Active Learning of Causal Bayes Net Structure

Kevin P. Murphy
Department of Computer Science
University of California
Berkeley, CA 94720-1776
murphyk@cs.berkeley.edu

Abstract

We propose a decision theoretic approach for deciding which interventions to perform so as to learn the causal structure of a model as quickly as possible. Without such interventions, it is impossible to distinguish between Markov equivalent models, even given infinite data. We perform online MCMC to estimate the posterior over graph structures, and use importance sampling to find the best action to perform at each step. We assume the data is discrete-valued and fully observed.

1 Introduction

There are essentially two kinds of approaches for learning the structure of Bayesian networks (BNs) from data. The first approach tries to find a graph which satisfies all the constraints implied by the empirical conditional independencies measured in the data [Pea00, SGS01]. The second approach searches through the space of graphs and uses some scoring metric to evaluate them [CH92, Hee95, Hee98], typically returning the highest scoring model found.

Both approaches to structure learning suffer from the fundamental problem that, even given infinite data, they can only identify the model up to Markov equivalence.\(^1\) This is adequate for density estimation (i.e., if our goal is just to predict future observations), but is inadequate if our goal is causal discovery, since two BNs might be Markov equivalent and yet make different predictions about the consequences of interventions (e.g., \(X \rightarrow Y\) and \(Y \rightarrow X\) are Markov equivalent, but make very different assertions about the effect on \(Y\) of changing \(X\)).

The only way to distinguish members of the same Markov equivalence class is to perform experiments. By “experiments” we mean ideal interventions in the sense of Pearl [Pea00], i.e., the learning agent can clamp a subset of the variables to fixed values. For example, in the genetics domain, an experiment might consist of “knocking out” a gene, which we can think of as clamping it to a fixed value. The manipulation theorem [SGS01, Pea00] says that we can compute the consequences of such interventions by “cutting” all the arcs coming into the nodes which have been clamped by intervention, and then doing probabilistic inference in the “mutilated” graph in the usual way. (We are assuming all nodes are observed; if there are hidden nodes, we must use Pearl’s “do calculus” to compute the consequences of interventions [Pea00]).

It is straightforward to modify existing Bayesian scoring methods to handle data obtained by interventional studies (in addition to the usual passive observational data). Specifically, we simply refrain from updating the parameters of the nodes that were clamped [CY99].

(\(^1\)Two graphs are Markov equivalent if they imply the same set of (conditional) independencies. For example, \(X \rightarrow Y \rightarrow Z\), \(X \leftarrow Y \rightarrow Z\) and \(X \leftarrow Y \leftarrow Z\) are Markov equivalent, since they all represent \(X \perp Z \mid Y\). In general, two graphs are Markov equivalent iff they have the same structure ignoring arc directions, and have the same v-structures [VP90]. (A v-structure consists of converging directed edges into the same node, such as \(X \rightarrow Y \leftarrow Z\).)
pected utility of this action with respect to our current beliefs about the model. We then update our beliefs given the outcome of the experiment and repeat. The basic framework is discussed in Sections 2 and 3.

Since the number of directed acyclic graphs (DAGs) grows super-exponentially with the number of nodes, we use a form of online MCMC to approximate our belief state, $F(G_{t+1})$, where $D_{t+1}$ is the data we have seen up to time-step $t$ (i.e., $t$ is the number of examples we have seen so far). In addition, computing the expected utility of an action requires enumerating all possible observations, which takes $O(2^n)$ time (assuming binary nodes). We approximate this using importance sampling. We discuss these approximations in Section 4. In Section 5, we show some experimental results using these approximations with three different Bayes nets.

Before diving into the technical details, we remark on the controversy concerning attempts to learn causality from data. Our claim is merely that statistical signatures in the data can suggest causal hypotheses that can be checked by experiment.

2 Active learning

The basic idea of our approach is illustrated in the influence diagram in Figure 1. We define the value (expected utility) of performing an action $A = a$ as

$$V(a) = \sum_{g \in \mathcal{G}} \sum_{y \in \mathcal{Y}} P(y|g, a, D)P(g|D)U(g, a, y, D)$$

where $U(\cdot)$ is a utility function, and $P(y|g, a, D)$ is the probability of generating observation $y$ given that we have performed action $a$ on graph $g$ (e.g., if $a$ is an intervention action, we need to mutilate $g$). $\mathcal{G}$ is the set of hypotheses (DAGs) we are considering, $\mathcal{Y}_{g, a}$ is the set of possible observations that $g$ could generate after action $a$, and $D$ is the past data. The best (myopic) action is defined to be $a^* = \arg \max_{a \in \mathcal{A}} V(a)$, where $\mathcal{A}$ is the set of possible actions (i.e., the set of values to which we can clamp the settable nodes).

If the goal is to infer the model structure, and all actions cost the same, we can use the following utility function: $U(g, a, y, D) = \log P(a, y, D)$. In Section 5, we will show experimentally that inferring the "correct" model structure is necessary if we are to predict the effect of interventions, but is not necessary if we are simply to predict future observations.

Before going into details, we will show that maximizing $\log P(g|a, y, D)$ is equivalent to maximizing the expected KL divergence between our posterior and our prior, or equivalently, to minimizing the conditional entropy of $H(G|Y, a, D)$ [Ber79], which is perhaps more familiar criteria.

$$V^* = \max_a E_Y KL(P(G|a, y, D)||P(G|D))$$

$$= \max_a \sum_y P(y|a, D) \sum_g P(g|a, y, D) \log \frac{P(g|a, y, D)}{P(g|D)}$$

Since the denominator $P(g|D)$ is independent of $a$, we may drop it to get

$$V^* = \min_a \sum_g \sum_y P(g|D) P(y|g, a, D) \log P(g|a, y, D)$$

3 Optimal algorithm

Let $\mathcal{G}$ be the (finite) set of all DAGs that we are considering. If all nodes are discrete (and hence $\mathcal{Y}$ and $\mathcal{A}$ are also finite sets), we can compute the optimal action by exhaustive enumeration, as follows.

for each $a \in \mathcal{A}$

$$V(a) = 0$$

for each $g \in \mathcal{G}$

$\quad$ Compute $P(g|a, y, D)$ $\forall g \in \mathcal{G}$

$\quad$ Compute $P(g|a, y, D)$ $\forall g \in \mathcal{G}$

$\quad$ $V(a) += \sum_g P(y|g, a, D)P(g|D) \log P(g|a, y, D)$

For completeness, we briefly summarise how to compute the various equations in the above algorithm. We use standard techniques for sequential Bayesian structure learning in fully observed, discrete domains (see [SL90, Bun94, Heo98] for details).

The expression $P(y|g, a, D)$ is the predictive density of $g_a$ (the graph $g$ modified by action $a$) given the past
data \(D\) evaluated at \(y\). This is given by the following equation:

\[
P(y|g,a,D) = \prod_{i=1}^{n} \prod_{j=1}^{q_i} \prod_{k=1}^{r_i} \beta_{ijk}^{\theta_{ijk}(y)} P(\theta_{ijk} | g, D) d\theta_{ijk}
\]

where \(\beta_{ijk}(y)\) is an indicator function that is 1 if the event \((X_i = k, \Pi_i = j)\) occurs in case \(y\), and is 0 otherwise. \(r_i\) is the number of values \(X_i\) can take on, \(q_i = \prod_{j \in \Pi_i} r_j\) is the number of values \(X_i\)'s parents can take on. For undamped nodes, we define \(\theta_{ijk} = P(X_i = k | \Pi_i = j)\). For damped nodes, we define \(\theta_{ijk} = 1\) if \(X_i\) is damped to \(k\) and \(\theta_{ijk} = 0\) otherwise. (Hence \(P(y|g,a,D) = 0\) if \(y\) contradicts the values of the damped nodes implied by \(a\)). If we assume the parameters of each node have independent Dirichlet priors with hyperparameters \(\alpha_{ijk}\), the posterior mean parameters are given by

\[
\bar{\theta}_{ijk} = E[\theta_{ijk} | g, D] = \frac{\alpha_{ijk} + N_{ijk}}{\sum_{j=1}^{s} \alpha_{ijl} + N_{ij}}
\]

where \(N_{ijk} = \sum_{y \in D} \beta_{ijk}(y)\). In this paper, we use the priors \(\alpha_{ijk} = 1/(r_i q_i)\); [HGC95] call this the BDeu metric. This ensures that Markov equivalent models have the same marginal likelihood given observational data alone, unlike using \(\alpha_{ijk} = 1\).

Since many of the graphs in \(G\) will share the same families, we can use a cache to efficiently compute \(P(y|g,a,D)\) for all \(g \in G\). (For example, if \(g_1\) and \(g_2\) only differ by a single edge addition/deletion, then \(P(y|g_1,a,D)\) and \(P(y|g_2,a,D)\) will only differ by one term.) Given the marginal likelihoods \(P(y|g,a,D)\) and the priors \(P(g|D)\) we can compute the posterior probability of each graph as follows:

\[
P(g|a,y,D) = \frac{P(y|g,a,D)P(g|D)}{\sum_{g'} P(y|g',a,D)P(g'|D)}
\]

In this paper, we use uniform structural priors, \(P(g)\).

4 Sampling algorithm

The optimal algorithm assumes we can exhaustively evaluate \(G, Y\) and \(A\). Typically this will be too expensive. We now discuss how to approximate each of these in turn.

4.1 Sampling graphs

The basic idea is to use the Metropolis–Hastings (MH) algorithm to draw samples from \(P(G|D)\). The algorithm is summarized below, where \(Q(G'|G)\) is the probability of proposing a move from \(G\) to \(G'\), \(B\) is the burn-in period, and \(N\) is the number of samples we want to draw. (See [MY95] for details.)

Choose \(G_1\) somehow e.g., at random

For \(t = 1, \ldots, B + N\)

Sample \(G' \sim Q( \cdot | G_t)\)

Compute \(R = \frac{P(G|D)Q(G'|D)}{P(G'|D)Q(G|D)}\)

Sample \(u \sim \text{Unif}(0,1)\)

If \(u < \min \{1, R\} \)

then \(G_{t+1} := G'\)

else \(G_{t+1} = G_t\)

Return \(G_{B+1}, \ldots, G_{B+N}\)

The proposal distribution we use is to sample uniformly from the neighborhood of \(G\), defined to be the set of all DAGs that differ from \(G\) by a single edge addition, deletion or reversal. (A way of quickly checking that the proposed graph is acyclic, based on the ancestor matrix, is described in [GC01].) In other words, \(Q(G'|G) = 1/\text{nbdl}(G)\), for \(G' \in \text{nbdl}(G)\), and \(Q(G' | G) = 0\) for \(G' \notin \text{ndb}(G)\), so

\[
R = \frac{\text{nbdl}(G)}{\text{nbdl}(G')} \frac{P(G|D)P(D|G')}{P(D|G)P(G'|D)}
\]

where the marginal likelihood is given by [CH92]

\[
P(D | G) = \prod_{i=1}^{n} \prod_{j=1}^{q_i} \frac{\Gamma(\alpha_{ij})}{\Gamma(\alpha_{ij} + N_{ij})} \cdot \prod_{k=1}^{r_i} \frac{\Gamma(\alpha_{ijk} + N_{ijk})}{\Gamma(\alpha_{ijk})}
\]

The main advantage of this proposal distribution is that it is efficient to compute the Bayes factor \(P(D|G')/P(D|G)\), since all but one (or two, in the case of an edge reversal) terms in the marginal likelihood ratio cancel.

[MAPV96] suggested searching the (smaller) space of (Markov) equivalence classes of DAGs, but this is inappropriate when we have interventional data. [FK00] suggested searching the (even smaller) space of total orderings of the nodes, marginalizing out the actual structure. Although this converges much faster, we chose not to pursue this technique, since we find it easier to design priors and heuristic proposal distributions in the space of graphs rather than orderings (see Section 6).

The MH algorithm as described above is appropriate for offline (batch) computation. However, we need to compute \(P(G|D_{1:t})\) online (sequentially). We therefore combine the ideas of particle filtering (see e.g., [DiFG01]) with MH as follows. The belief state, \(P(G|D_{1:t})\), is represented as a set of weighted particles (samples). When a new observation arrives, we apply a small number, \(B\), of MH moves to each particle to
get an approximation to \(P(G|D_{1:t+1})\). The justification for this is that the new belief state is likely to be very similar to the old one (since we only have one new observation). We initialise by sampling from our prior \(P(G)\).

Finally, we remark that in some domains, we have enough prior knowledge to construct a small set of hypothetical models, so we can feasibly enumerate all of \(\mathcal{G}\) without needing to use MCMC.

### 4.2 Sampling observations

Even if we can find a small set of probable candidate models, the size of each model in this set, \(n\), might be large, making it expensive to sum over all possible observations. (If all nodes are binary, there are \(O(2^n)\) possible observations, and for continuous-valued nodes, there are an infinite number.) In this case, we can use importance sampling. The basic idea is to make the following approximation

\[
E_Y f(Y) \approx \sum_{y \in \mathcal{Y}_s} w_y f(y)
\]

where \(f(y) = P(g|D) \log P(g|a, y, D)\), \(\mathcal{Y}_s\) is a set of sampled \(y\)'s drawn from some proposal distribution \(Q(\cdot)\), and \(w_y\) are the normalized importance weights:\n\(w_y \propto P(y|g, a, D)/Q(y)\).

Combining these two approximations, we modify the above active learning algorithm as follows.

1. Sample \(\mathcal{G}_s \sim P(\cdot|D)\) using MCMC for each \(a \in A\)
2. Compute \(V(a) = 0\)
3. Sample \(\mathcal{Y}_s \sim Q(\cdot|a, D)\) for each \(y \in \mathcal{Y}_s\)
4. Compute \(w_y(g) = P(y|g, a, D)/Q(y)\) \(\forall g \in \mathcal{G}_s\)
5. Compute \(P(g|a, y, D)\) \(\forall g \in \mathcal{G}_s\)
6. Set \(w_y(g) = \sum_{g'} w_{y'}(g) P(g|D) \log P(g|a, y, D)\)

The simplest proposal distribution for \(y\) is the uniform one: \(Q(y) = 1/2^n\), where we have assumed that all nodes are binary and the action \(a\) has clamped \(k\) nodes. The optimal proposal is of course \(Q(y) = P(y|g, a, D)\).

In this case, the algorithm becomes

1. Sample \(\mathcal{G}_s \sim P(\cdot|D)\) using MCMC for each \(a \in A\)
2. Compute \(V(a) = 0\)
3. for each \(g \in \mathcal{G}_s\)
4. Sample \(\mathcal{Y}_s \sim P(\cdot|g, a, D)\)
5. Set \(w_y = 1/|\mathcal{Y}_s|\)
6. for each \(y \in \mathcal{Y}_s\)
7. Compute \(P(g'|a, y, D)\) \(\forall g' \in \mathcal{G}_s\)

Since this is \(O(|\mathcal{G}_s|^2)\), it is typically too expensive. A cheaper approximation would be to sample from the mixture distribution \(\sum_y P(y|g, a, D)P(g|D)\). In this paper, however, we just sample from the uniform distribution.

### 4.3 Sampling actions

Finally, we consider the \(\max_a\) computation. If we can clamp up to \(k\) nodes simultaneously, and all nodes are binary, then \(|A| \leq \binom{n}{k} 2^k = O(n^k)\). Since it is often difficult or expensive to clamp many nodes simultaneously, \(k\) is often small; hence \(n^k\) is a low order polynomial. Nevertheless, since we must do \(O(|\mathcal{G}_s| |\mathcal{Y}_s|)\) computations per action, this can be expensive. We are currently working on some heuristic methods to avoid this brute force enumeration.

For continuous-valued nodes, the number of actions is in principle infinite, although in practice it might be reasonable to discretize the action space. For example, in the genetics domain, we might be able to clamp a node to its “wildtype” (mean) value \(\mu\), to “overexpress” it (clamp it to \(\mu + \sigma\), where \(\sigma\) is the standard or to “underexpress” it (clamp it to \(\mu - \sigma\)). (See [BMI99] for an interesting MCMC approach to selecting continuous-valued actions.)

### 4.4 How many samples?

The question of how many samples we need to take is an interesting one. The key insight is that, for action selection, it is the relative values of \(V(a)\) that matter. This idea has been exploited in [OK00] to reduce the number of samples used (see also the “Hoeffding traces” approach of [MM93]). However, in this paper, we just use a fixed number of samples.

### 5 Results

We compare the behavior of the active learner with two other algorithms: passive observation, and random interventions. We assume we can clamp up to two nodes simultaneously to any of their legal values. There are various ways to compare the algorithms. Since the posterior over all graphs is too big to easily visualize, one way of compressing it, following [TK01], is to compute the \(L_1\) edge error induced by belief state at time

\[V(a) = w_y P(g) \log P(g|a, y, D)\]
Figure 2: $L_1$ edge error against number of examples for the cancer network using random CPD parameters from a uniform distribution. The lines from top to bottom represent passive, random and active learning. We used 10 sampled observations, 100 sampled graphs, and averaged over 5 trials.

Figure 3: $L_1$ edge error against number of examples for the Asia network using the published CPD parameters. The lines from top to bottom represent passive, random and active learning. We computed $\sum_y$ exactly, used 100 sampled graphs, and averaged over 10 trials.

Figure 4: $L_1$ edge error against number of examples for the car troubleshooting network using random CPD parameters from a Beta(0.2,0.2) distribution. The top, dotted line is the passive learner, the other two lines are the random and active learners. We used 100 sampled observations, 300 sampled graphs, and averaged over 5 trials.

Figure 5: Prediction performance after 0, 1, 2 or 3 interventions to the Asia network. The vertical axis is negative log likelihood, the horizontal axis is number of examples. The dotted line is the passive learner, the other two lines are the random and active learners. We averaged over 10 trials.
$t, P_t = P(G|D_{1:t})$:

\[
err_t^{L_1}(P_t) = \sum_{i=1}^{n} \sum_{j=i+1}^{n} I_{G^*}(X_i \rightarrow X_j)(1 - P(X_i \rightarrow X_j)) + I_{G^*}(X_i \leftarrow X_j)(1 - P(X_i \leftarrow X_j)) + I_{G^*}(X_i \perp X_j)(1 - P(X_i \perp X_j))
\]

where $I_{G^*}(X_i \rightarrow X_j)$ is an indicator variable that is 1 if there is an edge from $X_i$ to $X_j$ in the true graph structure $G^*$, and $X_i \perp X_j$ means there is no connection between $X_i$ and $X_j$. (Henceforth we shall call the true model the “oracle”.)

Another metric is to evaluate the ability of the models to predict future observations, either drawn from the oracle, or generated in response to an intervention in the oracle. To do this, we simply generate a test set of size $M$ using the (possibly mutilated) oracle, and compute its average negative log likelihood according to the current belief state of the learner:

\[
err_t^{\text{pred}}(P_t) = \frac{-1}{M} \sum_{m=1}^{M} \sum_{g} \log P(y_m, g)P(g|D_{1:t})
\]

We consider performing 0, 1 and 2 interventions in the oracle, which corresponds to clamping 0, 1 and 2 nodes simultaneously to random values, and then sampling the other nodes. A test set consists of $M = 20$ such cases.

To be comparable with [TK01], we test our algorithm on three commonly-used networks: the 5 node cancer network [FMR98], the 8 node Asia network [LS88], and the 12 node car trouble-shooter network [HBR94]. All networks have binary nodes with multinomial conditional probability distributions (CPDs). For the Asia network, we used the published parameters. For the other networks, we sampled the CPD parameters from a Dirichlet distribution. By changing the parameters of the Dirichlet, we can control the degree of determinism. Specifically, as $\alpha_{i,j,k} \rightarrow 0$, the CPTs become more deterministic; for $\alpha_{i,j,k} = 1$, the CPT entries are chosen uniformly on $[0,1]$ (subject to the sum-to-one constraint); and as $\alpha_{i,j,k} \rightarrow \infty$, each row of the CPT tends towards the maximum entropy distribution of $[1/r_i, \ldots, 1/r_i]$.

In Figures 2, 3 and 4, we show how the $L_1$ error decreases as the number of examples increases. For the cancer and Asia networks, we see that the active learner identifies the structure much more quickly than the random or passive learners. For the car trouble-shooter network, however, the active learner does not seem to do any better than the random learner; presumably this is because we are not sampling for long enough. This is something we plan to investigate further.

In Figure 5, we plot the prediction performance of the learners for the Asia network. In Figure 5(a) we see that the passive learner can predict observations from the unmutated oracle slightly better than the other learners (initially, at least), even though it has the “wrong” structure. However, Figures 5(b-d) indicate that knowing the right structure helps to predict the effect of interventions, as expected, especially as the number of clamped nodes increases. We have found this to be true for the other models as well, especially in the more deterministic parameter regime.

6 Related work

Most previous work on active learning has been in the context of classification, regression or function optimization. In the case of linear regression, the minimum posterior entropy criterion discussed in Section 2 is called D-optimality, and can be maximized in closed form. Many other results (such as A-optimality, G-optimality, etc.) have been derived for the linear regression model, in both a Bayesian and non-Bayesian setting (see e.g., [CV95] for a review). There has also been work on active learning for non-linear regression models (e.g., neural networks [Mac92] and locally weighted regression [CG96]), where the objective is to minimize the expected variance of the predictor.

In the above works, the active learner can choose any point in the input space. By contrast, in the query filtering paradigm, the learner can choose to see the label of certain items from a stream of inputs (see e.g., [FSST97]).

In the PAC setting, [Ang88] showed how the ability to ask questions reduces the problem of identifying certain kinds of boolean functions from NP-complete to polynomial time. [BBH95] and [TR98] have extended this to active learning of tree-structured boolean functions, where the internal nodes are hidden. [AKMM98] have some results concerning upper and lower bounds on the number of experiments necessary to learn (possibly cyclic) boolean networks. [ITK00] discusses active learning techniques for learning boolean networks using an entropy-based cost function.

The most closely related work is that of Tong and Koller [TK01], who also use a decision theoretic framework for BN structure learning. (We shall henceforth refer to this as the “TK” algorithm.) The TK algorithm builds upon [FK00], who do MCMC over total orderings of the nodes, instead of over DAGs. The space of orderings is “only” of size $n!$, much smaller than the space of DAGs, which is a space of size $O(2^n)$. The key insight is that, conditioned on an ordering $\prec$, the parents for each node can be chosen independently (because there is no longer any global
acyclicity constraint), and hence can be marginalized out. TK extend this by showing how, conditioned on \( \prec \), one can perform \( \sum_y \) (needed for the expected utility computation) using the variable elimination algorithm.

The advantages of our algorithm over TK are its simplicity, the fact that it makes no assumptions about the form of the loss function, and the fact that it can incorporate prior structural knowledge. The loss function used by TK is \( \text{Loss}(P(G|a, y, D)) = \sum_{ij} H_{ij} \), where \( H_{ij} \) is the entropy associated with the edge distribution between nodes \( i \) and \( j \). Although this is fairly intuitive, it is not as theoretically well motivated as \( H(G|Y, a, D) \), which we used above.

The advantage of the TK algorithm over ours is speed. Firstly, it computes \( \sum_y \) analytically, instead of using importance sampling. And secondly, it uses MCMC in the smaller space of orderings. However, it is not clear how big the former speedup is: the cost of variable elimination depends on the induced width of the graph, which in turn depends on the summation ordering and the structure of the graphs induced by the set of all possible families; hence the induced width can become quite large. Also, while [FK00] have shown that MCMC in the space of orderings converges faster than in the space of DAGs, we believe that for either approach to be really practical, one will need strong prior knowledge, and it is easier to specify a prior as \( P(G) \) rather than the much less natural \( P(G|\prec) \).

7 Future work

There are many issues we would like to pursue in the future, the main ones being: continuous variables, missing data, online learning, and dynamical systems, and applications to biology.

For continuous variables, we plan to use linear-Gaussian CPDs, possibly with non-linear basis functions, as discussed above. (The use of such non-linearities makes this different from the global joint Gaussian approach of [HG95].) For missing data, we plan to use sampling (data augmentation). The actions might now also consist of choosing to measure a hidden variable, as in classical value-of-information computations. For online learning, we can no longer keep the whole dataset \( D \), nor can we store the (expected) sufficient statistics for all possible models. One approach would be to keep the statistics just for a “fringe” of probable models, as in [FG97].

It is straightforward to adapt the above techniques to learn the structure of a dynamic Bayesian network (DBN) from time series data c.f., [FMR98]. If we only allow arcs between time-slices (“diachronic” arcs), the parents for each node can be chosen independently, as in feature subset selection. Hence we can get the advantages of the TK algorithm without the need to sample node orderings.

Finally, we eventually hope to apply the algorithm to the problem of experiment design for inferring the structure of gene regulatory networks.

Acknowledgements

I would like to thank Stuart Russell and Michael Jordan for comments on an earlier draft of this paper.

References


