Incorporating Interpretable Output Constraints in Bayesian Neural Networks

Wanqian Yang
Harvard University
Cambridge, MA, USA
yangw@college.harvard.edu

Lars Lorch∗
ETH Zürich
8092 Zürich, Switzerland
llorch@student.ethz.ch

Moritz A. Graule
Harvard University
Cambridge, MA, USA
graulem@g.harvard.edu

Himabindu Lakkaraju
Harvard University
Cambridge, MA, USA
hlakkaraju@seas.harvard.edu

Finale Doshi-Velez
Harvard University
Cambridge, MA, USA
finale@seas.harvard.edu

Abstract
Domains where supervised models are deployed often come with task-specific constraints, such as prior expert knowledge on the ground-truth function, or desiderata like safety and fairness. We introduce a novel probabilistic framework for reasoning with such constraints and formulate a prior that enables us to effectively incorporate them into Bayesian neural networks (BNNs), including a variant that can be amortized over tasks. The resulting Output-Constrained BNN (OC-BNN) is fully consistent with the Bayesian framework for uncertainty quantification and is amenable to black-box inference. Unlike typical BNN inference in uninterpretable parameter space, OC-BNNs widen the range of functional knowledge that can be incorporated, especially for model users without expertise in machine learning. We demonstrate the efficacy of OC-BNNs on real-world datasets, spanning multiple domains such as healthcare, criminal justice, and credit scoring.

1 Introduction
In domains where predictive errors are prohibitively costly, we desire models that can both capture predictive uncertainty (to inform downstream decision-making) as well as enforce prior human expertise or knowledge (to induce appropriate model biases). Performing Bayesian inference on deep neural networks, which are universal approximators [11] with substantial model capacity, results in BNNs — models that combine high representation power with quantifiable uncertainty estimates [21, 20] 1. The ability to encode informative functional beliefs in BNN priors can significantly reduce the bias and uncertainty of the posterior predictive, especially in regions of input space sparsely covered by training data [27]. Unfortunately, the trade-off for their versatility is that BNN priors, defined in high-dimensional parameter space, are uninterpretable. A general approach for incorporating functional knowledge (that human experts might possess) is therefore intractable.

Recent work has addressed the challenge of incorporating richer functional knowledge into BNNs, such as preventing miscalibrated model predictions out-of-distribution [9], enforcing smoothness constraints [2] or specifying priors induced by covariance structures in the dataset (cf. Gaussian processes) [25, 19]. In this paper 2, we take a different direction by tackling functional knowledge expressed as output constraints — the set of values \( y \) is constrained to hold for any given \( x \). Unlike other types of functional beliefs, output constraints are intuitive, interpretable and easily specified,

∗Work done while at Harvard University.
1See Appendix A for a technical overview of BNN inference and acronyms used throughout this paper.
2Our code is publicly available at: https://github.com/dtak/ocbnn-public.
We propose a sampling-based prior that assigns probability mass to BNN parameters based on how well the BNN output obeys constraints on drawn samples. The resulting Output-Constrained BNN (OC-BNN) allows the user to specify any constraint directly in its functional form, and is amenable to all black-box BNN inference algorithms since the prior is ultimately evaluated in parameter space.

Our contributions are: (a) we present a formal framework that lays out what it means to learn from output constraints in the probabilistic setting that BNNs operate in, (b) we formulate a prior that enforces output constraint satisfaction on the resulting posterior predictive, including a variant that can be amortized across multiple tasks, (c) we demonstrate proof-of-concepts on toy simulations and apply OC-BNNs to three real-world, high-dimensional datasets: (i) enforcing physiologically feasible interventions on a clinical action prediction task, (ii) enforcing a racial fairness constraint on a recidivism prediction task where the training data is biased, and (iii) enforcing recourse on a credit scoring task where a subpopulation is poorly represented by data.

2 Related Work

Noise Contrastive Priors Hafner et al. [9] propose a generative “data prior” in function space, modeled as zero-mean Gaussians if the input is out-of-distribution. Noise contrastive priors are similar to OC-BNNs as both methods involve placing a prior on function space but performing inference in parameter space. However, OC-BNNs model output constraints, which encode a richer class of functional beliefs than the simpler Gaussian assumptions encoded by NCPs.

Global functional properties Previous work have enforced various functional properties such as Lipschitz smoothness [2] or monotonicity [29]. The constraints that they consider are different from output constraints, which can be defined for local regions in the input space. Furthermore, these works focus on classical NNs rather than BNNs.

Tractable approximations of stochastic process inference Garnelo et al. [7] introduce neural processes (NP), where NNs are trained on sequences of input-output tuples \( \{(x, y)\}_{i=1}^{m} \) to learn distributions over functions. Louizos et al. [19] introduce a NP variant that models the correlation structure of inputs as dependency graphs. Sun et al. [25] define the BNN variational objective directly over stochastic processes. Compared to OC-BNNs, these models represent a distinct direction of work, since (i) VI is carried out directly over function-space terms, and (ii) the set of prior functional assumptions is different; they cannot encode output constraints of the form that OC-BNNs consider.

Equality/Inequality constraints for deep probabilistic models Closest to our work is that of Lorenzi and Filippone [18], which incorporates equality and inequality constraints, specified as differential equations, into regression tasks. Similar to OC-BNNs, constraint (C) satisfaction is modeled as the conditional \( p(Y, C|X) \), e.g. Gaussian or logistic. However, we (i) consider a broader framework for reasoning with constraints, allowing for diverse constraint formulations and defined for both regression and classification tasks, and (ii) verify the tractability and accuracy of our approach on a comprehensive suite of experiments, in particular, high-dimensional tasks.

3 Notation

Let \( X \in X \) where \( X = \mathbb{R}^{Q} \) be the input variable and \( Y \in Y \) be the output variable. For regression tasks, \( Y = \mathbb{R} \). For \( K \)-classification tasks, \( Y \) is any set with a bijection to \( \{0, 1, \ldots, K - 1\} \). We denote the ground-truth mapping (if it exists) as \( f^*: X \rightarrow Y \). While \( f^* \) is unknown, we have access to observed data \( D_{tr} = \{x_i, y_i\}_{i=1}^{N} \), which may be noisy or biased. A conventional BNN is denoted as \( \Phi_{W} : X \rightarrow Y \). \( W \in \mathcal{W} \), where \( \mathcal{W} = \mathbb{R}^{M} \), are the BNN parameters (weights and biases of all layers) represented as a flattened vector. All BNNs that we consider are multilayer perceptrons with RBF activations. Uppercase notation denotes random variables; lowercase notation denotes instances.

4 Output-Constrained Priors

In joint \( X \times Y \) space, our goal is to constrain the output \( y \) for any set of inputs \( x \). In this setting, classical notions of “equality” and “inequality” (in constrained optimization) respectively become positive constraints and negative constraints, specifying what values \( y \) can or cannot take.
Definition 4.1. A deterministic output constraint \( \mathcal{C} \) is a tuple \((\mathcal{C}_x, \mathcal{C}_y, \circ)\) where \( \mathcal{C}_x \subseteq \mathcal{X} \), \( \mathcal{C}_y : \mathcal{C}_x \to 2^Y \) and \( \circ \in \{\in, \notin\} \). \( \mathcal{C} \) is satisfied by an output \( y \) iff \( \forall x \in \mathcal{C}_x, y \circ \mathcal{C}_y(x) \). \( \mathcal{C}^+ := \mathcal{C} \) is a positive constraint if \( \circ \) is \( \in \), \( \mathcal{C} \) is a negative constraint if \( \circ \) is \( \notin \). \( \mathcal{C} \) is a local constraint if \( \mathcal{C}_x \subset \mathcal{X} \).

The distinction between positive and negative constraints is not trivial because the user typically has access to only one of the two forms. Positive constraints also tend to be more informative than negative constraints. Definition 4.1 alone is not sufficient as we must define what it means for a BNN, which learns a predictive distribution, to satisfy a constraint \( \mathcal{C} \). A natural approach is to evaluate the probability mass of the prior predictive that satisfies a constraint.

Definition 4.2. A deterministic output constraint \( \mathcal{C} = (\mathcal{C}_x, \mathcal{C}_y, \circ) \) is \( \epsilon \)-satisfied by a BNN with prior \( \mathcal{W} \sim p(\mathcal{W}) \) if, \( \forall x \in \mathcal{C}_x \) and for some \( \epsilon \in [0, 1] \):

\[
\int_Y \mathbb{I}[y \circ \mathcal{C}_y(x)] \cdot p(\Phi \mathcal{W} = y | x) \, dy \geq 1 - \epsilon
\]  

(1)

where \( p(\Phi \mathcal{W} | x) := \int_{\mathcal{W}} p(\Phi \mathcal{W}(x) | x, \mathcal{W}) \, p(\mathcal{W}) \, d\mathcal{W} \) is the BNN prior predictive.

The strictness parameter \( \epsilon \) can be related to hard and soft constraints in optimization literature; the constraint is hard iff \( \epsilon = 0 \). Note that \( \epsilon \) is not a parameter of our prior, instead, (1) is the goal of inference and can be empirically evaluated on a test set. Since BNNs are probabilistic, we can generalize Definition 4.1 further and specify a constraint directly as some distribution over \( Y \).

Definition 4.3. A probabilistic output constraint \( \mathcal{C} \) is a tuple \((\mathcal{C}_x, \mathcal{D}_y)\) where \( \mathcal{C}_x \subseteq \mathcal{X} \) and \( \mathcal{D}_y(x) \) is a distribution over \( Y \). (That is, \( \mathcal{D}_y \), like \( \mathcal{C}_y \), is a partial function well-defined on \( \mathcal{C}_x \).) \( \mathcal{C} \) is \( \epsilon \)-satisfied by a BNN with prior \( \mathcal{W} \sim p(\mathcal{W}) \) if, \( \forall x \in \mathcal{C}_x \) and for some \( \epsilon \in [0, 1] \):

\[
D_{DIV} \left( p(\Phi \mathcal{W} | x) \ \| \ \mathcal{D}_y(x) \right) \leq \epsilon
\]  

(2)

where \( D_{DIV} \) is any valid measure of divergence between two distributions over \( Y \).

We seek to construct a prior \( \mathcal{W} \sim p(\mathcal{W}) \) such that the BNN \( \epsilon \)-satisfies, for some small \( \epsilon \), a specified constraint \( \mathcal{C} \). An intuitive way to connect a prior in parameter space to \( \mathcal{C} \) (defined in function space) is to evaluate how well the implicit distribution of \( \Phi \mathcal{W} \), induced by the distribution of \( \mathcal{W} \), satisfies \( \mathcal{C} \). In Section 4.1, we construct a prior that is conditioned on \( \mathcal{C} \) and explicitly factors in the likelihood \( p(C | \mathcal{W}) \) of constraint satisfaction. In Section 4.3, we present an amortized variant by performing variational optimization on objectives (1) or (2) directly.

4.1 Conditional Output-Constrained Prior

A fully Bayesian approach requires a proper distribution that describes how well any \( \mathcal{W} \in \mathcal{W} \) satisfies \( \mathcal{C} \) by way of \( \Phi \mathcal{W} \). Informally, this distribution must be conditioned on all \( x \in \mathcal{C}_x \) (though we sample finitely during inference) and is the “product” of how well \( \Phi \mathcal{W}(x) \) satisfies \( \mathcal{C} \) for each \( x \in \mathcal{C}_x \). This notion can be formalized by defining \( \mathcal{C} \) as a stochastic process indexed on \( \mathcal{C}_x \).

Let \( x \in \mathcal{C}_x \) be any single input. In measure-theoretic terms, the corresponding output \( Y : \Omega \to \mathcal{Y} \) is defined on some probability space \((\Omega, \mathcal{F}, \mathbf{P}_{g,x})\), where \( \Omega \) and \( \mathcal{F} \) are the typical sample space and \( \sigma \)-algebra, and \( \mathbf{P}_{g,x} \) is any valid probability measure corresponding to a distribution \( p_g(\cdot | x) \) over \( \mathcal{Y} \). Then \((\Omega, \mathcal{F}, \mathbf{P}_g)\) is the joint probability space, where \( \Omega := \prod_{x \in \mathcal{C}_x} \Omega \), \( \mathcal{F} \) is the product \( \sigma \)-algebra and \( \mathbf{P}_g := \prod_{x \in \mathcal{C}_x} \mathbf{P}_{g,x} \) is the product measure (a pushforward measure from \( \mathbf{P}_{g,x} \)). Let \( \mathcal{C}P : \Omega \to \mathcal{Y}^{\mathcal{C}_x} \) be the stochastic process indexed by \( \mathcal{C}_x \), where \( \mathcal{Y}^{\mathcal{C}_x} \) denotes the set of all measurable functions from \( \mathcal{C}_x \) into \( \mathcal{Y} \). The law of the process \( \mathcal{C}P \) is \( p(S) = \mathbf{P}_g \circ \mathcal{C}P^{-1}(S) \) for all \( S \in \mathcal{Y}^{\mathcal{C}_x} \).

For any finite subset \( \{Y^{(1)}, \ldots, Y^{(T)}\} \subseteq \mathcal{C}P \) indexed by \( \{x^{(1)}, \ldots, x^{(T)}\} \subseteq \mathcal{C}_x \),

\[
p(Y^{(1)} = y^{(1)}, \ldots, Y^{(T)} = y^{(T)}) \equiv \prod_{t=1}^{T} p_g(Y^{(t)} = y^{(t)} | x^{(t)})
\]  

(3)

\( \mathcal{C}P \) is a valid stochastic process as it satisfies both (finite) exchangeability and consistency, which are sufficient conditions via the Kolmogorov Extension Theorem [23]. As the BNN output \( \Phi \mathcal{W}(x) \) can be evaluated for all \( x \in \mathcal{C}_x \) and \( \mathcal{W} \in \mathcal{W} \), \( \mathcal{C}P \) allows us to formally describe how much \( \Phi \mathcal{W} \) satisfies \( \mathcal{C} \) by determining the measure of the realization \( \Phi \mathcal{W} \in \mathcal{Y}^{\mathcal{C}_x} \).
Definition 4.4. Let $C$ be any (deterministic or probabilistic) constraint and $CP$ the the stochastic process defined on $Y^x$ for some measure $P_y$. The conditional output-constrained prior (COCP) on $W$ is defined as
\[ p_C(w) = p_f(w)p(\Phi_w^C) \] (4) 
where $p_f(w)$ is any distribution on $W$ that is independent of $C$, and $\Phi_w^C \in Y^x$ is the realization of $CP$ corresponding to the BNN output $\Phi_w(x)$ for all $x \in C_x$.

We can view (4) loosely as an application of Bayes’ Rule, where the realization $\Phi_w^C$ of the stochastic process $CP$ is the evidence (likelihood) of $C$ being satisfied by $w$ and $p_f(w)$ is the unconditional prior over $W$. This implies that the posterior that we are ultimately inferring is $W|D_tr, CP$, i.e. with extra conditioning on $CP$. To ease the burden on notation, we will drop the explicit conditioning on $CP$ and treat $p_C(w)$ as the unconditional prior over $W$. To make clear the presence of $C$, we will denote the constrained posterior as $p_C(w|D_tr)$. Definition 4.4 generalizes to multiple constraints $C^{(1)}, \ldots, C^{(m)}$ by conditioning on all $C^{(i)}$ and evaluating $\Phi_w$ for each constraint. Assuming the constraints to be mutually independent, $p_{C^{(1)},\ldots,C^{(m)}}(w) = p_f(w) \prod_{i=1}^m p(\Phi_w^{C^{(i)}})$.

It remains to describe what measure $P_y$ we should choose such that $p(\Phi_w^C)$ is a likelihood distribution that faithfully evaluates the extent to which $C$ is satisfied. For probabilistic output constraints, we simply set $p_y(\cdot|y)$ to be $D_y(x)$. For deterministic output constraints, we propose a number of distributions over $Y$ that corresponds well to $C_y$, the set of permitted (or excluded) output values.

Example: Positive Mixture of Gaussian Constraint A positive constraint $C^+$ for regression, where $C_y(x) = \{y_1, \ldots, y_K\}$ contains multiple values, corresponds to the situation wherein the expert knows potential ground-truth values over $C_x$. A natural choice is the Gaussian mixture model:
\[ CP(x) \sim \sum_{k=1}^K \omega_k N(y_k, \sigma_k^2), \] where $\sigma_C$ is the standard deviation of the Gaussian, a hyperparameter controlling the strictness of $C$ satisfaction, and $\omega_k$ are the mixing weights: $\sum_{k=1}^K \omega_k = 1$.

Example: Positive Dirichlet Constraint For K-classification, the natural distribution to consider is the Dirichlet distribution, whose support (the standard K-simplex) corresponds to the K-tuple of predicted probabilities on all classes. For a positive constraint $C^+$, we specify:
\[ CP(x) \sim Dir(\alpha); \quad \alpha_i = \begin{cases} \gamma & \text{if } i \in C_y(x) \\ \gamma(1-c) & \text{otherwise} \end{cases} \quad \text{where } \gamma \geq 1, \ 0 < c < 1 \] (5)

Example: Negative Exponential Constraint A negative constraint $C^-$ for regression takes $C_y(x)$ to be the set of values that cannot be the output of $x$. For the case where $C_y$ is determined from a set of inequalities of the form $\{g_i(x, y) \leq 0, \ldots, g_i(x, y) \leq 0\}$, where obeying all inequalities implies that $y \in C_y(x)$ and hence $C^-$ is not satisfied, we can consider an exponential distribution that penalizes $y$ based on how each inequality is violated:
\[ p_y(CP(x) = y|x) \propto \exp \left\{-\gamma \cdot \prod_{i=1}^I \sigma_{\tau_i, \tau_i}(g_i(x, y))\right\} \] (6)
where $\sigma_{\tau_i, \tau_i}(z) = \frac{1}{2}(\tanh(-\tau_i z) + 1)(\tanh(-\tau_i z) + 1)$ and $\gamma$ is a decay hyperparameter. The sigmoidal function $\sigma_{\tau_i, \tau_i}(g_i(x, y'))$ is a soft indicator of whether $g_i \leq 0$ is satisfied. $p_y(CP(x) = y|x)$ is small if every $g_i(x, y') \leq 0$, i.e. all inequalities are obeyed and $C^-$ is violated.

4.2 Inference with COCPs
A complete specification of (4) is sufficient for inference using COCPs, as the expression $p_C(w)$ can simply be substituted for that of $p(w)$ in all black-box BNN inference algorithms. Since (4) cannot be computed exactly due to the intractability of $p(\Phi_w^C)$ for uncountable $C_x$, we will draw a finite sample $\{x(t)|T\}_{t=1}$ of $x \in C_x$ (e.g. uniformly across $C_x$ or Brownian sampling if $C_x$ is unbounded) at the start of the inference process and compute (3) as an estimator of $p(\Phi_w^C)$ instead:
\[ \tilde{p}_C(w) = p_f(w) \prod_{t=1}^T p_y(\Phi_w(x^{(t)})|x^{(t)}) \] (7)
The computational runtime of COCPs increases with the input dimensionality $Q$ and the size of $C_x$. However, we note that many sampling techniques from statistical literature can be applied to COCPs in lieu of naive uniform sampling. We use the isotropic Gaussian prior for $p_f(w)$. 

4
Posterior predictive plots.

was intentionally chosen. Unlike the naive baseline BNN, the OC-BNN satisfies the constraint, with As (8) and (9) are defined for a specific $x \in \mathcal{X}$, the predictive variance smoothly narrowing as $x$ approaches $\mathcal{X}$ so as to be entirely confined within $\mathcal{Y} - \mathcal{C}_y$. After posterior inference, the OC-BNN fits all data points in $D_{tr}$ closely while still respecting the constraint. Far from $\mathcal{C}_x$, the OC-BNN is not overconfident, maintaining a wide variance like the baseline. Figure 2 shows an analogous example for classification. Similarly, the OC-BNN fits the data and respects the constraint within $\mathcal{C}_x$, without showing a strong preference for any class OOD.

OC-BNNs can capture global input-output relationships between $\mathcal{X}$ and $\mathcal{Y}$, subject to sampling efficacy. Figure 3a shows an example where we enforce the constraint $xy \geq 0$. Even though the
Figure 2: 2D 3-classification with the positive constraint: $C^+_x = (1, 3) \times (-2, 0)$ and $C^+_y = \{\text{green}\}$. The main plots are the OC-BNN predictives; insets are the baselines. Input region is shaded by the predicted class if above a threshold certainty. The positive Dirichlet COCP (5) is used. In both the prior and posterior, the constrained region (green rectangle) enforces the prediction of the green class.

Figure 3: (a) 1D regression with the positive constraint: $C^+_x = \mathbb{R}$ and $C^+_y(x) = \{y \mid x \cdot y \geq 0\}$ (green), using AOCP. (b) 1D regression with the negative constraint: $C^-_x = [-1, 1]$ and $C^-_y = [1, 2.5]$ (red), with the negative exponential COCP (6). The 50 SVGD particles represent functions passing above and below the constrained region, capturing two distinct predictive modes. (c) Fraction of rejected SVGD particles (out of 100) for the OC-BNN (blue, plotted as a function of log-samples used with COCP) and the baseline (black). All baseline particles were rejected, however, only 4% of particles were rejected, using just only 5 COCP samples.

training data itself adheres to this constraint, learning from $D_{tr}$ alone is insufficient. The OC-BNN posterior predictive narrows significantly (compared to the baseline) to fit the constraint, particularly near $x = 0$. Note, however, that OC-BNNs can only learn as well as sampling from $C_x$ permits.

**OC-BNNs can capture posterior multimodality.** As NNs are highly expressive, BNN posteriors can contain multiple modes of significance. In Figure 3b, the negative constraint is specified in such a way as to allow for functions that fit $D_{tr}$ to pass both above or below the constrained region. Accordingly, the resulting OC-BNN posterior predictive contains significant probability mass on either side of $C_y$. Importantly, note that the negative exponential COCP does not explicitly indicate the presence of multiple modes, showing that OC-BNNs naturally facilitate mode exploration.

**OC-BNNs can model interpretable desiderata represented as output constraints.** OC-BNNs can be used to enforce important qualities that the system should possess. Figure 4 demonstrates a fairness constraint known as **demographic parity**:

$$p(Y = 1|x_A = 1) = p(Y = 1|x_A = 0)$$  \hspace{1cm} (10)

where $x_A$ is a protected attribute such as race or gender. (10) is expressed as a probabilistic output constraint. The OC-BNN not only learns to respect this constraint, it does so in the presence of conflicting training data ($D_{tr}$ is an unfair dataset).

**Sensitivity to Inference and Conflicting Data** Figure 5 in Appendix D shows the same negative constraint used in Figure 1, except using different inference algorithms. There is little difference in these predictive plots besides the idiosyncrasies unique to each algorithm. Hence **OC-BNNs behave reliably on, and are agnostic to, all major classes of BNN inference.** If $C$ and $D_{tr}$ are incompatible, such as with adversarial or biased data, the posterior depends on (i) model capacity and (ii) factors affecting the prior and likelihood, e.g. volume of data or OC-BNN hyperparameters. For example, Figure 6 in Appendix D shows a BNN with enough capacity to fit both the noisy data.
Figure 4: 2D binary classification. Suppose a hiring task where $X_1$ (binary) indicates membership of a protected trait (e.g., gender or race) and $X_2$ denotes skill level. Hence a positive (orange) classification should be correlated with higher values of $X_2$. The dataset $D_{tr}$ displays historic bias, where members of the protected class ($x_1 = 1$) are discriminated against ($Y = 1$ iff $x_1 = 1, x_2 \geq 0.8$, but $Y = 1$ iff $x_1 = 0, x_2 \geq 0.2$). A naive BNN (a) would learn an unfair linear separator. However, learning the probabilistic constraint: $D_y(x)$ as the distribution where $p(\Phi(x) = 1) = x_2$ with the AOCP allows the OC-BNN (b) to learn a fair separator, despite a biased dataset.

as well as ground-truth constraints, resulting in “overfitting” of the posterior predictive. However, the earlier example in Figure 4 prioritizes the fairness constraint, as the small size of $D_{tr}$ constitutes weaker evidence.

### Ensuring Hard Constraints using Rejection Sampling
A few SVGD particles in Figure 3b violate the constraint. While COCPs cannot guarantee $\epsilon = 0$ satisfaction, hard constraints can be practically enforced. Consider the idealized, truncated predictive distributions of the baseline BNN and OC-BNN, whereby for each $x \in C_x$, we set $p(Y = y|x) = 0$ where the constraint is violated and normalize the remaining density to 1. These distributions represent zero constraint violation (by definition) and can be obtained via rejection sampling from the baseline BNN or OC-BNN posteriors. Figure 3c shows the results of performing such rejection sampling, using the same setup as Figure 3b. As shown, rejection sampling is intractable for the baseline BNN (not a single SVGD particle accepted), but works well on the OC-BNN, even when using only a small sample count from $C_x$ to compute $p_C(w)$. This experiment shows not only that naive rejection sampling (on ordinary BNNs) to weed out posterior constraint violation is futile, but also that doing the same on OC-BNNs is a practical workaround to ensure that hard constraints are satisfied, which is generally difficult to achieve in ideal, probabilistic settings.

### 6 Experiments with Real-World Data

To demonstrate the efficacy of OC-BNNs, we apply meaningful and interpretable output constraints on real-life datasets. As our method is the first such work for BNN classification, the baseline that we compare our results to is an ordinary BNN with the isotropic Gaussian prior. Experimental details for all three applications can be found in Appendix C.

#### 6.1 Application: Clinical Action Prediction

<table>
<thead>
<tr>
<th></th>
<th>Train Accuracy</th>
<th>$F_1$ Score</th>
<th>Test Accuracy</th>
<th>$F_1$ Score</th>
<th>Constraint Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>BNN</td>
<td>0.713</td>
<td>0.548</td>
<td>0.738</td>
<td>0.222</td>
<td>0.783</td>
</tr>
<tr>
<td>OC-BNN</td>
<td>0.735</td>
<td>0.565</td>
<td>0.706</td>
<td>0.290</td>
<td>0.136</td>
</tr>
</tbody>
</table>

Table 1: Compared to the baseline, the OC-BNN maintains equally high accuracy and $F_1$ score on both train and test sets. The violation fraction decreased about six-fold when using OC-BNNs.

The MIMIC-III database [12] contains physiological features of intensive care unit patients. We construct a dataset ($N = 405K$) of 8 relevant features and consider a binary classification task of whether clinical interventions for hypotension management — namely, vasopressors or IV fluids — should be taken for any patient. We specify two **physiologically feasible**, positive (deterministic) constraints: (1) if the patient has high creatinine, high BUN and low urine, then action should be taken ($C_y = \{1\}$); (2) if the patient has high lactate and low bicarbonate, action should also be taken. The positive Dirichlet COCP (5) is used. In addition to **accuracy** and **$F_1$ score** on the test
Young adults tend to be disadvantaged by credit scoring models as their lack of credit history results in actionability constraint.

### Results
Table 1 summarizes the experimental results. The main takeaway is that OC-BNNs maintain classification accuracy while reducing constraint violations. The results show that OC-BNNs match standard BNNs on all predictive accuracy metrics, while satisfying the constraints to a far greater extent. This is because the constraints are intentionally specified in input regions out-of-distribution, and hence incorporating this knowledge augments what the OC-BNN learns from $D_{tr}$ alone. This experiment affirms the low-dimensional simulations in Section 5, showing that OC-BNNs are able to obey interpretable constraints without sacrificing predictive power.

#### 6.2 Application: Recidivism Prediction
COMPAS is a proprietary model, used by the United States criminal justice system, that scores criminal defendants on their risk of recidivism. A study by ProPublica in 2016 found it to be racially biased against African American defendants [1, 16]. We use the same dataset as this study, containing 9 features on $N = 6172$ defendants related to their criminal history and demographic attributes. We consider the same binary classification task as in Slack et al. [24] — predicting whether a defendant is profiled by COMPAS as being high-risk. We specify the fairness constraint that the probability of predicting high-risk recidivism should not depend on race: for all $(C_k = \mathbb{R}^3)$ individuals, the high-risk probability should be identical to their actual recidivism history ($D_y$ is such that $p(y = 1) = \text{two\_year\_recid}$). The AOCP is used. $D_{tr}$ is incompatible with this constraint since COMPAS itself demonstrates racial bias. We train on two versions of $D_{tr}$ — with/without the inclusion of race as an explicit feature. As the dataset is small and imbalanced, we directly evaluate the training set. To measure c-satisfaction, we report the fraction of the sensitive attribute (African American defendants vs. non-African American defendants) predicted as high-risk recidivists.

### Results
Table 2 summarizes the results. By constraining recidivism prediction to the defendant’s actual criminal history, OC-BNNs strictly enforce a fairness constraint. On both versions of $D_{tr}$, the baseline BNN predicts unequal risk for the two groups since the output labels (COMPAS decisions) are themselves biased. This inequality is more stark when the race feature is included, as the model learns the explicit, positive correlation between race and the output label. For both datasets, the fraction of the two groups being predicted as high-risk recidivists equalized after imposing the constraint using OC-BNNs. Unlike the previous example, OC-BNNs have lower predictive accuracy on $D_{tr}$ than standard BNNs. This is expected since the training dataset is biased, and enforcing racial fairness comes at the expense of correctly predicting biased labels.

#### 6.3 Application: Credit Scoring Prediction
Young adults tend to be disadvantaged by credit scoring models as their lack of credit history results in them being poorly represented by data (see e.g. [14]). We consider the Give Me Some Credit dataset ($N = 133K$) [13], containing binary labels on whether individuals will experience impending financial distress, along with 10 features related to demographics and financial history. Motivated by Ustun et al. [26]’s work on recourse (defined as the extent that input features must be altered to change the model’s outcome), we consider the feature RevolvingUtilizationOfUnsecuredLines (RUUL), which has a ground-truth positive correlation with financial distress. We analyze how much a young adult under 35 has to reduce RUUL to flip their prediction to negative in three cases: (i) a BNN trained on the full dataset, (ii) a BNN trained on a blind dataset (age $\geq 35$), (iii) an OC-BNN with an actionability constraint: for young adults, predict “no financial distress” even if RUUL is large. The positive Dirichlet COCP (5) is used. In addition to scoring accuracy and $F_1$ score on the entire test set ($N = 10K$), we measure the effort of recourse as the mean difference of RUUL between the two outcomes ($\hat{Y} = 0$ or 1) on the subset of individuals where age $< 35$ ($N = 1.5K$).
Results As can be seen in Table 3, the ground-truth positive correlation between RUUL and the output is weak, and the effort of recourse is consequentially low. However, the baseline BNN naturally learns a stronger correlation, resulting in a higher effort of recourse. This effect is amplified if the BNN is trained on a limited dataset without data on young adults. When an actionability constraint is enforced, the OC-BNN reduces the effort of recourse without sacrificing predictive accuracy on the test set, reaching the closest to the ground-truth recourse.

<table>
<thead>
<tr>
<th>Test</th>
<th>Ground Truth</th>
<th>BNN (Full)</th>
<th>BNN (Blind)</th>
<th>OC-BNN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>0.890</td>
<td>0.871</td>
<td>0.895</td>
<td></td>
</tr>
<tr>
<td>$F_1$ Score</td>
<td>0.355</td>
<td>0.346</td>
<td>0.350</td>
<td></td>
</tr>
<tr>
<td>Effort of Recourse</td>
<td>0.287</td>
<td>0.419</td>
<td>0.529</td>
<td>0.379</td>
</tr>
</tbody>
</table>

Table 3: All three models have comparable accuracy on the test set. However, the OC-BNN has the lowest recourse effort (closest to ground truth).

7 Discussion

The usage of OC-BNNs depends on how we view constraints in relation to data. The clinical action prediction and credit scoring tasks are cases where the constraint is a complementary source of information, being defined in input regions where $D_{tr}$ is sparse. The recidivism prediction task represents the paradigm where $D_{tr}$ is inconsistent with the constraint, which serves to correct an existing bias. Both approaches are fully consistent with the Bayesian framework, whereby coherent inference decides how the likelihood and prior effects each shape the resulting posterior.

In contrast with [7, 19, 25], OC-BNNs take a sampling-based approach to bridge functional and parametric objectives. The simplicity of this can be advantageous — output constraints are a common currency of knowledge easily specified by domain experts, in contrast to more technical forms such as stochastic process priors. While effective sampling is a prerequisite for accurate inference, we note that the sampling complexity of OC-BNNs is tractable even at the dimensionality we consider in Section 6. Note that we sample in $X$-space, which is much smaller than $W$-space.

OC-BNNs are intuitive to formulate and work well in real-life settings. Even though COCPs and AOCPs echo well-known notions of data-based regularization, it is not immediately clear that these ideas are effectual in practice, and lead to well-behaved posteriors with appropriate output variance (both within and without constrained regions). Our work represents the first such effort (i) to create a broad framework for reasoning with diverse forms of output constraints, and (ii) that solidly demonstrates its utility on a corresponding range of real-life applications.

8 Conclusion

We propose OC-BNNs, which allow us to incorporate interpretable and intuitive prior knowledge, in the form of output constraints, into BNNs. Through a series of low-dimensional simulations as well as real-world applications with realistic constraints, we show that OC-BNNs generally maintain the desirable properties of ordinary BNNs while satisfying specified constraints. OC-BNNs complement a nascent strand of research that aims to incorporate rich and informative functional beliefs into deep Bayesian models. Our work shows promise in various high-stakes domains, such as healthcare and criminal justice, where both uncertainty quantification and prior expert constraints are necessary for safe and desirable model behavior.

Broader Impact

Our work incorporates task-specific domain knowledge, in the form of output constraints, into BNNs. We wish to highlight two key positive impacts. (1) OC-BNNs allow us to manipulate an interpretable form of knowledge. They can be useful even to domain experts without technical machine learning expertise, who can easily specify such constraints for model behavior. A tool like this can be used alongside experts in the real world, such as physicians or judges. (2) Bayesian models like BNNs and OC-BNNs are typically deployed in “high-stakes” domains, which include those with societal impact. We intentionally showcase applications of high societal relevance, such as recidivism prediction and credit scoring, where the ability to specify and satisfy constraints can lead to fairer and more ethical model behavior.
That being said, there are considerations and limitations. (1) If the model capacity is low (e.g. the BNN is small), constraints and model capacity may interact in unexpected ways that are not transparent to the domain expert. (2) Our sampling approach allows us to be very general in specifying constraints, but it also creates a trade-off between computational efficiency and accuracy of constraint enforcement. (3) Finally, the expert could mis-specify or even maliciously specify constraints. The first two considerations can be mitigated by careful optimization and robustness checks; the latter by making the constraints public and reviewable by others.

Acknowledgments and Disclosure of Funding

The authors are grateful to Srivatsan Srinivasan, Anirudh Suresh, Jiayu Yao and Melanie F. Pradier for contributions to an initial version of this work [28], as well as Gerald Lim, M.B.B.S. for helpful discussions on the clinical action prediction task. HL acknowledges support from Google. WY and FDV acknowledge support from the Sloan Foundation.

References


