What-If Reasoning with Counterfactual Gaussian Processes

Peter Schulam 1, Suchi Saria 1

Abstract
Answering “What if?” questions is important in many domains. For example, would a patient’s disease progression slow down if I were to give them a dose of drug A? Ideally, we answer our question using an experiment, but this is not always possible (e.g., it may be unethical). As an alternative, we can use non-experimental data to learn models that make counterfactual predictions of what we would observe had we run an experiment. In this paper, we propose a model to make counterfactual predictions about how continuous-time trajectories (time series) respond to sequences of actions taken in continuous-time. We develop our model within the potential outcomes framework of Neyman (1990) and Rubin (1978). One challenge is that the assumptions commonly made to learn potential outcome (counterfactual) models from observational data are not applicable in continuous-time as-is. We therefore propose a model using marked point processes and Gaussian processes, and develop alternative assumptions that allow us to learn counterfactual models from continuous-time observational data. We evaluate our approach on two tasks from healthcare: disease trajectory prediction and personalized treatment planning.

1. Introduction
What change to a click prediction model will have the largest impact on an online advertising firm’s revenue? Which drug, dosage, and frequency should a physician recommend to a patient with a chronic disease? These types of questions are commonly formalized using counterfactual queries about observable outcomes (see e.g., Pearl 2009; Bottou et al. 2013), such as “How many more users per day will click an ad if I include this feature in the model?”.

Ideally, we would get our answer by running an experiment and measuring the outcome under the different actions.

Experiments, however, are not always feasible. An alternative is to learn models from observational (non-experimental) data that can make counterfactual predictions of the outcomes we would have observed had we run an experiment (see e.g., Pearl 2009). The key challenge when learning from observational data is that it can be difficult to distinguish between statistical and causal relationships. For instance, consider a drug that is often given to sicker patients who are also more likely to die. Without accounting for this bias, a model might learn that the drug kills patients even if it is actually beneficial.

This challenge is commonly addressed using the potential outcomes framework (Neyman, 1990; Rubin, 1978), which models outcomes under different actions using a collection of random variables \( \{ Y[a] : a \in C \} \) indexed by actions \( a \) from a set of choices \( C \). Within this framework, we can clearly state assumptions that equate statistical models of observed data to statistical models of the potential outcomes (we will review these ideas later).

Counterfactual models have been used to answer “what if?” questions using observational data in a wide variety of domains. For example, in online advertising, Bottou et al. (2013) model the interaction between click prediction models, user intent, and advertiser bids in order to answer questions about how improvements to the click prediction model will change the probability that a user actually clicks an ad. Many have also studied counterfactual models for discrete time series data. For instance, in health care and epidemiology, Robins (1997) develop counterfactual models of a single outcome measured after a sequence of actions in discrete time. Brodersen et al. (2015) build counterfactual models to estimate the impact that a single, discrete event has on a time series of interest (e.g. daily sales after a product launch).

In this paper, we use Gaussian processes (GPs; see e.g. Rasmussen and Williams 2006) to model counterfactual continuous-time trajectories \( \{ Y_t : t \in [0, \tau] \} \) within an interval \( [0, \tau] \) that predict the effects of sequences of actions taken in continuous-time. Figure 1 illustrates this idea with an example from health care. We show an individual with a disease that affects lung capacity, and would like to pre-
dict how her lung capacity will progress in response to different treatment plans. Panel (a) shows the history in the red box, which contains previous lung capacity measurements (black dots) and previous treatments (green and blue bars). Panels (b) and (c) illustrate the type of predictions we would like to make: given the history, what is the likely future trajectory of lung capacity under a single dose of Drug B (green) vs. under two doses of drug A (blue)?

We learn counterfactual GPs using collections of discrete and irregularly sampled observational traces of previous actions and trajectories, which we denote using

\[
\mathcal{D} \triangleq \left\{ \mathbf{h}_i = \{(t_{ij}, y_{ij}, a_{ij})\}_{j=1}^{n_i} \right\}_{i=1}^{m},
\]

where \(y_{ij}\) is an observation of the \(i^{th}\) trajectory at time \(t_{ij}\), and \(a_{ij}\) is an action at time \(t_{ij}\). We allow either \(y_{ij}\) or \(a_{ij}\) to be the null variable \(\emptyset\) (but not both) to account for times when an action was taken but an outcome was not observed, and vice versa. For example, the traces might consist of laboratory test results and drug prescriptions extracted from electronic health records. We emphasize that both the size and timing of traces are not shared across traces.

One challenge is that the assumptions typically made in the potential outcomes framework are not applicable to continuous-time traces (we elaborate later). To address this issue, we combine marked point processes (MPP; see e.g., Daley and Vere-Jones 2007) with GPs to model traces, and develop assumptions that equate our statistical model with the counterfactual models of interest.

We report experiments on two tasks in health care. First, we use our counterfactual GP for disease trajectory prediction (the task illustrated in Figure 1). The goal is to predict what an individual’s future trajectory will look like given their history, if the individual were given a specific treatment. Using simulated data, we compare our counterfactual model to a standard ML regression model (e.g., SVM or random forest, that predicts an outcome given past features), and show that the regression model is sensitive to the policy used in the training data, which hurts generalization. The counterfactual model, however, does not suffer from this. Simulations are commonly used to evaluate counterfactual predictions because accuracy cannot otherwise be measured without running a randomized experiment (see e.g., Brodersen et al. 2015).

Second, we report a qualitative experiment on a challenging real data set demonstrating how counterfactual GPs can be used for personalized treatment planning by making counterfactual predictions of disease progression under alternative treatment strategies. We cannot evaluate our counterfactual predictions using observational data alone, but we quantitatively check model fit on held out data against two baselines and report statistically significant improvements.

### 1.1. Related Work

The difference between counterfactual predictions of an outcome if an action had been taken and if it had not been taken is defined as the causal effect in the causal inference community (see e.g., Pearl 2009 or Morgan and Winship 2014). Potential outcomes are commonly used to formalize counterfactual predictions and obtain causal effect estimates (Neyman, 1990; Rubin, 1978); we will review them shortly. Potential outcomes are often applied to cross-sectional data (e.g., Bottou et al. 2013; Johansson et al. 2016), but have also been used to estimate the causal effect of a sequence of actions in discrete time on a final outcome (e.g. Robins 1997). Conversely, Brodersen et al. (2015) estimate the effect that a single discrete intervention has on a discrete time series.

Recent work on optimal dynamic treatment regimes uses the sequential potential outcomes framework proposed by Robins (1997) to learn lists of discrete-time treatment rules that optimize a scalar outcome. Algorithms for learning these rules often use value-function approximations (Q-learning; e.g., Nahum-Shani et al. 2012). Alternatively, A-learning directly learns the relative differences between
competing policies (Murphy, 2003). Others have extended the potential outcomes framework in Robins (1997) to learn causal effects of actions taken in continuous-time on a single final outcome using observational data. Lok (2008) proposes an estimator based on structural nested models (Robins, 1992) that learns the instantaneous effect of administering a single type of treatment. Arjas and Parner (2004) develop an alternative framework for causal inference using Bayesian posterior predictive distributions to estimate the effects of actions in continuous time on a final outcome. Xu et al. (2016) also learn effects of actions in continuous-time on outcomes measured in continuous-time, but make one-step-ahead scalar predictions. Both Lok (2008) and Arjas and Parner (2004) use marked point processes to formalize assumptions that make it possible to learn causal effects from continuous-time observational data. We build on these ideas to learn causal effects of actions on continuous-time trajectories instead of a single outcome.

Causal effects in continuous-time have also been studied using differential equations. Mooij et al. (2013) formalize an analog of Pearl’s “do” operation for deterministic ordinary differential equations. Sokol and Hansen (2014) make similar contributions for stochastic differential equations by studying limits of discrete-time non-parametric structural equation models (Pearl, 2009).

Reinforcement learning (RL) algorithms learn from data where actions and observations are interleaved in discrete time (see e.g., Sutton and Barto 1998). In RL, however, the focus is on learning a policy (a map from states to actions) that optimizes the expected reward, rather than a model that predicts the effects of the agent’s actions on future observations. In model-based RL, a model of an action’s effect on the subsequent state is produced as a by-product either offline before optimizing the policy (e.g., Ng et al. 2006) or incrementally as the agent interacts with its environment. In most RL problems, however, learning algorithms rely on active experimentation to collect samples, which is not always possible in domains like health care where frequent mistakes are unacceptable.

A related sub-problem within RL is off-policy evaluation (e.g., Dudík et al. 2011; Jiang and Li 2016; Păduaru et al. 2012) where the goal is to use observed traces of an agent operating under an unknown policy (that is, non-experimental data) to estimate the expected reward of another policy. Off-policy algorithms typically use value-function approximations, importance reweighting, or doubly robust combinations of the two to estimate the expected reward, which do not explicitly learn the effects of actions.

1.2. Background: Potential Outcomes

To formalize causality, we adopt the potential outcomes framework (Neyman, 1990; Rubin, 1978), which uses a collection of random variables \{Y[a] : a ∈ C\} to model the distribution over outcomes under each action \(a\) from a set of choices \(C\).

To make counterfactual predictions, we must learn the distribution \(P(Y[a])\) for each action \(a \in C\). If we can freely experiment by repeatedly taking actions and recording the effects, then it is straightforward to learn a probabilistic model for each potential outcome \(Y[a]\). Often, however, running experiments may not be possible because they are too expensive, too time-consuming, or not ethical.

An alternative approach is to use observational data, where we have example actions \(A\) and outcomes \(Y\), but do not know how actions were chosen. Note the difference between the action \(a\) and the random variable \(A\) that models the observed actions in our data. The index notation \(Y[a]\) serves to formally distinguish between the observed distribution \(P(Y \mid A = a)\) and the target distribution \(P(Y[a])\).

Without further assumptions, we can only use observational data to estimate \(P(Y \mid A = a)\), which may be different from \(P(Y[a])\) for two reasons. First, taking an action and observing that the action was taken are two different events. The latter is strictly more general, and so we must make an assumption that they are equivalent. Second, the actions may have been chosen using variables that are predictive of the outcome, which creates a non-causal statistical dependency between the action and outcome. These variables are known as confounders (Morgan and Winship, 2014). To handle these issues, we make the following two common assumptions.

**Assumption 1** (Consistency). Let \(Y\) be the observed outcome, \(A ∈ C\) be the observed action, and \(Y[a]\) be the potential outcome for action \(a ∈ C\), then the following conditional equivalence holds:

\[
(Y \overset{d}{=} Y[a]) \mid A = a.
\]

**Assumption 2** (No Unmeasured Confounders). Let \(Y\) be the observed outcome, \(A ∈ C\) be the observed action, \(X = x\) be a vector containing potential confounders, and \(Y[a]\) be the potential outcome under action \(a ∈ C\), then the following conditional independence holds:

\[
(Y[a] \perp A) \mid X = x.
\]

Using these assumptions, we can link the conditional distribution of the observed data to the distribution of the potential outcome

\[
P(Y \mid A = a, X = x) = P(Y[a] \mid A = a, X = x) = P(Y[a] \mid X = x),
\]

\[
(1)
\]

\[
(2)
\]
where Equation 1 is true under Assumption 1, and Equation 2 is true under Assumption 2. To estimate the marginal 
\( P(Y[a]) \), we can average the conditional distribution in Equation 2 with respect to an estimate of 
\( P(X) \).

To estimate causal effects from longitudinal clinical trials, Robins (1997) introduced an extension of Assumption 2 for discrete time series data. In a trial with \( n \) time points, a set of intermediate variables \( X_i \) is observed at each step \( i \in \{1, \ldots, n\} \), and an action \( A_i \) is then chosen based on \( X_i \) and all previous intermediate outcomes and actions \( \{(X_j, A_j)\}_{j=1}^{i-1} \). Finally, an outcome \( Y \) is measured after the completed follow-up. In order to make causal inferences about how a sequence of actions \( a_{1:n} \) affects the outcome, Robins (1997) uses the Sequential No Unobserved Confounders assumption, which posits that each observed action \( A_i \) depends only on previous intermediate outcomes \( X_{1:i-1} \) and actions \( A_{1:i-1} \), but no unobserved variables that are predictive of \( Y \). We will make a similar assumption to learn causal effects for continuous-time data.

2. Methods

We denote the trajectory (also referred to as the outcome) using \( \{Y_t : t \in [0, \tau]\} \), where \( Y_t \in \mathbb{Y} \) and \( [0, \tau] \) defines the interval of time over which the trajectory is defined. We use \( C \) to denote the set of possible action types, \( a \in C \) to denote the elements of the set, and define an action to be a 2-tuple \((a, t)\) specifying an action type \( a \in C \) and a time \( t \in [0, \tau] \) at which it is taken. To refer to multiple future actions, we use \( a = [(a_1, t_1), \ldots, (a_m, t_m)] \). We assume that an action \((a, t)\) may only affect future values of the outcome \( \{Y_{s} : s > t\} \) (a cause must precede its effect).

Finally, we define the history \( \mathcal{H}_t \) at a time \( t \in [0, \tau] \) to be a list of all previous observations of the outcome and all previous actions. Our goal is to make counterfactual predictions about the trajectory \( \{Y_t : t \in [0, \tau]\} \) under future actions \( a \) at any time \( t \) given the history \( \mathcal{H}_t \).

2.1. Counterfactual Gaussian Processes

We use potential outcomes to formalize our problem. For an arbitrary time \( t \in [0, \tau] \), let \( q = [s_q, \ldots, s_m] \) denote an ordered sequence of future times at which we would like to make counterfactual predictions of the outcome under a set of future actions \( a \). Using potential outcomes notation, we use GPs to model

\[
P(\{Y_s[a] : s \in q\} | \mathcal{H}_t).
\]

The vector \( q \) must be finite, but otherwise has no restrictions, so we can approximate the continuous trajectory arbitrarily well by using a dense grid.

To learn Equation 3, we use a collection of traces

\[
\mathcal{D} \triangleq \left\{ h_i = \{(t_{ij}, y_{ij}, a_{ij})\}_{j=1}^{n_i} \right\}_{i=1}^{m}.
\]

In the potential outcomes framework, we can learn from observational data if, after making Assumptions 1 and 2, we can show equivalence between conditional distributions learnable from data and the distributions of potential outcomes. However, Assumption 2 is not applicable to continuous-time traces. To see why, note that in general a sequence of actions for any trace in our training data will be unique (two actions are taken at the same time with probability zero), and so the sets of random variables representing observed actions across traces will be different. Assumption 2 is stated in terms of a random variable \( A \) modeling observed actions, and so it is no longer well-posed when there are different sets of random variables across observations. More formally, Assumption 2 places conditions on null events (events with probability zero), and so we need an alternative formulation (Lok, 2008).

To address this issue, we model traces using marked point processes (MPP; see e.g., Daley and Vere-Jones 2007) and Gaussian processes (GP; see e.g., Rasmussen and Williams 2006). We state an assumption analogous to Assumption 2 that is framed in terms of the MPP’s intensity function, and show that these assumptions allow us to link distributions learnable from the data \( \mathcal{D} \) to Equation 3.

2.2. Marked Point Processes

Point processes are distributions over sequences of timestamps \( \{T_i\}^N_{i=1} \), which we call points, and a marked point process (MPP) is a point process where each point is annotated with an additional random variable \( X_i \), called its mark. For example, a point \( T \) might represent the arrival time of a customer at a store, and we might annotate each customer arrival with the amount \( X \) that she ultimately spent at the store. If we use an MPP to model customer arrivals and spending over the course of the day, then \( \{(T_i, X_i)\}^N_{i=1} \) denotes the arrival times and amounts spent for all customers at the store for a given day. We emphasize that both the annotated points \( (T_i, X_i) \) and the number of points \( N \) are random variables. We review key ideas and notation below, but point to Daley and Vere-Jones (2007) for additional details.

A point process can be characterized as a counting process \( \{N_t : t \geq 0\} \) that counts the number of points that occurred up to and including time \( t \):

\[
N_t = \sum_{i=1}^{N} I(T_i \leq t).
\]

By definition, this processes can only take integer values, and \( N_t \geq N_s \) if \( t \geq s \). In addition, it is commonly assumed that \( N_0 = 0 \) and that \( \Delta N_t = \lim_{\delta \to 0^+} (N_{t+\delta} - N_t) \in \{0, 1\} \).
We can parameterize a point process using a probabilistic model of $\Delta N_t$ given the history of the process $\mathcal{H}_t$—up to but not including time $t$ (we use $t^-$ to denote the left limit of $t$). Using the Doob-Meyer decomposition, we can write $\Delta N_t = \Delta M_t + \Delta \Lambda_t$, where $M_t$ is a martingale and $\Lambda_t$ is a cumulative intensity function, and

$$P(\Delta N_t = 1 \mid \mathcal{H}_t^-) = E[\Delta N_t \mid \mathcal{H}_t^-] = E[\Delta M_t \mid \mathcal{H}_t^-] + \Delta \Lambda_t(\mathcal{H}_t^-) = 0 + \Delta \Lambda_t(\mathcal{H}_t^-),$$

which shows that we can parameterize the point process using the conditional intensity function

$$\lambda^*(t) \, dt \triangleq \Delta \Lambda_t(\mathcal{H}_t^-) = P(\Delta N_t = 1 \mid \mathcal{H}_t^-). \quad (5)$$

The star superscript on the intensity function serves as a reminder that it depends on the history $\mathcal{H}_t^-$. For example, in homogeneous Poisson processes, $\lambda^*(t)$ is a constant, while in non-homogeneous Poisson processes $\lambda^*(t)$ is a function of time that does not depend on the history $\mathcal{H}_t^-$ (see e.g., Daley and Vere-Jones 2007). On the other hand, a Hawkes process is an example of a point process where $\lambda^*(t)$ does depend on the history (Hawkes, 1971).

### MPPs are defined by an intensity that is a function of both the time $t$ and the mark $x$:

$$\lambda^*(t, x) = \lambda^*(t)p^*(x \mid t). \quad (6)$$

We have written the joint intensity in a factored form, where $\lambda^*(t)$ is the intensity of any point occurring (that is, the mark is unspecified), and $p^*(x \mid t)$ is the pdf of the observed mark given the point’s time. For an MPP, the history $\mathcal{H}_t$ contains each prior point’s time and mark.

#### 2.2.1. OUTCOMES AND ACTIONS IN MPPs

We frame our problem using MPPs by defining the mark space as the Cartesian product of the outcome space $\mathcal{Y}$ and the set of action types $\mathcal{C}$. To allow either the outcome or the action (but not both) to be the null variable $\emptyset$, we introduce binary random variables $z_y \in \{0, 1\}$ and $z_a \in \{0, 1\}$ to indicate when the outcome $y$ and action $a$ are not $\emptyset$. The mark space is therefore

$$\mathcal{X} = (\mathcal{Y} \cup \{\emptyset\}) \times (\mathcal{C} \cup \{\emptyset\}) \times \{0, 1\} \times \{0, 1\}$$

The pdf of the mark space can be factoredized

$$p^*(x \mid t) = p^*(y, a, z_y, z_a \mid t) = p^*(z_y, z_a \mid t)p^*(y \mid t, z_y)p^*(a \mid y, t, z_a), \quad (7)$$

where we have again used a $*$ superscript as a reminder that the density is implicitly conditioned on the history $\mathcal{H}_t^-$. From this factorization, we see that the MPP has four components: (1) the intensity function $\lambda^*(t)$, (2) the mark type distribution $p^*(z_y, z_a \mid t)$, (3) the outcome model $p^*(y \mid t, z_y)$, and (4) the action model $p^*(a \mid y, t, z_a)$.

### 2.3. Gaussian Process Trajectory Model

For a trace $h_i = \{(t_{ij}, y_{ij}, a_{ij})\}_{j=1}^{n_i}$, the outcome model determines the joint density over all outcome observations:

$$\prod_{j:z_{a_{ij}}=1} p^*(y_{ij} \mid t_{ij}, z_{y_{ij}}). \quad (8)$$

We parameterize this density using a mixture of Gaussian processes, and later show that, under appropriate assumptions, learning the parameters from observational traces is equivalent to learning Equation 3. We therefore do not need to specify the intensity, mark type model, or action model.

Let $K$ denote the number of mixture components, then we assume the following generative model

$$c_i \sim \text{Categorical}(\pi) \quad (9)$$
$$b_i \sim \text{Normal}(\beta_{c_i}, \Sigma_{c_i}) \quad (10)$$
$$\omega_i \sim \text{Normal}(\omega_{c_i}, S_{c_i}) \quad (11)$$
$$f_i \sim \text{GP}(\phi_c(\cdot)^\top b_i + \psi_c(\cdot \mid a)\top \omega_i, k_c(\cdot, \cdot)) \quad (12)$$
$$y_i \sim \text{Normal}(f_i(t), \sigma^2) \quad (13)$$

where $\phi_c(\cdot) \in \mathbb{R}^p$ is a basis modeling the trajectory under no interventions, and $\psi_c(\cdot \mid a) \in \mathbb{R}^q$ is a basis modeling the effect that the sequence of actions $a$ has on the outcome. The basis vector $\psi_c(t \mid a)$ for time $t$ can only depend on actions in $a$ that are taken before $t$. It is straightforward to include any baseline (time independent) features into the prior over $c_i$ and into the bases $\phi$ and $\psi$.

#### 2.4. Learning

We learn the model using the likelihood of traces $\{h_i\}_{i=1}^m$ observed over a fixed interval $[0, \tau]$. We discuss the likelihood function using a single trace, but we can learn from several iid traces by adding the likelihoods together. Let $\theta$ be the model parameters, then the likelihood is

$$\ell(\theta, \{(t_j, x_j)\}_{j=1}^{n}) = \sum_{j=1}^{n+1} \log p^*(t_j, x_j), \quad (14)$$

where the parameters $\theta$ are implicitly included on the right-hand side to reduce clutter, and $x_j = (y_j, a_j, z_{y_j}, z_{a_j})$. Note that we have included an additional non-random point and mark $(t_{n+1}, x_{n+1}) = (\tau, \emptyset)$ indicating that the process was censored at time $\tau$. Let $t_0 = 0$, then the pdf in each summand is

$$p^*(t_j, x_j) = \begin{cases} 
\lambda^*(t_j)p^*(x_j \mid t_j) \exp \{-\Lambda_j\} & \text{if } j \in \{1, \ldots, n\}, \\
\exp \{-\Lambda_j\} & \text{if } j = n+1,
\end{cases} \quad (15)$$

where $\Lambda_j = \int_{t_{j-1}}^{t_j} \lambda^*(t) \, dt$. In this paper, we learn model parameters using penalized maximum likelihood. More-
2.5. Learning Potential Outcomes for MPPs

We can now formally state the assumptions needed to learn counterfactual models from observational traces. The first assumption is an alternative to Assumption 2 and the Sequential No Unobserved Confounders assumption proposed by Robins (1997).

**Assumption 3** (Continuous-Time NUC). For all times \( t \) and all histories \( \mathcal{H}_{t-} \), the densities \( \lambda^*(t) \), \( p^*(z_y, z_a | t) \), and \( p^*(a | y, t, z_a) \) do not depend on \( Y_s[a] \) for all times \( s > t \) and all action sequences \( a \).

The key implication of this assumption is that the policy used to choose actions in the observational data did not depend on any unobserved information that is predictive of the future potential outcomes.

**Assumption 4** (Non-Informative Measurement Times). For all times \( t \) and any history \( \mathcal{H}_{t-} \), the following holds

\[
p^*(y | t, z_y = 1) = P(Y_t \in dy | \mathcal{H}_{t-}). \tag{16}
\]

Under Assumptions 1, 3, and 4, we can show that Equation 3 can be expressed using the MPP measurement component \( p^*(y | t, z_y = 1) \). Because this is a component of the posited statistical model, we can estimate it from data and use it to make causal predictions. The argument for this equivalence is in Section B of the supplementary material.

3. Experiments

We report experimental results on two health care-related tasks. First, we predict a counterfactual trajectory given a two year history, if the individual were treated at the current time. We compare our counterfactual model’s predictions against predictions made by a classical ML regression model that predicts outcomes given features. We show statistically significant improvements, and demonstrate that the ML regression model is sensitive to the treatment policy in the training data. Second, we perform a qualitative experiment that shows how our model’s counterfactual predictions can be used for personalized treatment planning.

For the first task, we use simulated data because measuring performance requires that we know the true counterfactuals (as is done in Brodersen et al. 2015). In the second experiment, we train the model on traces of the progression of interstitial lung disease (ILD) in patients with scleroderma, a complex autoimmune disease (Varga et al., 2012).

### 3.1. Simulated Data

We simulate trajectories from a mixture of three Gaussian processes (following Section 2.3) over a period of ten years.

<table>
<thead>
<tr>
<th>Bin</th>
<th>On-Policy Residual Δ</th>
<th>Off-Policy Residual Δ</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2, 4)</td>
<td>0.15 (0.12, 0.18)</td>
<td>0.18 (0.15, 0.21)</td>
</tr>
<tr>
<td>(4, 6)</td>
<td>0.98 (0.92, 1.04)</td>
<td>1.20 (1.13, 1.28)</td>
</tr>
<tr>
<td>(6, 8)</td>
<td>1.46 (1.39, 1.53)</td>
<td>1.47 (1.39, 1.54)</td>
</tr>
<tr>
<td>(8, 10)</td>
<td>1.72 (1.64, 1.79)</td>
<td>1.64 (1.55, 1.72)</td>
</tr>
</tbody>
</table>

Table 1. Mean paired differences between absolute residuals of predictions made by the statistical model and the counterfactual model on simulated data (and 95% CI). Results are scaled by inverse observation noise \( \sigma = 0.1 \). * superscript indicates statistical significance.

Each sampled trajectory is observed at random, irregular times. We also simulate two dynamic treatment policies. The first, denoted P1, is more likely to administer treatment if observations in the previous two years are low on average. The second, denoted P2, does the opposite (treatment is more likely if past observations are high). The treatment increases the outcome within a window \( h \) of its administration by a constant amount. We list further details of our simulation in Section A of the supplementary material. The simulation model satisfies Assumptions 1, 3, and 4.

#### 3.1.1. Disease Trajectory Prediction

We train two models to predict the future progression of a trajectory if the individual were treated at year two (but no other future times), given all previously observed outcomes and treatments at two years. The first model, which we refer to as the ML regression model, learns

\[
P(\{Y_s : s \in q\} | A = (a, 2), \mathcal{H}_2), \tag{17}
\]

which predicts the outcome given features (the treatment \( A \) and the history \( \mathcal{H}_2 \)). The second model, referred to as the counterfactual model, learns the distribution

\[
P(\{Y_s[a = (a, 2)] : s \in q\} | \mathcal{H}_2). \tag{18}
\]

Both models are mixtures of GPs (as described in 2.3), where the bases \( \phi(\cdot) \) and \( \psi(\cdot | a) \) match those used in the simulation (described in the supplementary material). Both models also use the correct number of mixture components \( K = 3 \) and treatment window size \( h = 2 \). They therefore have the same form, but they are trained using different objectives. For a given trace, let \( y_{2+} \) and \( a_{2+} \) denote the observations and actions taken after year two, and let \( y_2 \) and \( a_2 \) denote the observations and actions taken up to and including year two. The ML regression model maximizes

\[
\mathcal{L}_M = \int p(y_{2+}, a_{2+} | y_2, a_2) da_{2+} \tag{19}
\]

over all traces in the training data. On the other hand, the counterfactual model maximizes

\[
\mathcal{L}_C = p(y_{2+}[a_{2+}] | y_2, a_2). \tag{20}
\]
The difference is that $\mathcal{L}_M$ marginalizes over actions beyond year two (which are not needed to predict in the test set), while the $\mathcal{L}_C$ explicitly controls for the future actions.

Table 1 reports the results of the experiment. We sample a single set of train and test trajectories, then create two training sets and one test set by applying treatment policies. One training set is treated using policy P1, and the other is treated using policy P2. The test set is treated using policy P1. We refer to models fit to the P1 training set as “On-Policy” (since the test set uses P1 too), and models fit to the P2 training set as “Off-Policy”.

For both models, we predict using the mean of Equations 17 and 18 for the ML regression and counterfactual models respectively. To compare the two models’ predictions, we compute pairwise differences in absolute residuals $|\text{resid}_{\text{ML}} - |\text{resid}_{\text{Causal}}|$, and report the average difference and 95% CI using a pivotal bootstrap estimator. All numbers are scaled by the inverse of the observation noise $\sigma = 0.1$. The counterfactual model’s predictions are statistically significantly smaller in all time bins for both On-Policy and Off-Policy (at level $\alpha = 0.05$). Moreover, the counterfactual’s predictions are not statistically significantly different in the On-Policy and Off-Policy settings.

To understand this result, we highlight that the ML regression model (Equation 17) makes predictions by implicitly marginalizing over possible future actions using the distribution over actions in the training data, which depends on the training data policy. On the other hand, the counterfactual model explicitly controls for the actions in the training data, and so is robust to changes in treatment policy between training and test conditions. In the Off-Policy setting, the ML regression model performs poorly because there is a mismatch in distribution over actions due to different policies. In the On-Policy setting, there is no policy mismatch, but the ML regression model does not control for actions beyond two years.

This result has important consequences for the practice of building models from observational data. State-of-the-art predictive models (e.g., Alaa et al. 2016; Wu et al. 2016; Liwei et al. 2015; Schumal and Saria 2015; Wiens et al. 2016) do not explicitly control for future actions in the training data (compare Eq. 19 to 20), and are therefore sensitive to small changes in treatment policy, which compromises their reliability (Dyagilev and Saria, 2016). Counterfactual models do not have this issue, and offer a new, more reliable way to train predictive models.

3.2. Personalized Treatment Planning

Our model’s counterfactual predictions can be used for personalized treatment planning in clinical practice. By estimating an individual’s future disease progression under alternative treatment options, physicians and patients can consider the risks and benefits of each. We demonstrate this use case using traces of scleroderma-related interstitial lung disease (ILD), a leading cause of death among individuals with scleroderma (Varga et al., 2012).

**Data.** Our data set is extracted from the Johns Hopkins Hospital Scleroderma Center; one of the largest scleroderma patient registries in the world. To monitor ILD, clinicians use forced vital capacity, which is reported as a percentage of the expected capacity of a comparable, healthy individual (denoted PFVC). We consider four types of treatment in our analysis: prednisone (a steroid), methotrexate (an immunosuppressant), hydroxychloroquine (an immunosuppressant), and cyclophosphamide (an immunosuppressant).

We align individuals using their first visit to the clinic, and consider the 10 year period thereafter. We select individuals with at least 4 PFVC measurements, and exclude those who received a lung transplant, which causes sharp changes in PFVC. Our final cohort contains 395 individuals and a total of 2,818 PFVC measurements. The median number of PFVC observations per individual is 6 and the mean is 7.1 ± 3.3. We use 200 individuals to train, and hold out 195 for our evaluation. Our analysis is predicated on Assumptions 1, 3, and 4, which are reasonable in this data; clinicians primarily base treatment decisions for ILD on the previous trajectory of PFVC measurements.

**Model.** Individuals either have or do not have ILD, but the severity of ILD can vary. We therefore posit two mixture components: one uses a constant basis function $\phi_1(t) = 1$ for the baseline trajectory and the other uses a linear function $\phi_2(t) = [1, t]$. We allow individual-specific parameters $\mathbf{b}_i$ for both subtypes. For both subtypes, the effect at a given time $t$ of a drug is proportional to the cumulative number of times the individual has taken that medication. The basis $\psi_e$ is therefore 4-dimensional; one for each drug.

In exploratory analysis we found that treatment effects were heterogeneous. Some individuals do not respond to treatment, and, among those who do, the response can vary (this observation is also supported by recent trial results: Tashkin et al. 2016). We therefore model individual-specific parameters $\mathbf{w}_i \in \mathbb{R}^4$ for the treatment model, but also include additional binary latent variables that determine whether an individual will respond (have non-zero coefficient for that drug). We model the marginal distributions over the response binary variables independently, and so introduce four additional parameters $\{r_1, r_2, r_3, r_4\}$.

**Checking model fit.** We cannot validate Assumptions 1, 3, and 4 without checking our model’s predictions against experimental data. However, we can evaluate fit and compare to baselines to evaluate our modeling decisions. We compare fit on heldout data with two baselines. The first base-
What-If Reasoning with Counterfactual Gaussian Processes

Table 2. Average paired differences (with 95% CI) between residuals of both baselines and the proposed model. Positive values show that the proposed model has better fit. * superscript indicates statistical significance.

sequence of treatments will stabilize the patient and bring their PFVC back to baseline levels.

In the right column, we show a patient who has a similar starting PFVC as the first example (40–45 PFVC), but who receives Cytoxan consistently throughout the course of the disease. In the top-right, we show the model’s factual (treated) future trajectory assuming the declining subtype. Interestingly, this individual’s factual trajectory could plausibly reflect what the first individual’s would have been if they immediately received treatment. In the bottom-right, we see the model predicts that the patient would likely remain stable if treatment were stopped, but would not recover as much lung capacity. The physician can use this prediction to decide whether the small additional gain in lung capacity is worth additional drug exposure.

4. Discussion

We proposed counterfactual Gaussian processes to model the effects of actions taken in continuous-time on continuous-time outcome trajectories. We combined marked point processes with GPs to model observational traces, and showed that Assumptions 3 and 4 equate the statistical model to the counterfactual GP. To evaluate our approach, we reported results on two tasks in health care. In the first, we showed that our counterfactual GP makes more accurate predictions of future trajectories than standard ML regression models because the counterfactual model is robust to the treatment policy in the training data.

In the second, we used a challenging real health care data set to learn a counterfactual GP and showed how it can be used for personalized treatment planning. Our work suggests several exciting future research directions. The conclusions drawn from our models are conditioned upon a set of assumptions. Formal sensitivity analyses that assess the robustness of conclusions to deviations from the assumptions are critical if our models are to be incorporated into high-impact domains (see e.g., Robins et al. 2000; Scharfstein et al. 2014). Also, there may be other sufficient assumptions that allow us to learn counterfactual GPs and are also easier to validate in practice.
A. Simulated Data Details

Our simulated data set is generated from a mixture of three Gaussian processes over a period of ten years. For each component, we define \( \phi_c(.) \) to be a second-order B-spline basis (see, for example, Ch. 20 of Gelman et al. 2013) with five degrees of freedom and knots spaced uniformly over the ten year period. We assume only a single action type, and define \( \psi_c(t \mid \alpha) = \sum_{\alpha_i \in \alpha} \int_{0 \leq \nu \leq k} \) where \( h \) is a window size controlling the duration of a treatment's effect; we use \( h = 2 \). We do not include individual-specific parameters, and so the covariance function is simply \( k_c(t_1, t_2) = \sigma^2 \mathbb{I}_{(t_1 = t_2)} \) (we set \( \sigma^2 = 0.01 \)). We chose the mean function's weights for each component by hand to reflect (1) a stable trajectory, (2) a mildly declining trajectory, and (3) a rapidly declining trajectory. To simulate a single trajectory, we randomly sampled a component, sampled a number of observations from a Poisson distribution with mean 15, and sampled the times of the observations from a uniform distribution over the ten year period. We then sampled the GP at those observation times.

We also simulate a dynamic action policy. At each observation time, the previous two years of observations are averaged and passed through a logistic function to determine the probability of an action. If an action is taken, all outcomes in the next two years are increased by 0.5. Different policies are parameterized using a bias and weight applied to the prior outcome average before being passed through the logistic function.

B. Equivalence of MPP Outcome Model and Counterfactual Model

At a given time \( t \), we want to make predictions about the potential outcomes that we will measure at a set of future query times \( q = \{s_1, \ldots, s_m\} \) given a specified future sequence of actions \( a \). This can be written formally as

\[
P(\{Y_s[a] \mid s \in q\} \mid H_t)
\]

Without loss of generality, we can use the chain rule to factor this joint distribution over the potential outcomes. We choose a factorization in time order; that is, a potential outcome is conditioned on all potential outcomes at earlier times. We now describe a sequence of steps that we can apply to each factor in the product.

\[
P(\{Y_s[a] \mid s \in q\} \mid H_t) = \prod_{i=1}^{m} P(Y_{s_i}[a] \mid \{Y_s[a] \mid s \in q, s < s_i\}, H_t).
\]

Using Assumption 3, we can introduce random variables for marked points that have the same timing and actions as the proposed sequence of actions without changing the probability. Recall our assumption that actions can only affect future values of the outcome, so we only need to introduce marked points for actions taken at earlier times. Formally, we introduce the set of marked points for the potential outcome at each time \( s_i \)

\[
A_i = \{(t', \varnothing, a, 0, 1) : (t', a) \in a, t' < s_i\}.
\]

We can then write

\[
P(Y_{s_i}[a] \mid A_i, \{Y_s[a] \mid s \in q, s < s_i\}, H_t) = P(Y_{s_i}[a] \mid A_i, \{Y_s[a] : s \in q, s < s_i\}, \mathcal{H}_t).
\]

This step is analogous to the logic used going from Equation 1 to 2. In those equations, we use Assumption 2 to remove the random variable \( A \) from the conditioning information without changing the probability. We reverse that logic here by adding \( A_i \).

Now, under Assumption 1, after conditioning on \( A_i \), we can replace the potential outcome \( Y_{s_i}[a] \) with \( Y_{s_i} \). We therefore have

\[
P(Y_{s_i}[a] \mid A_i, \{Y_s[a] : s \in q, s < s_i\}, \mathcal{H}_t) = P(Y_{s_i} \mid A_i, \{Y_s : s \in q, s < s_i\}, \mathcal{H}_t).
\]

Similarly, because the set of proposed actions affecting the outcome at time \( s_i \) contain all actions that affect the outcome at earlier times \( s < s_i \), we can invoke Assumption 1 again and replace all potential outcomes at earlier times with the value of the observed process at that time.

\[
P(Y_{s_i} \mid A_i, \{Y_s : s \in q, s < s_i\}, \mathcal{H}_t) = P(Y_{s_i} \mid A_i, \{Y_s \in q, s < s_i\}, \mathcal{H}_t).
\]

Next, Assumption 4 posits that the outcome model \( p^*(y \mid t', z_y = 1) \) is the density of \( P(Y_{t'} \mid \mathcal{H}_t) \), which implies that the mark \( t', y, \varnothing, 1, 0 \) is equivalent to the event \( (Y_{t'} \in dy) \). Therefore, for each \( s_i \) define

\[
O_i = \{(s, Y_s, \varnothing, 1, 0) : s \in q, s < s_i\}.
\]

Using this definition, we can write

\[
P(Y_{s_i} \mid A_i, \{Y_s : s \in q, s < s_i\}, \mathcal{H}_t) = (Y_{s_i} \mid A_i, O_i, \mathcal{H}_t).
\]

The set of information \( (A_i, O_i, \mathcal{H}_t) \) is a valid history of the marked point process \( \mathcal{H}_{s_i} \) up to but not including time \( s_i \). We can therefore replace all information after the conditioning bar in each factor of Equation 23 with \( \mathcal{H}_{s_i} \).

\[
P(Y_{s_i} \mid A_i, O_i, \mathcal{H}_t) = P(Y_{s_i} \mid \mathcal{H}_{s_i}).
\]

Finally, by applying Assumption 4 again, we have

\[
P(Y_{s_i} \in dy \mid \mathcal{H}_{s_i}) = p^*(y \mid s_i, z_y = 1) dy.
\]

The potential outcome query can therefore be answered using the outcome model, which we can estimate from data.
References


