# A Constrained Bayesian Approach to Out-of-Distribution Prediction (Supplementary Material) 

Ziyu Wang ${ }^{k 1} \quad$ Binjie Yuan ${ }^{* 1} \quad$ Jiaxun Lu ${ }^{2} \quad$ Bowen Ding ${ }^{3} \quad$ Yunfeng Shao ${ }^{2} \quad$ Qibin Wu ${ }^{3} \quad$ Jun Zhu $^{\# 1}$<br>${ }^{1}$ Dept. of Comp. Sci. \& Tech., BNRist Center, Tsinghua-Huawei Joint Center for AI, THBI Lab, Tsinghua University<br>${ }^{2}$ Huawei Noah's Ark Lab<br>${ }^{3}$ Huawei Technologies Co., Ltd.

Additional notations and conventions The following conventions are used throughout appendix: the denotation of constants $\left(c_{1}, c_{2}, \ldots, C_{1}, C_{2}, \ldots\right)$ may change from line to line. $\|\cdot\|_{2}$ denotes the Euclidean norm for vectors, or the $L_{3}\left(P_{x}^{*}\right)$ norm for functions of $x .\langle\cdot, \cdot\rangle_{2}$ denotes the respective inner product. $\|\cdot\|_{F}$ denotes the Frobenius norm. $\phi_{z}, \Phi_{z}$ denote the PDF and CDF of the standard Gaussian distribution. Recall the inequality $1-\Phi_{z}(x) \leq e^{-x^{2} / 2}$ for $x>0$.

## S1 PROOF FOR LEMMA 1 AND ADDITIONAL REMARKS

Proof for the lemma The first two claims in the lemma are implied by the following two lemmas:
Lemma S1. When $\alpha>0, m \ll \max \left\{1, \sigma_{s}^{-2} \tau_{s}^{2}\right\} d_{\text {spu }}$, the classifier parameterized by $\tilde{\theta}=\left(0, \tilde{\theta}_{s}\right)=\left(0, \alpha \sum_{e \in \mathcal{E}_{t r}} \bar{\beta}_{s p u}^{e}\right)$ satisfies

$$
\begin{equation*}
R_{e, 01}\left(f_{\tilde{\theta}}\right) \leq c_{1} \exp \left(-c_{2} \sigma_{s}^{-2} \tau_{s}^{2} d_{s p u} / m+o_{p}(1)\right) \rightarrow 0, \forall e \in \mathcal{E}_{t r} \tag{S1}
\end{equation*}
$$

Moreover, the same bound holds for the logistic loss, if in addition $\alpha \leq \mathcal{O}\left(\operatorname{poly}\left(d_{s p u} / m\right)\right), \alpha \tau_{s}^{2} \gtrsim 1 / \sigma_{s}^{2} m$.
Lemma S2. Denote by $\mathbf{x}_{i} \in \mathbb{R}^{d_{i n v}}, \mathbf{x}_{s} \in \mathbb{R}^{d_{s p u}}$ the invariant and spurious components of the input $\mathbf{x}$. For any $e_{1}, e_{2} \in \mathcal{E}_{t r}$, let

$$
K L_{i j}:=\operatorname{KL}\left(p_{\text {marg }, e_{1}} \| p_{\text {marg }, e_{2}}\right)=\operatorname{KL}\left(p_{e_{1}}\left(\mathbf{y}, \tilde{\theta}_{s}^{\top} \mathbf{x}_{s}, \mathbf{x}_{i}\right) \| p_{e_{2}}\left(\mathbf{y}, \tilde{\theta}_{s}^{\top} \mathbf{x}_{s}, \mathbf{x}_{i}\right)\right)
$$

denote the KL divergence between the marginal distributions. When $\alpha>0, m<d_{\text {spu }} / 16$, with probability $\geq 1-e^{-m / 18}$ there exists an $\ell \in[m]$, determined by $\left\{\bar{\beta}_{s p u}^{e}: e \in \mathcal{E}_{t r}\right\}$ s.t.

$$
\begin{equation*}
\mathrm{KL}\left(\bigotimes_{e \in \mathcal{E}_{t r}} p_{\text {marg }, e} \| p_{\text {marg, } e_{\ell}}^{\otimes m}\right)=\sum_{j=1}^{m} \mathrm{KL}_{j \ell} \leq \frac{256 m}{\sigma_{s}^{2} d_{s p u}} \tag{S2}
\end{equation*}
$$

The last claim in the text, Eq. 2, follows by a standard argument following $\overline{\mathbf{S} 2}$ : consider the scenario $n_{e} \equiv n$ for simplicity. Denote by $\mathcal{D}_{\top}:=\left(\left(\left(y_{k}^{e_{j}}, \tilde{\theta}_{s}^{\top} x_{k, s}^{e_{j}}, x_{k, i}^{e_{j}}\right): j \in[m]\right): k \in[n]\right)$ the transposed dataset which contains the same information as $\mathcal{D}_{t r}$. Any test on $\mathcal{D}_{t r}$ for the null hypothesis " $\tilde{\theta}_{s}^{\top} \mathbf{x}_{s}$ is an invariant feature" always provides a two-sample test for

$$
H_{0}^{\prime}: \mathcal{D}_{\top} \sim\left(\left(p_{\text {marg }, e_{\ell}}\right)^{\otimes m}\right)^{\otimes n}=: P_{0, n}, \quad H_{1}^{\prime}: \mathcal{D}_{\top} \sim\left(\bigotimes_{e \in \mathcal{E}_{t r}} p_{\text {marg }, e}\right)^{\otimes n}=: P_{1, n}
$$

with the same size and power in the two scenarios. However, any such test must have its combined error lower bounded by

$$
1-D_{T V}\left(P_{0, n}, P_{1, n}\right) \geq 1-\sqrt{2 \mathrm{KL}\left(P_{1, n} \| P_{0, n}\right)} \geq 1-n \cdot \frac{256 m}{\sigma_{s}^{2} d_{s p u}}
$$

This completes the proof.

Remark 1 (IRM and GDRO). From lemmaS1 it is clear that $\tilde{\theta}$ constitutes an approximate optima for ERM and GRDO, as well as the variance-penalty based approaches such as Krueger et al. [2021]. It also shows that the predictor $f=w \circ \Phi$, where $\Phi=$ id and $w(h)=\tilde{\theta}^{\top} h$, approximately satisfies the hard constraints in (IRM) and constitutes an approximate optima in this sense ${ }^{1}$

Remark 2 (interpretations of the KL bound, additional error from feature learning). In addition to the testing-based interpretation as in Eq. 2 , (S2] can also be interpreted directly if we restrict to the family of tests based on a conditional KL divergence, since we have, for all $j \in[m]$,

$$
\mathrm{KL}\left(p_{e_{j}}\left(y \mid \tilde{\theta}^{\top} x_{s}\right) \| p_{e_{\ell}}\left(y \mid \tilde{\theta}^{\top} x_{s}\right)\right) \leq \mathrm{KL}\left(p_{e_{j}}\left(y \mid x_{i}, \tilde{\theta}^{\top} x_{s}\right) \| p_{e_{\ell}}\left(y \mid x_{i}, \tilde{\theta}^{\top} x_{s}\right)\right) \leq \mathrm{KL}_{j \ell} \leq \frac{256 m}{\sigma_{s}^{2} d_{s p u}}
$$

Such tests can be viewed as restricting to the validation of the definition of invariant features, which concerns such conditionals; they should reject $H_{0}$ if the estimated KL divergence becomes larger than a threshold $\delta_{n}=o_{n}(1)$, which at least needs to cover the estimation error for the KL divergence. It is thus clear that in the feature learning scenario we must use a threshold $\delta_{n}^{\prime} \gg \delta_{n}$, since even for the truly invariant part of the model, we can only learn approximately invariant features which will inevitably violate the KL bound by an extra margin. This makes for a larger threshold than (2): for example, if the feature learning process is such that $\delta_{n}^{\prime} \gtrsim d_{s p u} / n$, we would have the indistinguishability result as long as $d_{s p u} / n \gg m / \sigma_{s}^{2} d_{s p u}$, i.e.,

$$
\max _{e \in \mathcal{E}_{t r}} n_{e} \ll \frac{\sigma_{s}^{2} d_{s p u}^{2}}{m}
$$

Another issue that exists for any possible test is that in the feature learning scenario, we need to apply to a collection of feature extractors; we thus needs more stringent requirements on the power of the test, rather than merely requiring them to be $1-o(1)$. For $|\mathcal{M}|$ feature extractors with independent failure probabilities, we would require $n \gtrsim|\mathcal{M}| \sigma_{s}^{2} d_{s p u} / m$ for reliable learning of invariant features. Note how these regimes allow for successful fitting of an in-distribution predictor.

## S1.1 PROOF FOR AUXILIARY LEMMAS

We first introduce the following notations: $\mathcal{E}_{\text {tr }}=:\left\{e_{1}, \ldots, e_{m}\right\}, \overrightarrow{\mathbf{1}}:=\{1, \ldots, 1\} \in \mathbb{R}^{m}$, and define the $m \times m$ matrix $\left(\Sigma_{\mathcal{S}}\right)_{i j}=\left(\bar{\beta}_{s p u}^{e_{i}}\right)^{\top}\left(\bar{\beta}_{s p u}^{e_{j}}\right)$, so that $\left\|\tilde{\theta}_{s}\right\|_{2}^{2}=\alpha^{2} \overrightarrow{\mathbf{1}}^{\top} \Sigma_{\mathcal{S}} \overrightarrow{\mathbf{1}}$. Define $\bar{\Sigma}_{\mathcal{S}}:=\mathbb{E}_{\left\{\bar{\beta}_{s p u}^{e}\right\}} \Sigma_{\mathcal{S}}=\tau_{s}^{2} d_{s p u} I$. Note that by covariance concentration Wainwright, 2019. Ch. 6], we have, when $m \leq d_{\text {spu }}$,

$$
\begin{equation*}
\mathbb{P}_{\left\{\bar{\beta}_{s p u}^{e}\right\}}\left(\frac{1}{\tau_{s} \sqrt{d_{s p u}}}\left\|\bar{\Sigma}_{\mathcal{S}}-\Sigma_{\mathcal{S}}\right\| \leq 3 \sqrt{\frac{m}{d_{s p u}}}+\delta\right) \geq 1-e^{-d_{s p u} \delta^{2} / 18} \tag{S3}
\end{equation*}
$$

Proof for lemma S1. We first derive the 0-1 loss for $\tilde{\theta}$. Note that in the setting of the example, we have, for any $\theta=\left(\theta_{i}, \theta_{s}\right)$,

$$
R_{e, 01}\left(f_{\theta}\right):=\mathbb{E}_{\mathbf{x}^{e}, \mathbf{y}^{e}} \mathbf{1}\left\{\operatorname{sgn}\left(\theta^{\top} \mathbf{x}^{e}\right)=\mathbf{y}^{e}\right\}=\Phi_{z}\left(-\frac{\theta^{\top} \mathbb{E}\left(\mathbf{x}^{e} \mid \mathbf{y}^{e}=1\right)}{\sqrt{\theta^{\top} \operatorname{Cov}_{e}\left(\mathbf{x}^{e}\left(\mathbf{x}^{e}\right)^{\top}\right) \theta}}\right)=\Phi_{z}\left(-\frac{\theta_{i}^{\top} \bar{\beta}_{i n v}+\theta_{s}^{\top} \bar{\beta}_{s p u}^{e}}{\sqrt{\sigma_{i}^{2}\left\|\theta_{i}\right\|_{2}^{2}+\sigma_{s}^{2}\left\|\theta_{s}\right\|_{2}^{2}}}\right)
$$

Thus when $m<d_{s p u}$, we have, by central limit theorem and (S3),

$$
\begin{align*}
\left\|\tilde{\theta}_{s}\right\|_{2} & =\alpha \sqrt{\overrightarrow{\mathbf{1}}^{\top} \Sigma_{\mathcal{S}} \overrightarrow{\mathbf{1}}} \leq \alpha \sqrt{m\left(\left\|\bar{\Sigma}_{\mathcal{S}}\right\|+\left\|\bar{\Sigma}_{\mathcal{S}}-\Sigma_{\mathcal{S}}\right\|\right)}=\alpha \tau_{s} \sqrt{m d_{s p u}}\left(1+\mathcal{O}_{p}\left(\left(m / d_{s p u}\right)^{1 / 4}\right)\right),  \tag{S4}\\
\tilde{\theta}_{s}^{\top} \bar{\beta}_{s p u}^{e} & =\alpha\left(\left\|\bar{\beta}_{s p u}^{e}\right\|_{2}^{2}+\sum_{e^{\prime} \in \mathcal{E}_{t r}, e^{\prime} \neq e}\left\langle\bar{\beta}_{s p u}^{e^{\prime}}, \bar{\beta}_{s p u}^{e}\right\rangle_{2}\right)=\alpha \tau_{s}^{2}\left(d_{s p u}+\mathcal{O}_{p}\left(\sqrt{m d_{s p u}}\right)\right) . \tag{S5}
\end{align*}
$$

Thus, when $m \ll \min \left\{1, \sigma_{s}^{-2} \tau_{s}^{2}\right\} d_{s p u}$, we have

$$
R_{e, 01}\left(f_{\tilde{\theta}}\right)=\Phi_{z}\left(-\sigma_{s}^{-1} \tau_{s}\left(\sqrt{d_{s p u} / m}+o_{p}(1)\right)\right) \leq \exp \left(-2 \sigma_{s}^{-2} \tau_{s}^{2} d_{s p u} / m+o_{p}(1)\right) \xrightarrow{p} 1, \quad \forall e \in \mathcal{E}_{t r}
$$

[^0]Now we consider the logistic loss. Fix any $e \in \mathcal{E}_{t r}$, and recall $\bar{\theta}_{e}:=\bar{\beta}_{s p u}^{e} / 2 \sigma_{s}^{2}$ defines the Bayes classifier given the spurious features $\mathbf{x}_{s p u}^{e} \in \mathbb{R}^{d_{s p u}}$. Introduce the random variables

$$
\mathbf{x} \sim \mathcal{N}\left(\bar{\beta}_{s p u}^{e}, \sigma_{s}^{2} I\right), \quad \mathbf{z}_{1}=\bar{\theta}_{e}^{\top} \mathbf{x}, \quad \mathbf{z}_{2}=\tilde{\theta}_{s}^{\top} \mathbf{x}
$$

so that

$$
\begin{aligned}
R_{e, l o g}(\tilde{\theta}) & =\mathbb{E}_{\mathbf{x}_{s p u}^{e}} \sum_{y \in\{ \pm 1\}} p\left(\mathbf{y}^{e}=y \mid \mathbf{x}_{s p u}^{e}\right) \log \left(1+e^{-y \tilde{\theta}^{\top} \mathbf{x}_{s p u}^{e}}\right) \\
& =\mathbb{E}_{\mathbf{z}_{1}, \mathbf{z}_{2}} \mathbf{1}\left\{\mathbf{z}_{1} \geq 0\right\} \log \left(1+e^{-\mathbf{z}_{2}}\right)+\mathbf{1}\left\{\mathbf{z}_{1}<0\right\} \log \left(1+e^{\mathbf{z}_{2}}\right) \\
& \leq \mathbb{E} \log \left(1+e^{-\mathbf{z}_{2}}\right)+\mathbb{E}\left(\mathbf{1}\left\{\mathbf{z}_{1}<0\right\} \max \left\{1,2 \mathbf{z}_{2}\right\}\right) \\
& \leq \underbrace{\mathbb{E} \log \left(1+e^{-\mathbf{z}_{2}}\right)}_{(I)}+\underbrace{\mathbb{E} \mathbf{1}\left\{\mathbf{z}_{1}<0\right\}}_{(I I)}+\underbrace{\mathbb{E} \mathbf{1}\left\{\mathbf{z}_{1}<0, \mathbf{z}_{2}>1 / 2\right\} 2 \mathbf{z}_{2}}_{(I I I)} .
\end{aligned}
$$

We will bound the three terms in turn. Before that, we first derive the joint distribution of $\left(\mathbf{z}_{1}, \mathbf{z}_{2}\right)$. By S4-S5, we have

$$
\mu_{2}:=\mathbb{E} \mathbf{z}_{2}=\alpha \tau_{s}^{2} d_{s p u}\left(1+o_{p}(1)\right), \sigma_{2}^{2}:=\operatorname{Var}\left(\mathbf{z}_{2}\right)=\sigma_{s}^{2} \alpha^{2} \tau_{s}^{2} m d_{s p u}\left(1+o_{p}(1)\right), \operatorname{Cov}\left(\mathbf{z}_{1}, \mathbf{z}_{2}\right)=\frac{1+o_{p}(1)}{2 \sigma_{s}^{2}} \alpha \tau_{s}^{2} d_{s p u}
$$

Moreover, we have

$$
\mu_{1}:=\mathbb{E} \mathbf{z}_{1}=\frac{\left\|\bar{\beta}_{s p u}^{e}\right\|_{2}^{2}}{2 \sigma_{s}^{2}}=\frac{\tau_{s}^{2}\left(d_{s p u}+\mathcal{O}_{p}\left(\sqrt{d_{s p u}}\right)\right)}{2 \sigma_{s}^{2}}, \quad \sigma_{1}^{2}:=\operatorname{Var}\left(\mathbf{z}_{1}\right)=\frac{1}{2} \mu_{1}
$$

We now return to the three terms for $R_{e, l o g}$. For (I), consider the decomposition

$$
\begin{aligned}
(I) & =\mathbb{E} \log \left(1+e^{-\mathbf{z}_{2}}\right) \mathbf{1}\left\{\mathbf{z}_{2}<-1 / 2\right\}+\mathbb{E} \log \left(1+e^{-\mathbf{z}_{2}}\right) \mathbf{1}\left\{-1 / 2<\mathbf{z}_{2}<A\right\}+\mathbb{E} \log \left(1+e^{-\mathbf{z}_{2}}\right) \mathbf{1}\left\{\mathbf{z}_{2}>A\right\} \\
& \leq \mathbb{E}\left(-2 \mathbf{z}_{2} \mid \mathbf{z}_{2}<-1 / 2\right) \mathbb{P}\left(\mathbf{z}_{2}<-1 / 2\right)+\mathbf{1}\left\{-1 / 2<\mathbf{z}_{2}<A\right\}+\log \left(1+e^{-A}\right) \\
& \stackrel{(i)}{\lesssim} e^{-\mu_{2}^{2} / 2 \sigma_{2}^{2}} \cdot\left(1+\frac{\sigma_{2}^{2}}{\mu_{2}}\right)+e^{-\left(\mu_{2}-A\right)^{2} / 2 \sigma_{2}^{2}}+\log \left(1+e^{-A}\right) \\
& \stackrel{(i i)}{\lesssim} e^{-\mu_{2}^{2} / 3 \sigma_{2}^{2}}+e^{-\left(\mu_{2}-A\right)^{2} / 2 \sigma_{2}^{2}}+e^{-A} \stackrel{(i i i)}{\lesssim} e^{-\mu_{2}^{2} / 3 \sigma_{2}^{2}}
\end{aligned}
$$

In the above, (i) follows by the Gaussian CDF bound and lemma S3 below, (ii) follows since $\mu_{2}^{2} \gg \sigma_{2}^{2} \gg 1, \alpha=$ $\mathcal{O}\left(\operatorname{poly}\left(d_{\text {spu }} / m\right)\right)$, and (iii) sets $A=\mu_{2} / 10$. Now,

$$
\begin{aligned}
(I I) & \leq e^{-\mu_{2}^{2} / 2 \sigma_{2}^{2}} \\
(I I I) & =\int_{1 / 2}^{\infty} 2 t \mathbb{P}\left(\mathbf{z}_{1}<0 \mid \mathbf{z}_{2}=t\right) \mathbb{P}_{\mathbf{z}_{2}}(d t) \leq \mathbb{P}\left(\mathbf{z}_{1}<0\right) \mathbb{E}\left(2 \mathbf{z}_{2} \mid \mathbf{z}_{2}>1 / 2\right) \lesssim e^{-\mu_{1}^{2} / 2 \sigma_{1}^{2}}\left(\mu_{2}+2 \sigma_{2} e^{-\mu_{2}^{2} / 2 \sigma_{2}^{2}}\right)
\end{aligned}
$$

where the first inequality follows because $\mathbf{z}_{1}$ and $\mathbf{z}_{2}$ are positively correlated, and $\mu_{2}>0$, and the second follows by an application of lemma S3. Combining, we can see that in the regime $m \ll \sigma_{s}^{-2} \tau_{s}^{2} d_{s p u}$, there exists $c_{1}, c_{2}>0$ s.t.

$$
R_{e, \log }(\tilde{\theta}) \leq(I)+(I I)+(I I I) \leq c_{1} e^{-c_{2} \tau_{s}^{2} d_{s p u} / m \sigma_{s}^{2}}
$$

This proves S1.
Proof for lemma $S 2$. For any $e_{1}, e_{2} \in \mathcal{E}_{t r}$ and fixed realizations of $\left\{\bar{\beta}_{s p u}^{e_{1}}, \bar{\beta}_{s p u}^{e_{2}}\right\}$ (i.e., the following display implicitly conditions on the two), we have

$$
\begin{aligned}
\mathrm{KL}_{i j}=\operatorname{KL}\left(p_{e_{1}}\left(\mathbf{y}, \tilde{\theta}_{s}^{\top} \mathbf{x}_{s}, \mathbf{x}_{i}\right) \| p_{e_{2}}\left(\mathbf{y}, \tilde{\theta}_{s}^{\top} \mathbf{x}_{s}, \mathbf{x}_{i}\right)\right) & =\mathbb{E}_{p_{e_{1}}} \log \frac{p_{e_{1}}\left(\mathbf{y}, \tilde{\theta}_{s}^{\top} \mathbf{x}_{s}, \mathbf{x}_{i}\right)}{p_{e_{2}}\left(\mathbf{y}, \tilde{\theta}_{s}^{\top} \mathbf{x}_{s}, \mathbf{x}_{i}\right)}=\mathbb{E}_{p_{e_{1}}} \log \frac{p_{e_{1}}\left(\tilde{\theta}_{s}^{\top} \mathbf{x}_{s} \mid \mathbf{y}, \mathbf{y}_{i}\right) p_{e_{1}}\left(\mathbf{y}, \mathbf{x}_{i}\right)}{p_{e_{2}}\left(\tilde{\theta}_{s}^{\top} \mathbf{x}_{s} \mid \mathbf{y}, \mathbf{y}_{i}\right) p_{e_{2}}\left(\mathbf{y}, \mathbf{x}_{i}\right)} \\
& =\mathbb{E}_{p_{e_{1}}} \log \frac{p_{e_{1}}\left(\tilde{\theta}_{s}^{\top} \mathbf{x}_{s} \mid \mathbf{y}\right)}{p_{e_{2}}\left(\tilde{\theta}_{s}^{\top} \mathbf{x}_{s} \mid \mathbf{y}\right)}=\operatorname{KL}\left(\mathcal{N}\left(\mu_{21}, \sigma_{2}^{2}\right) \| \mathcal{N}\left(\mu_{22}, \sigma_{2}^{2}\right)\right)
\end{aligned}
$$

where $\mu_{2 j}:=\left\langle\bar{\beta}_{s p u}^{e_{j}}, \tilde{\theta}_{s}\right\rangle_{2} \forall j \in[m]$, and $\sigma_{2}^{2}:=\sigma_{s}^{2}\left\|\tilde{\theta}_{s}\right\|_{2}^{2}$. Plugging in the expression for KL divergence between Gaussian distributions, we find, for all $i, j \in[m]$,

$$
\begin{align*}
& \mathrm{KL}_{i j}=\frac{\left(\mu_{2 i}-\mu_{2 j}\right)^{2}}{2 \sigma_{2}^{2}}=\frac{\alpha^{2}}{2 \sigma_{2}^{2}}\left(\sum_{k=1}^{m}\left(\Sigma_{\mathcal{S}}\right)_{i k}-\left(\Sigma_{\mathcal{S}}\right)_{j k}\right)^{2} \\
= & \frac{\alpha^{2}}{2 \sigma_{2}^{2}}\left(\sum_{k=1}^{m}\left(\Sigma_{\mathcal{S}}\right)_{i k}-\left(\bar{\Sigma}_{\mathcal{S}}\right)_{i k}+\sum_{k=1}^{m}\left(\bar{\Sigma}_{\mathcal{S}}\right)_{j k}-\left(\Sigma_{\mathcal{S}}\right)_{j k}+\sum_{k=1}^{m}\left(\bar{\Sigma}_{\mathcal{S}}\right)_{i k}-\left(\bar{\Sigma}_{\mathcal{S}}\right)_{j k}\right)^{2} \\
\leq & \frac{4 \alpha^{2}}{2 \sigma_{2}^{2}}\left(\left(\sum_{k=1}^{m}\left(\Sigma_{\mathcal{S}}\right)_{i k}-\left(\bar{\Sigma}_{\mathcal{S}}\right)_{i k}\right)^{2}+\left(\sum_{k=1}^{m}\left(\Sigma_{\mathcal{S}}\right)_{j k}-\left(\bar{\Sigma}_{\mathcal{S}}\right)_{j k}\right)^{2}\right) \\
= & \frac{2 \alpha^{2}}{\sigma_{2}^{2}}\left(\left(\overrightarrow{\mathbf{1}}^{\top}\left(\Sigma_{\mathcal{S}}-\bar{\Sigma}_{\mathcal{S}}\right) \mathbf{e}_{i}\right)^{2}+\left(\overrightarrow{\mathbf{1}}^{\top}\left(\Sigma_{\mathcal{S}}-\bar{\Sigma}_{\mathcal{S}}\right) \mathbf{e}_{j}\right)^{2}\right) \tag{S6}
\end{align*}
$$

where $\mathbf{e}_{i}=(\underbrace{\ldots, 0}_{(i-1) \text { zeros }}, 1,0, \ldots)$ denotes the $i$-th Euclidean basis. We thus have, by symmetry and the trace formula,

$$
\sum_{i=1}^{m} \sum_{j=1}^{m} \mathrm{KL}_{i j} \leq 2 m \cdot \sum_{l=1}^{m} \frac{2 \alpha^{2}}{\sigma_{2}^{2}}\left(\overrightarrow{\mathbf{1}}^{\top}\left(\Sigma_{\mathcal{S}}-\bar{\Sigma}_{\mathcal{S}}\right) \mathbf{e}_{l}\right)^{2}=2 m \cdot \sum_{l=1}^{m} \frac{2 \alpha^{2}}{\sigma_{2}^{2}} \overrightarrow{\mathbf{1}}^{\top}\left(\Sigma_{\mathcal{S}}-\bar{\Sigma}_{\mathcal{S}}\right)^{2} \overrightarrow{\mathbf{1}}
$$

Plugging in $(\mathrm{S} 3)$ with $\delta \leftarrow \sqrt{m / d_{s p u}}$ we find, when $d \geq 64 m$, on that event we have

$$
\begin{aligned}
\sum_{i=1}^{m} \sum_{j=1}^{m} \mathrm{KL}_{i j} & \leq \frac{4 \alpha^{2} m\|\overrightarrow{\mathbf{1}}\|_{2}^{2}\left\|\Sigma_{\mathcal{S}}-\bar{\Sigma}_{\mathcal{S}}\right\|^{2}}{\sigma_{2}^{2}} \stackrel{\boxed{\mathrm{S3}}}{\leq} \frac{4 \alpha^{2} m^{2} \cdot\left(4 \tau_{s} \sqrt{m}\right)^{2}}{\sigma_{2}^{2}}=\frac{64 \alpha^{2} \tau_{s}^{2} m^{3}}{\sigma_{s}^{2}\left\|\tilde{\theta}_{s}\right\|_{2}^{2}} \\
& \leq \frac{64 \alpha^{2} \tau_{s}^{2} m^{3}}{\sigma_{s}^{2} \alpha^{2} \tau_{s}^{2} m d_{s p u} / 4}=\frac{256 m^{2}}{\sigma_{s}^{2} d_{s p u}}
\end{aligned}
$$

where we note that $[\mathbf{S 4}$ holds on the same event. Therefore, on that event there always exist some $\ell \in[m]$ which is determined by $\left\{\bar{\beta}_{s p u}^{e}\right\}$ s.t.

$$
\sum_{j=1}^{m} \mathrm{KL}_{\ell j} \leq \frac{256 m}{\sigma_{s}^{2} d_{s p u}}
$$

This completes the proof.
Lemma S3. Let $\mathbf{z} \sim \mathcal{N}\left(\mu, \sigma^{2}\right), b<\mu$. Then we have
$\mathbb{E}(\mathbf{z} \mid \mathbf{z}<b) \stackrel{(i)}{=} \mu-\sigma \frac{\phi_{z}((b-\mu) / \sigma)}{\Phi_{z}((b-\mu) / \sigma)} \stackrel{(i i)}{\geq} b-\frac{\sigma^{2}}{\mu-b}, \mathbb{E}(\mathbf{z} \mid \mathbf{z}<b) \stackrel{(i)}{=} \mu+\sigma \frac{\phi_{z}((b-\mu) / \sigma)}{1-\Phi_{z}((b-\mu) / \sigma)} \leq \mu+\sigma \phi_{z}((b-\mu) / \sigma)$.
Proof. (i) is a known property of truncated normal distribution [Greene, 2003]. (ii) follows by the bound $\Phi_{z}(-x) \geq$ $\frac{x}{x^{2}+1} \phi_{z}(-x)$ Abramowitz et al. 1988.

## S2 PROOF FOR PROPOSITION 2

Throughout the proof we will work with the transformed data and parameters: $\mathbf{x}^{e} \leftarrow M^{-1} \mathbf{x}^{e}, \theta \leftarrow M^{\top} \theta$. This allows us to ignore the presence of $M$, as long as we replace $U$ with $U^{\prime}:=\|M\| U$. We also introduce the following notations:

$$
\begin{aligned}
d:=d_{i n v}+d_{s p u}, X: & :=\left\{x_{1}^{*}, \ldots, x_{n_{*}}^{*}\right\} \in \mathbb{R}^{n_{*} \times d}, Y:=\left\{y_{1}^{*}, \ldots, y_{n_{*}}^{*}\right\} \in \mathbb{R}^{n_{*} \times 1} \\
\bar{\theta}_{s p u}^{e} & :=\left(\bar{\beta}_{i n v}, \bar{\beta}_{s p u}^{e}\right), \mathcal{S}_{t r}:=\left\{\bar{\beta}_{s p u}^{e}: e \in \mathcal{E}_{t r}\right\} .
\end{aligned}
$$

Note that given the above transformation, $\bar{\theta}_{s p u}^{e}$ now parameterizes the Bayes predictor for environment $e$. And across all environment $e$, we will also have

$$
R^{e}(\theta)=\mathbb{E}_{\mathbf{x}^{e}, \mathbf{y}^{e}}\left(\theta^{\top} \mathbf{x}^{e}-\mathbf{y}^{e}\right)^{2}=\left\|\theta-\bar{\theta}_{s p u}^{e}\right\|_{2}^{2}+\sigma^{2}
$$

and the constraint set, for which we have fixed $\rho+\varepsilon_{n}=0$, reduces to

$$
\begin{aligned}
\mathcal{C}_{t r} & =\left\{\theta \in \mathbb{R}^{d}:\left\|\theta-\bar{\theta}_{s p u}^{e}\right\|_{2}^{2} \leq\left\|\bar{\theta}_{i n v}-\bar{\theta}_{s p u}^{e}\right\|_{2}^{2} \forall e \in \mathcal{E}_{t r}\right\} \\
& =\left\{\theta=\left(\beta_{i}, \beta_{s}\right) \in \mathbb{R}^{d}:\left\|\beta_{i}-\bar{\beta}_{\text {inv }}\right\|_{2}^{2}+\left\|\beta_{s}-\bar{\beta}_{s p u}^{e}\right\|_{2}^{2} \leq\left\|\bar{\beta}_{s p u}^{e}\right\|_{2}^{2} \forall e \in \mathcal{E}_{t r}\right\} \\
& \subset\left\{\theta=\left(\beta_{i}, \beta_{s}\right) \in \mathbb{R}^{d}:\left\langle\beta_{s}, \bar{\beta}_{s p u}^{e}\right\rangle_{2} \geq \frac{1}{2}\left\|\beta_{s}\right\|_{2}^{2} \forall e \in \mathcal{E}_{t r}\right\} .
\end{aligned}
$$

The constrained parameter space is

$$
\mathcal{F}=\left\{f_{\theta}:\|\theta\|_{2}^{2} \leq U^{\prime}, \theta \in \mathcal{C}_{t r}\right\}
$$

Note that by construction, $\bar{\theta}_{\text {inv }} \in \mathcal{F}$ always holds.
Our main taks is to establish improved metric entropy bounds for the following "localized" space:

$$
\partial \mathcal{F}_{\delta}:=\left\{f_{\theta}-f_{\theta^{\prime}}: f_{\theta}, f_{\theta^{\prime}} \in \mathcal{F},\left\|f_{\theta}-f_{\theta^{\prime}}\right\|_{n, 2}^{2}:=\frac{1}{n_{*}} \sum_{i=1}^{n_{*}}\left(f_{\theta}\left(x_{i}^{*}\right)-f_{\theta^{\prime}}\left(x_{i}^{*}\right)\right)^{2} \leq \delta\right\}
$$

We first note that
Lemma S4. When $n_{*} \geq 5 d$, there exists $c>0$ s.t.

$$
\begin{equation*}
\mathbb{P}_{X}\left(\forall \theta, \theta^{\prime} \in \mathbb{R}^{d}, \frac{1}{2}\left\|\theta-\theta^{\prime}\right\|_{2}^{2} \leq\left\|f_{\theta}-f_{\theta^{\prime}}\right\|_{n, 2}^{2} \leq 2\left\|\theta-\theta^{\prime}\right\|_{2}^{2}\right) \geq 1-e^{-c n_{*}} \tag{S7}
\end{equation*}
$$

Proof. By the fact that $\left\|f_{\theta}-f_{\theta^{\prime}}\right\|_{n, 2}=\left\|n_{*}^{-1 / 2} X\left(\theta-\theta^{\prime}\right)\right\|_{2}$, and the concentration of Gaussian covariance matrices [Wainwright, 2019, Theorem 6.1].

Proposition S5 (entropy bound). On the event S7] we have, for any $\zeta, \delta, t, Z>0$, with $\mathcal{S}_{t r}$-probability $\geq 1-\zeta$,

$$
\begin{aligned}
& \log N\left(\partial \mathcal{F}_{\delta},\|\cdot\|_{n, 2}, t\right) \leq \min \left\{d_{s p u} \log \left(1+\frac{c^{\prime} \delta}{e^{m Z^{2} \delta^{2} / 2} t}\right)+d_{s p u} \log \left(1+\frac{c^{\prime} Z \delta}{t}\right)\right. \\
& \left.\quad d_{s p u} \log \left(1+\frac{c^{\prime} \delta}{2^{-m / d_{s p u} t}}\right)\right\}+d_{\text {inv }} \log \left(1+\frac{c^{\prime} \delta}{t}\right)+\log \zeta^{-1}
\end{aligned}
$$

Proof. We condition on the event (S7] throughout the proof. Then, any $\theta=\left(\beta_{i}, \beta_{s}\right)$ s.t. $f_{\theta} \in \partial \mathcal{F}_{\delta}$ must satisfy

$$
\left\|\beta_{i}-\bar{\beta}_{i n v}\right\|_{2}^{2}+\left\|\beta_{s}\right\|_{2}^{2}=\left\|\theta-\bar{\theta}_{i n v}\right\|_{2}^{2} \stackrel{\text { S77 }}{\leq} 2\left\|f_{\theta}-f_{\bar{\theta}_{i n v}}\right\|_{n, 2}^{2} \leq 2 \delta^{2} \Rightarrow \max \left\{\left\|\beta_{i}-\bar{\beta}_{i n v}\right\|_{2},\left\|\beta_{s}\right\|_{2}\right\} \leq \sqrt{2} \delta
$$

and

$$
\beta_{s} \in \mathcal{C}_{s}:=\left\{\beta_{s}:\left\langle\beta_{s}, \bar{\beta}_{s p u}^{e}\right\rangle_{2} \geq \frac{1}{2}\left\|\beta_{s}\right\|_{2}^{2} \quad \forall e \in \mathcal{E}_{t r}\right\}
$$

By S7], we also know that a $\left(\|\cdot\|_{n, 2}, t\right)$-covering for $\partial \mathcal{F}_{\delta}$ can be constructed as the Cartesian product of a $\left(\|\cdot\|_{2}, t / 3\right)$ covering for the ball $\mathbb{B}_{i, \delta}:=\left\{\beta_{i} \in \mathbb{R}^{d_{i n v}}:\left\|\beta_{i}-\bar{\beta}_{\text {inv }}\right\|_{2} \leq \sqrt{2} \delta\right\}$, and a $\left(\|\cdot\|_{2}, t / 3\right)$-covering for $\mathcal{C}_{s} \cap \mathbb{B}_{s, \delta}$, where $\mathbb{B}_{s, \delta}:=\left\{\beta_{s} \in \mathbb{R}^{d_{s p u}}:\left\|\beta_{s}\right\|_{2} \leq \sqrt{2} \delta\right\}$. Thus, we have, for some $c, c^{\prime}>0$,

$$
\begin{align*}
\log N\left(\partial \mathcal{F}_{\delta},\|\cdot\|_{n, 2}, t\right) & \leq \log N\left(\mathbb{B}_{i, \delta},\|\cdot\|_{2}, c t\right)+\log N\left(\mathbb{B}_{s, \delta} \cap \mathcal{C}_{s},\|\cdot\|_{2}, c t\right) \\
& \leq d_{i n v} \log \left(1+c^{\prime} \delta / t\right)+\log N\left(\mathbb{B}_{s, \delta} \cap \mathcal{C}_{s},\|\cdot\|_{2}, c t\right) \tag{S8}
\end{align*}
$$

where the second inequality can be found as Wainwright [2019, Example 5.8]. It remains to bound $\log N\left(\mathbb{B}_{s, \delta} \cap \mathcal{C}_{s},\|\cdot\|_{2}, c t\right)$. For this purpose, first note that, for any fixed $\beta \neq 0$, we have

$$
\begin{align*}
\mathbb{P}_{\mathcal{S}_{t r}}\left(\beta \in \mathcal{C}_{s}\right) & =\prod_{e \in \mathcal{E}_{t r}} \mathbb{P}_{\bar{\beta}_{s p u}^{e} \sim \mathcal{N}\left(0, d_{s p u}^{-1}\right)}\left(\left\langle\beta, \bar{\beta}_{s p u}^{e}\right\rangle_{2} \geq \frac{1}{2}\|\beta\|_{2}^{2}\right) \\
& =\prod_{j=1}^{m} \mathbb{P}\left(\mathcal{N}\left(0, d_{s p u}^{-1}\|\beta\|_{2}^{2}\right) \geq \frac{1}{2}\|\beta\|_{2}^{2}\right) \leq \min \left\{e^{-m d_{s p u}\|\beta\|_{2}^{2} / 4}, 2^{-m}\right\} \tag{S9}
\end{align*}
$$

Introduce

$$
B_{s 1}:=\left\{\beta_{s} \in \mathbb{R}^{d_{s p u}}:\left\|\beta_{s}\right\|_{2} \leq \sqrt{2} Z \delta\right\}, \quad B_{s 2}:=\mathbb{B}_{s, \delta} \backslash B_{s 1},
$$

and $\mathrm{C}_{s 1}, \mathrm{C}_{s 2}$ be $(\|\cdot\|, c t)$-coverings for $B_{s 1}, B_{s 2}$ with the optimal cardinality. Then

$$
\begin{aligned}
\mathbb{E}_{\mathcal{E}_{t r}} N\left(\mathbb{B}_{s, \delta} \cap \mathcal{C}_{s},\|\cdot\|_{2}, c t\right) & \leq \sum_{\beta \in \mathrm{C}_{s 1}} \mathbb{P}\left(\beta \in \mathcal{C}_{s}\right)+\sum_{\beta \in \mathrm{C}_{s 2}} \mathbb{P}\left(\beta \in \mathcal{C}_{s}\right) \\
& \leq N\left(B_{s 1},\|\cdot\|, c t\right)+N\left(\mathbb{B}_{s, \delta},\|\cdot\|, c t\right) e^{-m d_{s p u} Z^{2} \delta^{2} / 2} \\
& \leq(1+c Z \delta / t)^{d_{s p u}}+\left(1+c^{\prime} \delta / t\right)^{d_{s p u}} e^{-M d_{s p u} Z^{2} \delta^{2} / 2}
\end{aligned}
$$

By Markov's inequality and the monotonicity of $\log (\cdot)$, we find that for all $\zeta \in(0,1)$, with $\mathcal{S}_{t r}$-probability $\geq 1-\zeta$,

$$
\begin{aligned}
\log N\left(\mathbb{B}_{s, \delta} \cap \mathcal{C}_{s},\|\cdot\|_{2}, c t\right) & \leq d_{s p u} \log \left(1+c^{\prime} Z \delta / t\right)+d_{s p u} \log \left(\frac{1+c^{\prime} \delta / t}{e^{M Z^{2} \delta^{2} / 2}}\right)+\log \zeta^{-1} \\
& <d_{s p u} \log \left(1+c^{\prime} Z \delta / t\right)+d_{s p u} \log \left(1+\frac{c^{\prime} \delta}{e^{M Z^{2} \delta^{2} / 2} \cdot t}\right)+\log \zeta^{-1}
\end{aligned}
$$

Plugging back to (S8) proves the first claim. The second claim (involving $2^{-m / d_{s p u}}$ ) can be proved similarly, by using the second case in (S9) (involving $2^{-m}$ ).

This allows us to prove our main result:
Proof for Proposition 2 It suffices to bound the critical radius $\hat{\delta}_{n}^{2}$ of the Gaussian complexity of $\partial \mathcal{F}_{\delta}$ Wainwright, 2019 , Eq. (13.42a)]; given a high-probability bound $\hat{\delta}_{n}^{2} \leq \delta_{n}^{2}$ that holds w. p. $1-\zeta^{\prime}$, we will have, with probability $\geq 1-\zeta^{\prime}-$ $c_{1} e^{-c_{2} n \delta_{n}^{2}}$,

$$
\begin{equation*}
\left\|f_{\hat{\theta}}-f_{\bar{\theta}_{i n v}}\right\|_{2}^{2} \stackrel{\text { ST] }}{\leq} 2\left\|f_{\hat{\theta}}-f_{\bar{\theta}_{i n v}}\right\|_{2}^{2} \leq c_{0}\left\|f_{\bar{\theta}_{i n v}}-f_{\bar{\theta}_{s p u}^{e}}\right\|_{2}^{2}+c_{1} \delta_{n}^{2}, \tag{S10}
\end{equation*}
$$

where the last inequality is Wainwright [2019, Theorem 13.13].
By Wainwright 2019, Corollary 13.7], any solution $\delta$ to the following inequality will bound $\hat{\delta}_{n}^{2}$ :

$$
\begin{equation*}
\frac{16}{\sqrt{n}} \int_{\delta^{2}}^{\delta} \sqrt{\log N\left(\partial \mathcal{F}_{\delta},\|\cdot\|_{n, 2}, t\right)} d t \leq \frac{\delta^{2}}{4 \sigma} \tag{S11}
\end{equation*}
$$

Let us restrict to $\delta \geq n^{-1 / 2}$ and bound the LHS. Define $t_{j}=2^{-j \delta}$ for $j \leq J:=\left\lceil\log n^{1 / 2} \delta\right\rceil$. Then

$$
\int_{\delta^{2}}^{\delta} \sqrt{\log N\left(\partial \mathcal{F}_{\delta},\|\cdot\|_{n, 2}, t\right)} d t \leq \sum_{j=0}^{J} \sqrt{\log N\left(\partial \mathcal{F}_{\delta},\|\cdot\|_{n, 2}, t_{j}\right)}\left(t_{j}-t_{j+1}\right)
$$

For any fixed $Z>0, \delta \geq n^{-1 / 2}$, a union bound over $J$ applications of proposition S 5 to $\left(\zeta \leftarrow n^{-10}, \delta, t \leftarrow t_{j}, Z\right)$ shows that, with $\mathcal{S}_{t r}$-probability $\geq 1-n^{-10} \log \left(n^{1 / 2} \delta\right)$,

$$
\begin{align*}
& \sum_{j=0}^{J} \sqrt{\log N\left(\partial \mathcal{F}_{\delta},\|\cdot\|_{n, 2}, t_{j}\right)}\left(t_{j}-t_{j+1}\right)<\sqrt{10 \log n} \delta+\sum_{j=0}^{J}\left(t_{j}-t_{j+1}\right) \cdot\left(d_{i n v} \log \left(1+\frac{c^{\prime} \delta}{t}\right)+\right. \\
&\left.d_{s p u} \log \left(1+\frac{c^{\prime} \delta}{e^{m Z^{2} \delta^{2} / 2} \cdot t}\right)+d_{s p u} \log \left(1+\frac{c^{\prime} Z \delta}{t}\right)\right)^{1 / 2} \\
& \leq \sqrt{10 \log n} \delta+\sum_{j=0}^{J}\left(t_{j}-t_{j+1}\right) \cdot\left(\sqrt{d_{i n v} \log \left(1+\frac{c^{\prime} \delta}{t}\right)}+\right. \\
&\left.\sqrt{d_{s p u} \log \left(1+\frac{c^{\prime} \delta}{e^{M Z^{2} \delta^{2} / 2} \cdot t}\right)}+\sqrt{d_{s p u} \log \left(1+\frac{c^{\prime} Z \delta}{t}\right)}\right) \tag{S12}
\end{align*}
$$

and that

$$
\begin{gather*}
\sum_{j=0}^{J} \sqrt{\log N\left(\partial \mathcal{F}_{\delta},\|\cdot\|_{n, 2}, t_{j}\right)}\left(t_{j}-t_{j+1}\right)<\sqrt{10 \log n} \delta+\sum_{j=0}^{J}\left(t_{j}-t_{j+1}\right)( \\
\left.\sqrt{d_{i n v} \log \left(1+\frac{c^{\prime} \delta}{t}\right)}+\sqrt{d_{s p u} \log \left(1+\frac{c^{\prime} \delta}{2^{m / d_{s p u} \cdot t}}\right)}\right) \tag{S13}
\end{gather*}
$$

By basic calculus and a scaling argument as in Wainwright [2019, p. 427], we find the summation is bounded by

$$
\sqrt{10 \log n} \delta+c^{\prime \prime}\left(\sqrt{d_{i n v}}+\min \left\{Z+e^{-m Z^{2} \delta^{2} / 2}, 2^{-m / d_{s p u}}\right\} \sqrt{d_{s p u}}\right) \delta
$$

Therefore, for any $Z, \delta_{0, n}>0$, any solution to

$$
\delta \geq \max \left\{\delta_{0, n}, n^{-1 / 2}\right\}, \sqrt{10 \log n} \delta+c^{\prime \prime}\left(\sqrt{d_{i n v}}+\min \left\{Z+e^{-m Z^{2} \delta_{0, n}^{2} / 2}, 2^{-m / d_{s p u}}\right\} \sqrt{d_{s p u}}\right) \delta \leq \frac{\sqrt{n} \delta^{2}}{64 \sigma^{2}}
$$

always solves S11 with the claimed probability. Choosing $\delta_{0, n}=\sqrt{Z^{2} d_{s p u} / n}, Z^{2}=\left(\frac{2 n \log m}{m d_{s p u}}\right)^{1 / 4}$ yields

$$
\delta_{n}^{2} \leq c^{\prime \prime \prime}\left(\frac{\log n+d_{i n v}}{n}+\sqrt{\frac{d_{s p u} \log m}{n m}}\right)
$$

while considering the second argument of min yields

$$
\delta_{n}^{2} \leq c^{\prime \prime \prime} \frac{\log n+d_{i n v}+2^{-2 m / d_{s p u}} d_{s p u}}{n}
$$

Both bounds hold with the aforementioned $\mathcal{S}_{t r}$-probability. Plugging back to S 10 completes the proof.

## S3 EXPERIMENT SETUP AND FULL RESULTS

## S3.1 FULL RESULTS FOR SECTION 6.1

Full results for all methods in the setting of Figure 1 are reported in Figure S1, where we add the results for BLR-LC for $N:=0.3 n_{*}$, BLR-Prior for $\alpha \in\{1,3\}$, and CBLR for $\rho=0.2$. The results are consistent with the discussion in the text. We have also conducted experiments in a larger-scale setting, with $n_{e} \leftarrow 12000$ for classification and $n_{e} \leftarrow 18000, d_{\text {inv }} \leftarrow$ $80, d_{\text {spu }} \leftarrow 160, m \leftarrow 5$ for regression. As shown in Figure $\mathbf{S} 2$, the results are qualitatively similar, with our methods performing slightly better for the regression task.

We further experimented with generalized variants of both the regression and classification experiments, where we replace the definition of $\bar{\beta}_{s p u}^{*}$ with

$$
\bar{\beta}_{s p u}^{*} \sim \mathcal{N}\left(\frac{2 \alpha}{m} \sum_{e \in \mathcal{E}_{t r}} \bar{\beta}_{s p u}^{e},\left(1-\alpha^{2}\right) \tau_{*}^{2} I\right)
$$

where $\tau_{*}=1$ for classification and $d_{\text {spu }}^{-1 / 2}$ for regression. For regression, we also introduce environment-specific correlations between the invariant and spurious features, by replacing the generating process of $x_{s p u, i}^{e}$ with

$$
x_{s p u, i}^{e} \sim \mathcal{N}\left(\beta A^{e} x_{i n v, i}^{e},\left(1-\beta^{2}\right) I\right),
$$

where $A^{e} \in \mathbb{R}^{d_{s p u} \times d_{i n v}}$ is a random matrix with i.i.d. $\mathcal{N}\left(0, d_{i n v}^{-1}\right)$ components. The data generating process in the text thus corresponds to $\alpha=1, \beta=0$. Results for other choices of $(\alpha, \beta)$ are reported in Figure S3 and Figure S4 where we plot the distribution of test losses across 32 independently samples for $\left\{\bar{\beta}_{i n v}, \bar{\beta}_{s p u}\right\}$. As we can see, our method remains competitive across all settings.


Figure S1: Synthetic experiment: results for all methods in the setting of Figure 1

## S3.2 SETUP AND RESULTS FOR SECTION 6.2

Full results for all methods in the setting of Table 1 and Table 2 are reported in Table $S 1$ and Table $S 2$, respectively, where we also report the results for our method with $\rho \in\{0.05,0.2\}$. As we can see, our method achieves robust performance across all settings. In order to maintain a high acceptance rate for the M-H test of the Langevin Monte Carlo steps, we set the step-size upper bound $\bar{\eta}_{k}=0.001$ for ColoredMNIST and $\bar{\eta}_{k}=0.0025$ for PACS using binary search. To guarantee convergence, we run $2 \times 10^{4}$ steps with 50 parallel chains for each method. In accordance with the ERM baseline, the batch size for the BLR-LC method is set to 32 for each domain. For the BLR-LC-N_train method, because of the relatively large number of training examples $n_{e}$ on Colored MNIST, we set $N:=0.02 n_{e}$ for Colored MNIST, while $N:=n_{e}$ for PACS. The training-domain validation set selection approach from [Gulrajani and Lopez-Paz, 2020] is used to search the ERM baseline through 20 hyperparameter configurations $\times 3$ trials, which is important for ERM to establish itself as a strong baseline.

## References

Milton Abramowitz, Irene A Stegun, and Robert H Romer. Handbook of mathematical functions with formulas, graphs, and mathematical tables, 1988.

William H Greene. Econometric analysis. Pearson Education India, 2003.
Ishaan Gulrajani and David Lopez-Paz. In Search of Lost Domain Generalization. arXiv:2007.01434 [cs, stat], July 2020. URLhttp://arxiv.org/abs/2007.01434, arXiv: 2007.01434.

David Krueger, Ethan Caballero, Joern-Henrik Jacobsen, Amy Zhang, Jonathan Binas, Dinghuai Zhang, Remi Le Priol, and Aaron Courville. Out-of-distribution generalization via risk extrapolation (rex). In International Conference on Machine Learning, pages 5815-5826. PMLR, 2021.

Martin J Wainwright. High-Dimensional Statistics: A Non-Asymptotic Viewpoint, volume 48. Cambridge University Press, 2019.



|  | ERM (train. only) |
| :---: | :---: |
|  | BLR (adapt. only) |
|  | BLR-LC-0.3_Nadapt |
|  | BLR-LC-Nadapt |
|  | BLR-LC-N_train |
|  | BLR-Prior-1 |
|  | BLR-Prior-10 |
|  | BLR-Prior-3 |
|  | CBLR-0.05 |
|  | CBLR-0.1 |
| --i- | CBLR-0.2 |
|  | CBLR-0.4 |

Figure S2: Synthetic experiment: results for all methods at a larger scale.


Figure S3: Synthetic classification experiment: violin plot of classification errors, across independently sampled environments, in the setting of Figure 1. From left to right: results for $\alpha \in\{0,0.5,1\}$. From top to bottom: results for $n_{*} \in\{4,32,256\}$. Best viewed when zoomed.


Figure S4: Synthetic regression experiment: violin plot of test MSE across independently sampled environments in the larger-scale setting $\left(n_{e}=18000, m=5, d=240\right)$. From left to right: results for $(\alpha, \beta) \in\{(0,0),(1,0),(1,0.5)\}$.

Table S1: Colored MNIST: test accuracy for all methods on all domains. We report the 20th percentile / mean / 80th percentile across 20 independent runs.

| $n_{*}$ | Method / $e_{*}$ | 0.1 | 0.2 | 0.9 |
| :---: | :---: | :---: | :---: | :---: |
| 0 | ERM | 88.5 | 87.2 | 71.5 |
|  | CBLR | $87.8 / 88.2 / 88.5$ | $86.7 / 87.0 / 87.3$ | $81.5 / 81.9 / 85.6$ |
| 4 | CBLR_0.05 | $87.8 / 87.9 / 88.0$ | $87.1 / 87.3 / 87.7$ | $79.8 / 81.9 / 85.9$ |
|  | CBLR_0.20 | $85.0 / 85.7 / 87.2$ | $86.0 / 86.6 / 87.6$ | $79.3 / 76.4 / 86.9$ |
|  | BLR | $75.2 / 80.6 / 88.1$ | $77.5 / 79.3 / 85.8$ | $88.4 / 87.5 / 90.0$ |
|  | BLR-LC-N_adapt | $88.1 / 88.0 / 88.7$ | $86.6 / 87.0 / 87.4$ | $80.5 / 81.8 / 85.6$ |
|  | BLR-LC-N_train | $88.3 / 88.4 / 88.5$ | $87.2 / 87.3 / 87.4$ | $67.9 / 69.3 / 71.1$ |
|  | DivDis | $88.4 / 88.4 / 88.5$ | $87.8 / 87.8 / 87.9$ | $70.7 / 70.7 / 70.9$ |
|  | CBLR | $87.8 / 88.2 / 88.5$ | $86.5 / 87.0 / 87.4$ | $85.0 / 85.7 / 87.1$ |
| 8 | CBLR_0.05 | $87.8 / 88.1 / 88.6$ | $87.0 / 87.2 / 87.5$ | $83.9 / 85.1 / 86.8$ |
|  | CBLR_0.20 | $85.4 / 86.1 / 88.0$ | $85.1 / 86.0 / 87.1$ | $85.3 / 86.7 / 88.9$ |
|  | BLR | $83.0 / 86.1 / 88.4$ | $80.9 / 81.7 / 86.5$ | $89.2 / 89.3 / 90.0$ |
|  | BLR-LC-N_adapt | $87.9 / 88.3 / 88.7$ | $87.0 / 87.1 / 87.5$ | $82.9 / 83.5 / 86.0$ |
|  | BLR-LC-N_train | $88.3 / 88.4 / 88.5$ | $87.2 / 87.3 / 87.4$ | $68.3 / 69.9 / 71.8$ |
|  | DivDis | $88.4 / 88.4 / 88.5$ | $87.8 / 87.8 / 87.8$ | $70.6 / 70.7 / 70.8$ |
| 16 | CBLR | $87.6 / 88.2 / 88.7$ | $86.8 / 87.0 / 87.4$ | $87.1 / 87.7 / 88.5$ |
|  | CBLR_0.05 | $87.9 / 88.1 / 88.6$ | $86.9 / 87.2 / 87.5$ | $86.4 / 87.0 / 87.9$ |
|  | CBLR_0.20 | $85.7 / 86.3 / 88.5$ | $86.0 / 86.5 / 87.3$ | $87.9 / 88.6 / 89.4$ |
|  | BLR | $86.0 / 87.4 / 88.5$ | $85.4 / 85.5 / 87.0$ | $89.1 / 89.4 / 90.0$ |
|  | BLR-LC-N_adapt | $88.3 / 88.5 / 88.7$ | $87.1 / 87.3 / 87.5$ | $83.9 / 84.9 / 86.9$ |
|  | BLR-LC-N_train | $88.2 / 88.4 / 88.6$ | $87.2 / 87.3 / 87.4$ | $70.1 / 71.4 / 73.4$ |
|  | DivDis | $88.4 / 88.4 / 88.5$ | $87.8 / 87.8 / 87.9$ | $70.7 / 70.7 / 70.8$ |
|  | CBLR | $88.2 / 88.5 / 88.8$ | $86.7 / 87.0 / 87.4$ | $88.6 / 88.8 / 89.1$ |
| 32 | CBLR_0.05 | $88.1 / 88.4 / 88.7$ | $87.0 / 87.2 / 87.5$ | $87.5 / 88.0 / 88.4$ |
|  | CBLR_0.20 | $87.2 / 87.7 / 88.5$ | $86.2 / 86.8 / 87.4$ | $89.1 / 89.4 / 89.7$ |
|  | BLR | $87.8 / 88.2 / 88.8$ | $86.3 / 86.8 / 87.3$ | $89.6 / 89.8 / 90.0$ |
|  | BLR-LC-N_adapt | $88.5 / 88.6 / 88.7$ | $87.2 / 87.3 / 87.5$ | $84.8 / 85.6 / 86.4$ |
|  | BLR-LC-N_train | $88.2 / 88.4 / 88.6$ | $87.2 / 87.3 / 87.4$ | $72.7 / 73.6 / 75.4$ |
|  | DivDis | $88.4 / 88.4 / 88.5$ | $87.8 / 87.8 / 87.9$ | $70.7 / 70.7 / 70.8$ |

Table S2: PACS: test accuracy for all methods on all domains. We report the 20 th percentile / mean / 80th percentile across 20 independent runs.

| $n_{*}$ | Method / $e_{*}$ | A | C | P | S |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 0 | ERM | 87.8 | 72.6 | 96.1 | 76.3 |
| 16 | CBLR | 87.8 / 88.5 / 89.5 | 80.8 / 81.7 / 82.7 | 96.7 / 97.1 / 97.6 | 77.6 / 78.3 / 79.5 |
|  | CBLR_0.05 | 86.6 / 87.4 / 88.8 | 79.5 / 80.2 / 81.6 | 96.1/96.7 / 97.3 | $76.1 / 76.9 / 78.0$ |
|  | CBLR_0.20 | 83.9 / 85.4 / 87.0 | 78.2 / 79.3 / 81.0 | 95.8 / 96.3 / 96.7 | 73.8 / 74.9 / 76.4 |
|  | BLR | 86.8 / 87.7 / 89.2 | $76.1 / 78.8$ / 82.9 | 95.5 / 96.1 / 97.0 | $70.1 / 72.5$ / 75.5 |
|  | BLR-LC-N_adapt | 88.3 / 88.7 / 89.5 | 81.8 / 82.6 / 83.5 | 97.0 / 97.3 / 97.6 | 77.8 / 78.7 / 79.9 |
|  | BLR-LC-N_train | $86.1 / 86.8 / 87.5$ | 79.7 / 80.0 / 80.6 | 96.7 / 96.9 / 97.0 | $76.1 / 76.4$ / 77.6 |
|  | DivDis | 85.1 / 85.6 / 86.3 | 79.3 / 79.3 / 79.7 | 96.4 / 96.8 / 97.6 | 77.7 / 78.0 / 79.1 |
| 32 | CBLR | 88.8 / 89.8 / 90.7 | 82.7 / 83.3 / 84.2 | 96.7 / 97.1 / 97.3 | 78.6 / 79.2 / 80.1 |
|  | CBLR_0.05 | 87.5 / 88.5 / 89.5 | 80.3 / 81.6 / 82.7 | 96.1/96.6 / 97.0 | $77.2 / 78.3 / 79.5$ |
|  | CBLR_0.20 | 86.1 / 87.0 / 88.5 | 79.5 / 80.8 / 82.1 | 96.1/96.4 / 97.0 | 75.4 / $76.8 / 78.2$ |
|  | BLR | 88.8 / 89.6 / 90.7 | 82.1 / 82.9 / 84.4 | 96.4/96.9 / 97.6 | 76.4 / 77.6 / 79.2 |
|  | BLR-LC-N_adapt | 89.0 / 89.5 / 90.2 | 81.6 / 82.5 / 83.8 | 97.0 / 97.3 / 97.6 | $76.4 / 77.0$ / 79.9 |
|  | BLR-LC-N_train | 86.1 / 86.9 / 87.5 | 79.7 / 80.3 / 81.0 | 96.7 / 97.0 / 97.3 | 75.9 / 76.4 / 77.5 |
|  | DivDis | 85.1 / 85.1 / 85.6 | 79.1 / 79.6 / 81.2 | 96.4/96.8/97.3 | 77.1 / 77.3 / 78.5 |
| 64 | CBLR | 89.7 / 90.8 / 91.7 | 84.2 / 85.0 / 85.7 | 97.0 / 97.4 / 97.9 | 79.9 / 80.5 / 81.4 |
|  | CBLR_0.05 | $89.0 / 89.4 / 90.2$ | 82.3 / 83.3 / 84.2 | 96.4/96.9 / 97.3 | 78.5 / 79.4 / 80.4 |
|  | CBLR_0.20 | 88.0 / 88.8 / 90.0 | 82.7 / 83.1 / 83.8 | 96.4/96.8 / 97.3 | 76.7 / 78.3 / 79.6 |
|  | BLR | 90.0 / 90.5 / 91.4 | 84.2 / 85.3 / 86.1 | 97.0/97.3/97.9 | 79.4 / 80.0 / 81.3 |
|  | BLR-LC-N_adapt | 89.2 / 90.0 / 90.7 | 82.3 / 82.7 / 84.4 | 97.0/97.2/97.6 | 77.6 / 79.0 / 80.5 |
|  | BLR-LC-N_train | 87.0 / 87.4 / 88.0 | 79.3 / 79.9 / 80.6 | 97.0 / $97.0 / 97.3$ | 75.5 / 76.3 / 77.2 |
|  | DivDis | 85.6 / 85.9 / 86.8 | 78.6 / 79.1 / 79.9 | 96.4/96.8 / 97.3 | 77.2 / $77.6 / 78.6$ |
| 128 | CBLR | 90.7/91.5/92.2 | 86.3 / 86.9 / 87.8 | 97.3 / 97.6 / 98.2 | 81.5 / 82.4 / 83.7 |
|  | CBLR_0.05 | 90.0 / 90.4 / 91.4 | 84.2 / 85.5 / 87.6 | 97.3/97.3/97.6 | 80.8 / 81.4 / 83.4 |
|  | CBLR_0.20 | 89.5 / 90.6 / 92.4 | 84.0 / 84.8 / 87.4 | 96.7/96.9 / 97.3 | 79.2 / 79.7 / 81.3 |
|  | BLR | 90.5 / 91.1 / 91.7 | 86.1 / 86.6 / 87.4 | 96.7/97.4/97.9 | 80.1 / 81.2 / 82.5 |
|  | BLR-LC-N_adapt | 89.2 / 89.9 / 90.7 | 82.7 / 83.2 / 84.2 | 97.0/97.3/97.9 | $79.1 / 79.8$ / 80.6 |
|  | BLR-LC-N_train | 86.6 / 87.2 / 88.0 | 79.5 / 80.4 / 81.2 | 96.7/97.0/97.3 | 75.7 / 76.4 / 77.6 |
|  | DivDis | 84.8 / 85.4 / 86.1 | 78.8 / 79.7 / 80.6 | 96.4/96.9 / 97.3 | 76.7 / 77.2 / 78.1 |
| 256 | CBLR | 91.9 / 92.5 / 92.9 | 86.3 / 86.7 / 88.5 | 97.6 / 97.9 / 98.2 | 83.7 / 84.2 / 85.1 |
|  | CBLR_0.05 | 91.9 / 92.3 / 92.7 | 78.4 / 82.9 / 87.6 | 97.3/97.5/97.9 | 82.9 / 83.5 / 84.2 |
|  | CBLR_0.20 | 91.4/91.9/92.4 | 85.7 / 86.9 / 88.7 | 97.3/97.5/97.9 | $81.8 / 82.9 / 83.8$ |
|  | BLR | 91.4/91.8 / 92.4 | 85.9 / 86.5 / 87.4 | 97.3/97.6/98.2 | 80.6 / 81.7 / 82.8 |
|  | BLR-LC-N_adapt | 89.7 / 90.0 / 90.5 | 80.8 / 82.5 / 84.2 | 97.0/97.4/97.9 | $77.2 / 78.3 / 80.1$ |
|  | BLR-LC-N_train | 87.5 / 87.9 / 88.5 | 79.9 / 80.4 / 81.0 | 96.7/96.8 / 97.0 | $76.9 / 77.2 / 78.5$ |
|  | DivDis | 85.3 / 85.8 / 87.0 | 80.6 / 80.6 / 80.8 | 96.7 / 96.9 / 97.3 | 76.3 / 77.0 / 78.1 |


[^0]:    ${ }^{1}$ In practice, soft constraints based on gradient penalty are used for IRM. But it is easy to adapt our proof to show that the gradient norm $\left\|\nabla_{w} R_{e, l o g}(w \circ \Phi)\right\|_{2}=\left\|\nabla_{\tilde{\theta}} R_{e, l o g} f_{\tilde{\theta}}\right\|_{2}$ vanishes at a similar exponential rate. Thus, such a $(w, \Phi)$ pair is also an approximate optima for the soft constraint-based formulation.

