)$	5.62 ± 0.29	16.20 ± 0.44	16.83 ± 0.39	16.14 ± 0.58
$(\rho_+, \rho_-) = (0.3, 0.49)$	12.81 ± 1.37	39.21 ± 1.43	25.62 ± 1.16	22.45 ± 0.34
$(\rho_+, \rho_-) = (0.4, 0.0)$	1.34 ± 0.08	6.67 ± 0.27	8.23 ± 0.52	5.64 ± 0.17
$(\rho_+, \rho_-) = (0.4, 0.1)$	1.59 ± 0.07	7.03 ± 0.13	8.52 ± 0.32	7.20 ± 0.14
$(\rho_+, \rho_-) = (0.4, 0.2)$	3.14 ± 0.09	10.65 ± 0.15	8.61 ± 0.15	8.70 ± 0.16
$(\rho_+, \rho_-) = (0.4, 0.3)$	6.21 ± 0.25	16.21 ± 0.55	14.99 ± 0.30	13.77 ± 0.45
$(\rho_+, \rho_-) = (0.4, 0.4)$	15.67 ± 1.52	41.24 ± 1.37	26.08 ± 1.17	22.87 ± 0.31
$(\rho_+, \rho_-) = (0.4, 0.49)$	37.37 ± 1.94	50.00 ± 0.00	42.22 ± 1.20	24.45 ± 0.00
$(\rho_+, \rho_-) = (0.49, 0.0)$	0.66 ± 0.07	4.26 ± 0.23	15.80 ± 0.40	8.84 ± 0.16
$(\rho_+, \rho_-) = (0.49, 0.1)$	2.05 ± 0.06	7.95 ± 0.13	9.68 ± 0.32	8.56 ± 0.17
$(\rho_+, \rho_-) = (0.49, 0.2)$	5.19 ± 0.15	13.49 ± 0.19	11.67 ± 0.22	11.13 ± 0.21
$(\rho_+, \rho_-) = (0.49, 0.3)$	12.57 ± 0.96	34.95 ± 1.54	23.21 ± 0.88	20.63 ± 0.44
$(\rho_+, \rho_-) = (0.49, 0.4)$	28.59 ± 1.74	49.82 ± 0.18	38.30 ± 1.20	24.48 ± 0.03
$(\rho_+, \rho_-) = (0.49, 0.49)$	48.98 ± 1.61	50.00 ± 0.00	50.33 ± 1.05	41.31 ± 2.41

Table 10. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `splice` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. ERR_{max} and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	$\mathbf{ERR}_{\max}$(%)	$\mathbf{ERR}_{\text{oracle}}$(%)
None	2.49 ± 0.00	6.93 ± 0.00	6.52 ± 0.00	6.52 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	2.71 ± 0.02	7.06 ± 0.03	6.87 ± 0.03	6.84 ± 0.03
$(\rho_+, \rho_-) = (0.0, 0.2)$	2.78 ± 0.03	7.30 ± 0.04	7.12 ± 0.04	7.07 ± 0.04
$(\rho_+, \rho_-) = (0.0, 0.3)$	2.94 ± 0.03	7.58 ± 0.05	7.40 ± 0.05	7.33 ± 0.04
$(\rho_+, \rho_-) = (0.0, 0.4)$	3.14 ± 0.04	8.01 ± 0.06	7.74 ± 0.06	7.63 ± 0.06
$(\rho_+, \rho_-) = (0.0, 0.49)$	3.35 ± 0.04	8.56 ± 0.08	8.37 ± 0.08	8.15 ± 0.07
$(\rho_+, \rho_-) = (0.1, 0.0)$	2.67 ± 0.02	7.10 ± 0.03	6.88 ± 0.03	6.89 ± 0.03
$(\rho_+, \rho_-) = (0.1, 0.1)$	2.82 ± 0.03	7.35 ± 0.04	7.21 ± 0.04	7.19 ± 0.04
$(\rho_+, \rho_-) = (0.1, 0.2)$	3.01 ± 0.03	7.66 ± 0.05	7.51 ± 0.05	7.48 ± 0.05
$(\rho_+, \rho_-) = (0.1, 0.3)$	3.31 ± 0.04	8.23 ± 0.06	7.97 ± 0.06	7.95 ± 0.06
$(\rho_+, \rho_-) = (0.1, 0.4)$	3.78 ± 0.06	8.90 ± 0.08	8.69 ± 0.08	8.56 ± 0.08
$(\rho_+, \rho_-) = (0.1, 0.49)$	4.38 ± 0.07	9.92 ± 0.11	9.87 ± 0.12	9.69 ± 0.11
$(\rho_+, \rho_-) = (0.2, 0.0)$	2.74 ± 0.02	7.19 ± 0.03	7.06 ± 0.04	7.04 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.1)$	2.97 ± 0.04	7.53 ± 0.05	7.38 ± 0.05	7.38 ± 0.05
$(\rho_+, \rho_-) = (0.2, 0.2)$	3.34 ± 0.05	8.20 ± 0.07	8.09 ± 0.07	8.07 ± 0.07
$(\rho_+, \rho_-) = (0.2, 0.3)$	4.00 ± 0.07	8.99 ± 0.08	9.02 ± 0.13	8.93 ± 0.09
$(\rho_+, \rho_-) = (0.2, 0.4)$	4.91 ± 0.09	10.52 ± 0.13	10.82 ± 0.31	10.26 ± 0.12
$(\rho_+, \rho_-) = (0.2, 0.49)$	6.51 ± 0.13	12.93 ± 0.18	15.40 ± 0.73	12.55 ± 0.16
$(\rho_+, \rho_-) = (0.3, 0.0)$	2.87 ± 0.04	7.29 ± 0.04	7.19 ± 0.04	7.20 ± 0.04
$(\rho_+, \rho_-) = (0.3, 0.1)$	3.21 ± 0.05	7.77 ± 0.07	7.77 ± 0.07	7.78 ± 0.07
$(\rho_+, \rho_-) = (0.3, 0.2)$	3.81 ± 0.07	8.91 ± 0.10	8.77 ± 0.11	8.69 ± 0.09
$(\rho_+, \rho_-) = (0.3, 0.3)$	5.01 ± 0.10	10.65 ± 0.13	10.90 ± 0.25	10.40 ± 0.12
$(\rho_+, \rho_-) = (0.3, 0.4)$	6.95 ± 0.12	13.41 ± 0.17	16.67 ± 0.92	13.11 ± 0.17
$(\rho_+, \rho_-) = (0.3, 0.49)$	9.14 ± 0.37	17.22 ± 0.69	19.29 ± 0.67	17.01 ± 0.51
$(\rho_+, \rho_-) = (0.4, 0.0)$	2.94 ± 0.03	7.47 ± 0.05	7.45 ± 0.05	7.41 ± 0.05
$(\rho_+, \rho_-) = (0.4, 0.1)$	3.62 ± 0.06	8.49 ± 0.09	8.41 ± 0.09	8.41 ± 0.08
$(\rho_+, \rho_-) = (0.4, 0.2)$	4.73 ± 0.10	10.24 ± 0.13	10.28 ± 0.19	10.09 ± 0.12
$(\rho_+, \rho_-) = (0.4, 0.3)$	6.86 ± 0.12	13.18 ± 0.16	15.41 ± 0.57	13.30 ± 0.17
$(\rho_+, \rho_-) = (0.4, 0.4)$	9.22 ± 0.23	17.89 ± 0.74	21.09 ± 0.77	18.49 ± 0.66
$(\rho_+, \rho_-) = (0.4, 0.49)$	14.90 ± 1.08	23.67 ± 1.06	27.99 ± 1.07	24.07 ± 0.76
$(\rho_+, \rho_-) = (0.49, 0.0)$	3.18 ± 0.04	7.74 ± 0.06	7.84 ± 0.06	7.79 ± 0.06
$(\rho_+, \rho_-) = (0.49, 0.1)$	4.14 ± 0.08	9.39 ± 0.11	9.25 ± 0.10	9.19 ± 0.09
$(\rho_+, \rho_-) = (0.49, 0.2)$	6.42 ± 0.13	12.64 ± 0.17	15.07 ± 0.46	12.57 ± 0.18
$(\rho_+, \rho_-) = (0.49, 0.3)$	8.98 ± 0.35	16.34 ± 0.49	20.40 ± 0.50	16.83 ± 0.39
$(\rho_+, \rho_-) = (0.49, 0.4)$	15.76 ± 0.84	27.15 ± 1.32	29.77 ± 1.13	26.94 ± 0.97
$(\rho_+, \rho_-) = (0.49, 0.49)$	40.46 ± 1.91	49.98 ± 0.02	45.94 ± 1.35	48.80 ± 1.00

Table 11. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `spambase` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. ERR_{max} and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	$\mathbf{ERR}_{\text{max}}(\%)$	$\mathbf{ERR}_{\text{oracle}}(\%)$
None	0.01 ± 0.00	1.18 ± 0.00	0.18 ± 0.00	0.18 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	0.07 ± 0.01	1.04 ± 0.05	0.61 ± 0.04	0.61 ± 0.04
$(\rho_+, \rho_-) = (0.0, 0.2)$	0.11 ± 0.02	1.61 ± 0.10	0.65 ± 0.04	0.66 ± 0.04
$(\rho_+, \rho_-) = (0.0, 0.3)$	0.07 ± 0.01	2.39 ± 0.16	0.58 ± 0.05	0.58 ± 0.05
$(\rho_+, \rho_-) = (0.0, 0.4)$	0.14 ± 0.02	2.96 ± 0.20	0.75 ± 0.06	0.74 ± 0.06
$(\rho_+, \rho_-) = (0.0, 0.49)$	0.15 ± 0.04	4.71 ± 0.22	0.77 ± 0.09	0.73 ± 0.09
$(\rho_+, \rho_-) = (0.1, 0.0)$	0.01 ± 0.00	0.86 ± 0.04	0.22 ± 0.01	0.22 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.1)$	0.09 ± 0.02	1.30 ± 0.06	0.65 ± 0.04	0.63 ± 0.04
$(\rho_+, \rho_-) = (0.1, 0.2)$	0.10 ± 0.02	1.82 ± 0.12	0.67 ± 0.04	0.67 ± 0.04
$(\rho_+, \rho_-) = (0.1, 0.3)$	0.12 ± 0.02	2.63 ± 0.19	0.77 ± 0.06	0.76 ± 0.06
$(\rho_+, \rho_-) = (0.1, 0.4)$	0.24 ± 0.04	3.44 ± 0.24	1.14 ± 0.09	1.13 ± 0.09
$(\rho_+, \rho_-) = (0.1, 0.49)$	0.36 ± 0.09	4.91 ± 0.35	1.49 ± 0.19	1.42 ± 0.18
$(\rho_+, \rho_-) = (0.2, 0.0)$	0.07 ± 0.02	1.00 ± 0.05	0.28 ± 0.01	0.28 ± 0.01
$(\rho_+, \rho_-) = (0.2, 0.1)$	0.13 ± 0.02	1.23 ± 0.06	0.76 ± 0.05	0.76 ± 0.05
$(\rho_+, \rho_-) = (0.2, 0.2)$	0.19 ± 0.03	2.05 ± 0.15	0.84 ± 0.06	0.83 ± 0.06
$(\rho_+, \rho_-) = (0.2, 0.3)$	0.46 ± 0.09	3.05 ± 0.22	1.39 ± 0.17	1.39 ± 0.17
$(\rho_+, \rho_-) = (0.2, 0.4)$	0.71 ± 0.23	4.45 ± 0.40	2.23 ± 0.52	1.65 ± 0.19
$(\rho_+, \rho_-) = (0.2, 0.49)$	1.44 ± 0.50	8.44 ± 0.72	4.42 ± 1.01	1.97 ± 0.18
$(\rho_+, \rho_-) = (0.3, 0.0)$	0.06 ± 0.02	1.16 ± 0.05	0.29 ± 0.01	0.30 ± 0.01
$(\rho_+, \rho_-) = (0.3, 0.1)$	0.21 ± 0.03	1.72 ± 0.10	0.85 ± 0.06	0.84 ± 0.06
$(\rho_+, \rho_-) = (0.3, 0.2)$	0.35 ± 0.04	2.64 ± 0.17	1.09 ± 0.08	1.08 ± 0.08
$(\rho_+, \rho_-) = (0.3, 0.3)$	0.85 ± 0.08	2.82 ± 0.17	1.99 ± 0.11	2.00 ± 0.10
$(\rho_+, \rho_-) = (0.3, 0.4)$	1.21 ± 0.49	10.79 ± 0.71	4.58 ± 1.03	1.67 ± 0.21
$(\rho_+, \rho_-) = (0.3, 0.49)$	0.30 ± 0.10	15.39 ± 0.31	7.48 ± 0.44	2.53 ± 0.25
$(\rho_+, \rho_-) = (0.4, 0.0)$	0.15 ± 0.03	1.25 ± 0.07	0.31 ± 0.01	0.31 ± 0.01
$(\rho_+, \rho_-) = (0.4, 0.1)$	0.25 ± 0.03	2.13 ± 0.12	0.98 ± 0.07	0.97 ± 0.07
$(\rho_+, \rho_-) = (0.4, 0.2)$	0.73 ± 0.24	4.21 ± 0.38	1.88 ± 0.55	1.41 ± 0.11
$(\rho_+, \rho_-) = (0.4, 0.3)$	0.60 ± 0.19	9.48 ± 0.52	2.39 ± 0.42	1.77 ± 0.21
$(\rho_+, \rho_-) = (0.4, 0.4)$	0.26 ± 0.03	15.29 ± 0.30	7.58 ± 0.48	3.01 ± 0.28
$(\rho_+, \rho_-) = (0.4, 0.49)$	5.51 ± 1.06	25.66 ± 1.27	26.14 ± 1.07	5.72 ± 0.27
$(\rho_+, \rho_-) = (0.49, 0.0)$	0.39 ± 0.07	1.75 ± 0.11	0.42 ± 0.02	0.42 ± 0.02
$(\rho_+, \rho_-) = (0.49, 0.1)$	0.53 ± 0.07	3.05 ± 0.16	1.25 ± 0.10	1.24 ± 0.10
$(\rho_+, \rho_-) = (0.49, 0.2)$	0.60 ± 0.11	7.33 ± 0.41	1.59 ± 0.14	1.66 ± 0.14
$(\rho_+, \rho_-) = (0.49, 0.3)$	0.26 ± 0.05	14.16 ± 0.34	4.92 ± 0.32	2.75 ± 0.25
$(\rho_+, \rho_-) = (0.49, 0.4)$	6.01 ± 1.15	26.32 ± 1.35	25.86 ± 1.27	5.66 ± 0.28
$(\rho_+, \rho_-) = (0.49, 0.49)$	39.89 ± 2.97	47.32 ± 0.81	49.02 ± 1.10	21.43 ± 2.79

Table 12. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `optdigits` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. ERR_{max} and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	**ERR**$_{\max}$(%)	**ERR**$_{\text{oracle}}$(%)
None	0.16 ± 0.00	0.78 ± 0.00	0.62 ± 0.00	0.62 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	0.44 ± 0.05	4.22 ± 0.19	0.66 ± 0.01	0.66 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.2)$	0.95 ± 0.16	7.03 ± 0.26	0.73 ± 0.01	0.73 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.3)$	1.55 ± 0.26	8.37 ± 0.33	1.02 ± 0.25	0.78 ± 0.02
$(\rho_+, \rho_-) = (0.0, 0.4)$	1.72 ± 0.23	10.31 ± 0.35	0.84 ± 0.02	0.83 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.49)$	2.56 ± 0.36	11.24 ± 0.43	1.64 ± 0.47	0.96 ± 0.03
$(\rho_+, \rho_-) = (0.1, 0.0)$	0.18 ± 0.00	0.98 ± 0.08	0.62 ± 0.01	0.61 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.1)$	0.84 ± 0.14	5.20 ± 0.23	0.77 ± 0.07	0.70 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.2)$	1.16 ± 0.17	7.46 ± 0.33	0.88 ± 0.08	0.79 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.3)$	1.95 ± 0.28	9.90 ± 0.36	0.86 ± 0.02	0.84 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.4)$	2.79 ± 0.38	12.80 ± 0.43	1.12 ± 0.11	0.97 ± 0.03
$(\rho_+, \rho_-) = (0.1, 0.49)$	3.67 ± 0.41	15.23 ± 0.52	1.95 ± 0.39	1.09 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.0)$	0.78 ± 0.15	3.17 ± 0.22	0.94 ± 0.14	0.66 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.1)$	1.17 ± 0.19	5.98 ± 0.30	0.97 ± 0.16	0.75 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.2)$	1.74 ± 0.21	9.54 ± 0.39	0.92 ± 0.07	0.84 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.3)$	2.36 ± 0.27	11.86 ± 0.41	1.02 ± 0.07	0.93 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.4)$	2.96 ± 0.31	15.76 ± 0.45	1.16 ± 0.10	1.05 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.49)$	18.08 ± 1.86	29.79 ± 1.61	22.81 ± 3.08	1.47 ± 0.06
$(\rho_+, \rho_-) = (0.3, 0.0)$	1.08 ± 0.18	3.95 ± 0.24	0.93 ± 0.14	0.65 ± 0.02
$(\rho_+, \rho_-) = (0.3, 0.1)$	1.43 ± 0.19	7.17 ± 0.34	0.88 ± 0.08	0.81 ± 0.02
$(\rho_+, \rho_-) = (0.3, 0.2)$	2.25 ± 0.26	10.96 ± 0.40	1.01 ± 0.09	0.92 ± 0.02
$(\rho_+, \rho_-) = (0.3, 0.3)$	3.93 ± 0.52	15.76 ± 0.62	3.95 ± 1.43	1.15 ± 0.06
$(\rho_+, \rho_-) = (0.3, 0.4)$	20.37 ± 1.97	31.50 ± 1.55	27.39 ± 3.25	1.36 ± 0.03
$(\rho_+, \rho_-) = (0.3, 0.49)$	34.85 ± 1.74	43.48 ± 1.11	42.50 ± 2.81	1.58 ± 0.06
$(\rho_+, \rho_-) = (0.4, 0.0)$	2.02 ± 0.29	5.42 ± 0.25	1.29 ± 0.20	0.70 ± 0.03
$(\rho_+, \rho_-) = (0.4, 0.1)$	2.07 ± 0.28	8.97 ± 0.36	0.85 ± 0.01	0.85 ± 0.01
$(\rho_+, \rho_-) = (0.4, 0.2)$	3.11 ± 0.31	14.88 ± 0.42	1.01 ± 0.03	1.00 ± 0.03
$(\rho_+, \rho_-) = (0.4, 0.3)$	19.14 ± 2.06	29.28 ± 1.52	18.96 ± 2.78	1.44 ± 0.05
$(\rho_+, \rho_-) = (0.4, 0.4)$	37.26 ± 1.64	44.28 ± 1.11	49.74 ± 2.81	1.58 ± 0.04
$(\rho_+, \rho_-) = (0.4, 0.49)$	44.46 ± 1.01	47.93 ± 0.50	53.37 ± 2.69	1.48 ± 0.01
$(\rho_+, \rho_-) = (0.49, 0.0)$	2.37 ± 0.31	5.71 ± 0.27	1.29 ± 0.20	0.70 ± 0.03
$(\rho_+, \rho_-) = (0.49, 0.1)$	3.02 ± 0.38	11.32 ± 0.43	1.24 ± 0.24	0.93 ± 0.02
$(\rho_+, \rho_-) = (0.49, 0.2)$	10.83 ± 1.57	23.80 ± 1.33	11.16 ± 2.30	1.19 ± 0.03
$(\rho_+, \rho_-) = (0.49, 0.3)$	36.81 ± 1.83	42.12 ± 1.14	43.88 ± 2.87	1.55 ± 0.03
$(\rho_+, \rho_-) = (0.49, 0.4)$	39.98 ± 1.07	48.45 ± 0.64	59.99 ± 2.40	1.97 ± 0.19
$(\rho_+, \rho_-) = (0.49, 0.49)$	47.04 ± 0.99	50.20 ± 0.35	54.23 ± 2.69	13.31 ± 2.58

Table 13. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `thyroid` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. ERR$_{\max}$ and ERR$_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	$\mathbf{ERR}_{\max}(\%)$	$\mathbf{ERR}_{\text{oracle}}(\%)$
None	0.95 ± 0.00	4.51 ± 0.00	3.09 ± 0.00	3.05 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	0.84 ± 0.00	4.60 ± 0.02	2.63 ± 0.01	2.64 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.2)$	0.87 ± 0.01	4.16 ± 0.04	2.33 ± 0.02	2.33 ± 0.02
$(\rho_+, \rho_-) = (0.0, 0.3)$	0.86 ± 0.01	4.07 ± 0.04	2.13 ± 0.02	2.12 ± 0.02
$(\rho_+, \rho_-) = (0.0, 0.4)$	0.86 ± 0.01	4.12 ± 0.04	2.11 ± 0.02	2.12 ± 0.02
$(\rho_+, \rho_-) = (0.0, 0.49)$	0.88 ± 0.01	4.34 ± 0.06	2.20 ± 0.02	2.19 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.0)$	0.94 ± 0.00	4.57 ± 0.01	2.96 ± 0.01	2.89 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.1)$	0.87 ± 0.01	4.50 ± 0.03	2.60 ± 0.02	2.60 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.2)$	0.89 ± 0.01	4.27 ± 0.05	2.35 ± 0.03	2.37 ± 0.03
$(\rho_+, \rho_-) = (0.1, 0.3)$	0.89 ± 0.01	4.27 ± 0.04	2.19 ± 0.02	2.19 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.4)$	0.92 ± 0.01	4.52 ± 0.05	2.22 ± 0.02	2.23 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.49)$	1.01 ± 0.03	4.96 ± 0.09	2.33 ± 0.02	2.32 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.0)$	0.95 ± 0.00	4.53 ± 0.02	2.97 ± 0.02	2.92 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.1)$	0.89 ± 0.01	4.51 ± 0.04	2.60 ± 0.02	2.60 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.2)$	0.92 ± 0.01	4.45 ± 0.13	2.37 ± 0.03	2.41 ± 0.05
$(\rho_+, \rho_-) = (0.2, 0.3)$	0.95 ± 0.01	4.58 ± 0.06	2.32 ± 0.03	2.31 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.4)$	1.04 ± 0.02	5.05 ± 0.10	2.39 ± 0.03	2.39 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.49)$	1.27 ± 0.04	6.21 ± 0.17	2.68 ± 0.04	2.67 ± 0.04
$(\rho_+, \rho_-) = (0.3, 0.0)$	0.97 ± 0.01	4.46 ± 0.02	2.98 ± 0.02	2.92 ± 0.02
$(\rho_+, \rho_-) = (0.3, 0.1)$	0.92 ± 0.01	4.55 ± 0.05	2.59 ± 0.03	2.59 ± 0.03
$(\rho_+, \rho_-) = (0.3, 0.2)$	0.97 ± 0.02	4.69 ± 0.08	2.39 ± 0.03	2.38 ± 0.03
$(\rho_+, \rho_-) = (0.3, 0.3)$	1.10 ± 0.02	5.21 ± 0.10	2.49 ± 0.03	2.46 ± 0.03
$(\rho_+, \rho_-) = (0.3, 0.4)$	1.46 ± 0.07	6.22 ± 0.17	2.82 ± 0.05	2.76 ± 0.05
$(\rho_+, \rho_-) = (0.3, 0.49)$	2.07 ± 0.11	9.41 ± 0.28	3.38 ± 0.07	3.26 ± 0.06
$(\rho_+, \rho_-) = (0.4, 0.0)$	0.99 ± 0.01	4.48 ± 0.03	3.03 ± 0.02	2.98 ± 0.02
$(\rho_+, \rho_-) = (0.4, 0.1)$	0.95 ± 0.01	4.67 ± 0.06	2.60 ± 0.03	2.58 ± 0.03
$(\rho_+, \rho_-) = (0.4, 0.2)$	1.07 ± 0.02	4.97 ± 0.09	2.48 ± 0.03	2.43 ± 0.03
$(\rho_+, \rho_-) = (0.4, 0.3)$	1.31 ± 0.04	6.51 ± 0.17	2.74 ± 0.04	2.68 ± 0.04
$(\rho_+, \rho_-) = (0.4, 0.4)$	2.12 ± 0.12	10.36 ± 0.31	3.86 ± 0.27	3.39 ± 0.08
$(\rho_+, \rho_-) = (0.4, 0.49)$	9.53 ± 1.24	24.53 ± 1.24	23.16 ± 1.78	6.99 ± 0.19
$(\rho_+, \rho_-) = (0.49, 0.0)$	1.00 ± 0.01	4.48 ± 0.03	3.05 ± 0.02	2.99 ± 0.02
$(\rho_+, \rho_-) = (0.49, 0.1)$	1.00 ± 0.01	4.75 ± 0.06	2.61 ± 0.03	2.54 ± 0.03
$(\rho_+, \rho_-) = (0.49, 0.2)$	1.22 ± 0.03	5.70 ± 0.12	2.70 ± 0.04	2.61 ± 0.03
$(\rho_+, \rho_-) = (0.49, 0.3)$	1.94 ± 0.10	9.15 ± 0.27	3.47 ± 0.09	3.27 ± 0.07
$(\rho_+, \rho_-) = (0.49, 0.4)$	6.02 ± 0.43	19.80 ± 0.52	19.31 ± 1.38	6.74 ± 0.21
$(\rho_+, \rho_-) = (0.49, 0.49)$	32.02 ± 2.02	48.16 ± 0.71	51.59 ± 1.24	18.81 ± 2.49

Table 14. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `pendigits` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. $\text{ERR}_{\max}$ and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	**ERR**$_{\text{max}}$(%)	**ERR**$_{\text{oracle}}$(%)
None	0.92 ± 0.00	3.63 ± 0.00	3.63 ± 0.00	3.63 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	0.93 ± 0.00	3.61 ± 0.01	3.59 ± 0.01	3.60 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.2)$	0.94 ± 0.01	3.63 ± 0.01	3.62 ± 0.01	3.62 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.3)$	0.96 ± 0.01	3.65 ± 0.01	3.63 ± 0.01	3.64 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.4)$	0.99 ± 0.01	3.65 ± 0.02	3.65 ± 0.02	3.66 ± 0.02
$(\rho_+, \rho_-) = (0.0, 0.49)$	1.00 ± 0.01	3.69 ± 0.02	3.68 ± 0.02	3.68 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.0)$	0.95 ± 0.01	3.56 ± 0.01	3.55 ± 0.01	3.55 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.1)$	0.96 ± 0.01	3.62 ± 0.01	3.61 ± 0.01	3.61 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.2)$	0.97 ± 0.01	3.63 ± 0.02	3.62 ± 0.02	3.62 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.3)$	1.00 ± 0.01	3.68 ± 0.02	3.67 ± 0.02	3.67 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.4)$	1.05 ± 0.01	3.78 ± 0.02	3.77 ± 0.02	3.78 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.49)$	1.10 ± 0.01	3.94 ± 0.03	3.94 ± 0.03	3.94 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.0)$	0.96 ± 0.01	3.60 ± 0.01	3.59 ± 0.01	3.59 ± 0.01
$(\rho_+, \rho_-) = (0.2, 0.1)$	0.98 ± 0.01	3.64 ± 0.02	3.63 ± 0.02	3.64 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.2)$	1.02 ± 0.01	3.67 ± 0.02	3.68 ± 0.02	3.67 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.3)$	1.07 ± 0.02	3.83 ± 0.02	3.82 ± 0.02	3.83 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.4)$	1.17 ± 0.02	4.06 ± 0.03	4.06 ± 0.03	4.05 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.49)$	1.33 ± 0.03	4.41 ± 0.04	4.41 ± 0.04	4.42 ± 0.04
$(\rho_+, \rho_-) = (0.3, 0.0)$	0.98 ± 0.01	3.65 ± 0.02	3.64 ± 0.02	3.64 ± 0.02
$(\rho_+, \rho_-) = (0.3, 0.1)$	1.03 ± 0.01	3.72 ± 0.02	3.73 ± 0.02	3.73 ± 0.02
$(\rho_+, \rho_-) = (0.3, 0.2)$	1.06 ± 0.02	3.80 ± 0.03	3.80 ± 0.03	3.81 ± 0.03
$(\rho_+, \rho_-) = (0.3, 0.3)$	1.15 ± 0.02	4.09 ± 0.03	4.09 ± 0.03	4.09 ± 0.03
$(\rho_+, \rho_-) = (0.3, 0.4)$	1.40 ± 0.03	4.55 ± 0.05	4.57 ± 0.05	4.54 ± 0.05
$(\rho_+, \rho_-) = (0.3, 0.49)$	1.62 ± 0.05	5.08 ± 0.07	5.12 ± 0.07	5.10 ± 0.07
$(\rho_+, \rho_-) = (0.4, 0.0)$	1.02 ± 0.01	3.69 ± 0.02	3.70 ± 0.02	3.70 ± 0.02
$(\rho_+, \rho_-) = (0.4, 0.1)$	1.06 ± 0.01	3.83 ± 0.02	3.85 ± 0.02	3.84 ± 0.02
$(\rho_+, \rho_-) = (0.4, 0.2)$	1.16 ± 0.02	4.05 ± 0.03	4.06 ± 0.03	4.05 ± 0.03
$(\rho_+, \rho_-) = (0.4, 0.3)$	1.37 ± 0.03	4.60 ± 0.04	4.63 ± 0.04	4.61 ± 0.04
$(\rho_+, \rho_-) = (0.4, 0.4)$	1.77 ± 0.05	5.44 ± 0.09	5.49 ± 0.08	5.48 ± 0.08
$(\rho_+, \rho_-) = (0.4, 0.49)$	2.82 ± 0.09	7.63 ± 0.14	7.95 ± 0.16	8.05 ± 0.16
$(\rho_+, \rho_-) = (0.49, 0.0)$	1.03 ± 0.01	3.72 ± 0.02	3.72 ± 0.02	3.72 ± 0.02
$(\rho_+, \rho_-) = (0.49, 0.1)$	1.13 ± 0.02	3.96 ± 0.03	3.98 ± 0.03	3.96 ± 0.03
$(\rho_+, \rho_-) = (0.49, 0.2)$	1.33 ± 0.02	4.47 ± 0.04	4.50 ± 0.05	4.48 ± 0.04
$(\rho_+, \rho_-) = (0.49, 0.3)$	1.63 ± 0.06	5.20 ± 0.08	5.26 ± 0.08	5.24 ± 0.08
$(\rho_+, \rho_-) = (0.49, 0.4)$	2.95 ± 0.09	7.93 ± 0.15	8.30 ± 0.18	8.15 ± 0.15
$(\rho_+, \rho_-) = (0.49, 0.49)$	19.56 ± 1.28	34.70 ± 1.60	35.45 ± 1.15	46.59 ± 0.82

Table 15. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `mnist` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. ERR$_{\text{max}}$ and ERR$_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	$\textbf{ERR}_{\max}$(%)	$\textbf{ERR}_{\text{oracle}}$(%)
None	1.54 ± 0.00	4.71 ± 0.00	1.92 ± 0.00	1.65 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	3.04 ± 0.11	5.46 ± 0.45	1.01 ± 0.04	0.99 ± 0.03
$(\rho_+, \rho_-) = (0.0, 0.2)$	3.32 ± 0.21	6.13 ± 0.45	0.79 ± 0.03	0.79 ± 0.03
$(\rho_+, \rho_-) = (0.0, 0.3)$	3.16 ± 0.04	6.06 ± 0.07	0.74 ± 0.01	0.74 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.4)$	3.12 ± 0.04	6.38 ± 0.07	0.75 ± 0.01	0.75 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.49)$	3.12 ± 0.04	6.67 ± 0.10	0.77 ± 0.01	0.76 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.0)$	1.68 ± 0.05	4.72 ± 0.02	1.85 ± 0.02	1.67 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.1)$	2.96 ± 0.05	5.10 ± 0.04	0.93 ± 0.01	0.92 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.2)$	3.58 ± 0.47	6.21 ± 0.44	0.82 ± 0.04	0.81 ± 0.04
$(\rho_+, \rho_-) = (0.1, 0.3)$	3.15 ± 0.05	6.31 ± 0.09	0.79 ± 0.01	0.78 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.4)$	3.16 ± 0.05	6.95 ± 0.14	0.79 ± 0.01	0.79 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.49)$	3.20 ± 0.06	7.42 ± 0.15	0.84 ± 0.01	0.84 ± 0.01
$(\rho_+, \rho_-) = (0.2, 0.0)$	1.92 ± 0.08	4.79 ± 0.02	1.90 ± 0.04	1.71 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.1)$	3.08 ± 0.06	5.19 ± 0.04	0.91 ± 0.02	0.89 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.2)$	3.12 ± 0.13	6.85 ± 0.41	0.89 ± 0.04	0.83 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.3)$	3.01 ± 0.05	7.41 ± 0.18	0.86 ± 0.01	0.82 ± 0.01
$(\rho_+, \rho_-) = (0.2, 0.4)$	3.18 ± 0.08	8.40 ± 0.47	0.90 ± 0.05	0.87 ± 0.04
$(\rho_+, \rho_-) = (0.2, 0.49)$	3.24 ± 0.07	9.34 ± 0.24	0.96 ± 0.02	0.94 ± 0.02
$(\rho_+, \rho_-) = (0.3, 0.0)$	2.08 ± 0.09	4.77 ± 0.03	1.93 ± 0.06	1.76 ± 0.05
$(\rho_+, \rho_-) = (0.3, 0.1)$	3.01 ± 0.06	5.57 ± 0.07	0.92 ± 0.02	0.89 ± 0.01
$(\rho_+, \rho_-) = (0.3, 0.2)$	3.05 ± 0.05	6.53 ± 0.11	0.85 ± 0.01	0.82 ± 0.01
$(\rho_+, \rho_-) = (0.3, 0.3)$	3.15 ± 0.06	8.10 ± 0.23	0.91 ± 0.02	0.86 ± 0.01
$(\rho_+, \rho_-) = (0.3, 0.4)$	3.18 ± 0.07	10.19 ± 0.28	0.99 ± 0.02	0.91 ± 0.02
$(\rho_+, \rho_-) = (0.3, 0.49)$	3.47 ± 0.08	12.00 ± 0.32	1.47 ± 0.10	1.23 ± 0.04
$(\rho_+, \rho_-) = (0.4, 0.0)$	2.31 ± 0.10	4.79 ± 0.03	2.00 ± 0.07	1.80 ± 0.05
$(\rho_+, \rho_-) = (0.4, 0.1)$	2.99 ± 0.06	5.92 ± 0.08	0.95 ± 0.02	0.90 ± 0.02
$(\rho_+, \rho_-) = (0.4, 0.2)$	3.45 ± 0.43	7.80 ± 0.45	1.01 ± 0.05	0.91 ± 0.04
$(\rho_+, \rho_-) = (0.4, 0.3)$	3.07 ± 0.07	10.25 ± 0.27	1.10 ± 0.03	0.93 ± 0.01
$(\rho_+, \rho_-) = (0.4, 0.4)$	4.34 ± 0.56	13.71 ± 0.66	2.58 ± 0.94	1.34 ± 0.06
$(\rho_+, \rho_-) = (0.4, 0.49)$	14.13 ± 1.75	29.15 ± 1.31	18.93 ± 1.71	3.74 ± 0.07
$(\rho_+, \rho_-) = (0.49, 0.0)$	2.79 ± 0.11	4.82 ± 0.04	1.91 ± 0.07	1.77 ± 0.06
$(\rho_+, \rho_-) = (0.49, 0.1)$	3.04 ± 0.07	6.47 ± 0.12	1.01 ± 0.02	0.92 ± 0.01
$(\rho_+, \rho_-) = (0.49, 0.2)$	2.96 ± 0.06	9.21 ± 0.25	1.11 ± 0.03	0.93 ± 0.02
$(\rho_+, \rho_-) = (0.49, 0.3)$	3.38 ± 0.11	12.48 ± 0.49	2.50 ± 0.94	1.24 ± 0.05
$(\rho_+, \rho_-) = (0.49, 0.4)$	11.11 ± 1.27	29.05 ± 1.32	22.02 ± 1.79	3.79 ± 0.09
$(\rho_+, \rho_-) = (0.49, 0.49)$	36.26 ± 2.06	47.07 ± 0.87	39.98 ± 1.77	8.33 ± 1.41

Table 16. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `letter` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. $\text{ERR}_{\max}$ and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	$\mathbf{ERR}_{\max}(\%)$	$\mathbf{ERR}_{\text{oracle}}(\%)$
None	5.58 ± 0.00	11.01 ± 0.00	7.26 ± 0.00	7.23 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	5.74 ± 0.09	11.24 ± 0.03	6.01 ± 0.04	5.88 ± 0.04
$(\rho_+, \rho_-) = (0.0, 0.2)$	5.85 ± 0.08	11.86 ± 0.04	5.44 ± 0.03	5.40 ± 0.02
$(\rho_+, \rho_-) = (0.0, 0.3)$	5.83 ± 0.03	12.24 ± 0.04	5.19 ± 0.02	5.17 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.4)$	6.03 ± 0.03	12.63 ± 0.09	5.04 ± 0.02	5.03 ± 0.01
$(\rho_+, \rho_-) = (0.0, 0.49)$	6.25 ± 0.04	13.51 ± 0.18	4.92 ± 0.02	4.92 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.0)$	5.68 ± 0.01	11.00 ± 0.02	7.57 ± 0.03	7.18 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.1)$	5.86 ± 0.11	11.30 ± 0.04	5.96 ± 0.04	5.84 ± 0.04
$(\rho_+, \rho_-) = (0.1, 0.2)$	5.88 ± 0.07	11.93 ± 0.05	5.40 ± 0.03	5.39 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.3)$	5.97 ± 0.04	12.33 ± 0.07	5.16 ± 0.02	5.18 ± 0.01
$(\rho_+, \rho_-) = (0.1, 0.4)$	6.23 ± 0.06	13.20 ± 0.16	5.03 ± 0.03	5.05 ± 0.02
$(\rho_+, \rho_-) = (0.1, 0.49)$	6.42 ± 0.07	14.02 ± 0.21	4.96 ± 0.03	5.00 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.0)$	5.62 ± 0.01	10.99 ± 0.02	7.46 ± 0.03	7.10 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.1)$	6.07 ± 0.14	11.43 ± 0.05	5.85 ± 0.04	5.76 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.2)$	5.99 ± 0.07	12.00 ± 0.05	5.42 ± 0.03	5.39 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.3)$	5.96 ± 0.04	12.62 ± 0.07	5.15 ± 0.02	5.18 ± 0.02
$(\rho_+, \rho_-) = (0.2, 0.4)$	6.35 ± 0.07	13.62 ± 0.18	5.04 ± 0.03	5.08 ± 0.03
$(\rho_+, \rho_-) = (0.2, 0.49)$	6.84 ± 0.10	14.63 ± 0.23	5.09 ± 0.04	5.12 ± 0.04
$(\rho_+, \rho_-) = (0.3, 0.0)$	5.61 ± 0.01	11.01 ± 0.03	7.44 ± 0.03	7.04 ± 0.02
$(\rho_+, \rho_-) = (0.3, 0.1)$	5.86 ± 0.11	11.59 ± 0.05	5.76 ± 0.04	5.72 ± 0.03
$(\rho_+, \rho_-) = (0.3, 0.2)$	6.04 ± 0.08	12.27 ± 0.07	5.38 ± 0.04	5.38 ± 0.03
$(\rho_+, \rho_-) = (0.3, 0.3)$	6.11 ± 0.05	13.24 ± 0.12	5.22 ± 0.03	5.19 ± 0.03
$(\rho_+, \rho_-) = (0.3, 0.4)$	6.76 ± 0.09	14.52 ± 0.19	5.22 ± 0.04	5.19 ± 0.04
$(\rho_+, \rho_-) = (0.3, 0.49)$	7.78 ± 0.17	16.22 ± 0.27	5.55 ± 0.06	5.48 ± 0.05
$(\rho_+, \rho_-) = (0.4, 0.0)$	5.62 ± 0.02	11.03 ± 0.03	7.48 ± 0.04	7.01 ± 0.03
$(\rho_+, \rho_-) = (0.4, 0.1)$	6.10 ± 0.12	11.73 ± 0.06	5.74 ± 0.04	5.68 ± 0.03
$(\rho_+, \rho_-) = (0.4, 0.2)$	6.10 ± 0.06	12.76 ± 0.10	5.34 ± 0.04	5.33 ± 0.03
$(\rho_+, \rho_-) = (0.4, 0.3)$	6.54 ± 0.07	14.23 ± 0.17	5.28 ± 0.05	5.24 ± 0.04
$(\rho_+, \rho_-) = (0.4, 0.4)$	8.09 ± 0.20	16.39 ± 0.26	5.91 ± 0.14	5.62 ± 0.06
$(\rho_+, \rho_-) = (0.4, 0.49)$	12.09 ± 0.35	24.95 ± 0.64	27.12 ± 1.67	6.69 ± 0.03
$(\rho_+, \rho_-) = (0.49, 0.0)$	5.59 ± 0.02	11.08 ± 0.03	7.37 ± 0.04	6.91 ± 0.03
$(\rho_+, \rho_-) = (0.49, 0.1)$	5.96 ± 0.10	12.03 ± 0.06	5.64 ± 0.04	5.62 ± 0.03
$(\rho_+, \rho_-) = (0.49, 0.2)$	6.46 ± 0.09	13.23 ± 0.11	5.50 ± 0.06	5.45 ± 0.04
$(\rho_+, \rho_-) = (0.49, 0.3)$	7.33 ± 0.12	15.50 ± 0.18	5.63 ± 0.06	5.49 ± 0.04
$(\rho_+, \rho_-) = (0.49, 0.4)$	13.37 ± 0.50	26.13 ± 0.74	30.22 ± 1.54	6.77 ± 0.06
$(\rho_+, \rho_-) = (0.49, 0.49)$	41.04 ± 2.03	47.96 ± 0.75	48.70 ± 1.28	7.36 ± 0.30

Table 17. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `covtype-binary` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. $\text{ERR}_{\max}$ and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.

Noise	1 - **AUC** (%)	**BER** (%)	$\mathbf{ERR}_{\max}$(%)	$\mathbf{ERR}_{\text{oracle}}$(%)
None	39.62 ± 0.00	42.46 ± 0.00	4.93 ± 0.00	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.1)$	39.91 ± 0.03	42.49 ± 0.08	9.80 ± 1.15	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.2)$	39.99 ± 0.06	42.53 ± 0.11	14.58 ± 1.92	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.3)$	39.96 ± 0.06	42.56 ± 0.08	14.37 ± 2.72	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.4)$	40.10 ± 0.06	42.70 ± 0.06	27.22 ± 8.16	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.0, 0.49)$	40.15 ± 0.06	42.84 ± 0.08	21.09 ± 2.95	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.1, 0.0)$	39.69 ± 0.03	42.46 ± 0.03	6.61 ± 0.66	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.1, 0.1)$	39.95 ± 0.06	42.48 ± 0.07	9.38 ± 1.65	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.1, 0.2)$	40.02 ± 0.07	42.54 ± 0.11	18.12 ± 1.75	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.1, 0.3)$	40.02 ± 0.09	42.55 ± 0.06	15.87 ± 2.80	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.1, 0.4)$	40.21 ± 0.07	42.82 ± 0.10	29.50 ± 8.24	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.1, 0.49)$	40.23 ± 0.09	42.93 ± 0.11	26.25 ± 2.71	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.2, 0.0)$	39.69 ± 0.03	42.39 ± 0.02	6.23 ± 0.66	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.2, 0.1)$	39.95 ± 0.04	42.49 ± 0.09	15.03 ± 2.16	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.2, 0.2)$	40.04 ± 0.08	42.63 ± 0.11	19.19 ± 1.62	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.2, 0.3)$	40.05 ± 0.10	42.61 ± 0.10	17.60 ± 2.82	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.2, 0.4)$	40.42 ± 0.11	43.01 ± 0.10	30.41 ± 8.32	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.2, 0.49)$	40.44 ± 0.12	43.40 ± 0.17	32.37 ± 5.50	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.3, 0.0)$	39.77 ± 0.03	42.36 ± 0.05	7.30 ± 0.61	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.3, 0.1)$	40.05 ± 0.07	42.53 ± 0.09	21.20 ± 8.22	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.3, 0.2)$	40.16 ± 0.12	42.74 ± 0.13	21.55 ± 2.08	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.3, 0.3)$	40.22 ± 0.13	42.79 ± 0.13	20.65 ± 3.46	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.3, 0.4)$	40.63 ± 0.12	43.28 ± 0.12	33.99 ± 8.64	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.3, 0.49)$	41.12 ± 0.24	44.43 ± 0.66	43.34 ± 6.98	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.4, 0.0)$	39.79 ± 0.04	42.39 ± 0.05	8.47 ± 1.01	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.4, 0.1)$	40.06 ± 0.06	42.61 ± 0.10	15.47 ± 2.57	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.4, 0.2)$	40.24 ± 0.12	42.83 ± 0.13	23.22 ± 2.33	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.4, 0.3)$	40.44 ± 0.20	43.08 ± 0.13	25.10 ± 2.55	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.4, 0.4)$	41.23 ± 0.18	43.81 ± 0.16	46.38 ± 8.74	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.4, 0.49)$	43.59 ± 1.18	47.74 ± 0.98	46.10 ± 7.06	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.49, 0.0)$	39.83 ± 0.04	42.44 ± 0.04	9.68 ± 0.93	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.49, 0.1)$	40.16 ± 0.06	42.68 ± 0.13	18.99 ± 3.78	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.49, 0.2)$	40.52 ± 0.20	43.19 ± 0.22	38.06 ± 8.22	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.49, 0.3)$	40.80 ± 0.26	43.40 ± 0.19	27.14 ± 4.51	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.49, 0.4)$	41.87 ± 0.41	44.37 ± 0.25	58.90 ± 9.60	4.93 ± 0.00
$(\rho_+, \rho_-) = (0.49, 0.49)$	49.83 ± 2.09	48.93 ± 1.05	47.44 ± 9.51	5.79 ± 0.84

Table 18. Mean and standard error (standard deviation scaled by $\sqrt{\tau}$) of performance measures on `kddcup98` injected with random label noise $\tau = 100$ times.The case $\rho_- = 0$ corresponds to the censoring version of PU learning. ERR_{max} and $\text{ERR}_{\text{oracle}}$ are the misclassification errors of the classifiers formed by thresholding using $\hat{\rho}_+, \hat{\rho}_-$, and by the ground-truth ρ_+, ρ_- respectively.