Generalization in Portfolio-Based Algorithm Selection

Maria-Florina Balcan,1 Tuomas Sandholm,1,2,3,4 Ellen Vitercik1

1Computer Science Department, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213
2Optimized Markets, Inc., Pittsburgh, PA 15213, USA
3Strategic Machine, Inc., Pittsburgh, PA 15213, USA
4Strategy Robot, Inc., Pittsburgh, PA 15213, USA
{ninamf, sandholm, vitercik}@cs.cmu.edu

Abstract

Portfolio-based algorithm selection has seen tremendous practical success over the past two decades. This algorithm configuration procedure works by first selecting a portfolio of diverse algorithm parameter settings, and then, on a given problem instance, using an algorithm selector to choose a parameter setting from the portfolio with strong predicted performance. Often times, both the portfolio and the algorithm selector are chosen using a training set of typical problem instances from the application domain at hand. In this paper, we provide the first provable guarantees for portfolio-based algorithm selection. We analyze how large the training set should be to ensure that the resulting algorithm selector’s average performance over the training set is close to its future (expected) performance. This involves analyzing three key reasons why these two quantities may diverge: 1) the learning-theoretic complexity of the algorithm selector, 2) the size of the portfolio, and 3) the learning-theoretic complexity of the algorithm’s performance as a function of its parameters. We introduce an end-to-end learning-theoretic analysis of the portfolio construction and algorithm selection together. We prove that if the portfolio is large, overfitting is inevitable, even with an extremely simple algorithm selector. With experiments, we illustrate a tradeoff exposed by our theoretical analysis: as we increase the portfolio size, we can hope to include a well-suited parameter setting for every possible problem instance, but it becomes impossible to avoid overfitting.

1 Introduction

Algorithms often come with a variety of tunable parameters. With a deft parameter tuning, these algorithms can often efficiently solve computationally challenging problems. However, the best parameter setting for one problem is rarely optimal for another. Algorithm portfolios, which are finite sets of parameter settings, are used in practice to deal with this variability. A portfolio is often used in conjunction with an algorithm selector, which is a function that determines which configuration in the portfolio to employ on any input problem instance. Portfolio-based algorithm selection has fueled breakthroughs in combinatorial auction winner determination (Leyton-Brown 2003; Sandholm 2013), SAT (Xu et al. 2008), integer programming (Xu, Hoos, and Leyton-Brown 2010; Kadioglu et al. 2010), planning (Núñez, Borrajo, and López 2015), and many other domains.

Both the portfolio and the algorithm selector are often chosen using a training set of problem instances from the application domain at hand. This training set is typically assumed to be drawn from an unknown, application-specific distribution. The portfolio and algorithm selector are chosen to have strong average performance (quantified by low average runtime, for example) over the training set. We investigate whether the learned algorithm selector also has strong expected performance on problems from the same application domain. The difference between average performance and expected performance is known as generalization error. If the generalization error is small, every parameter setting’s average performance over the training set is close to its expected performance, so the learned algorithm selector will not overfit. When overfitting occurs, the learned selector has strong average performance over the training set set but poor expected performance on the true distribution.

There are multiple reasons the generalization error might be large in this setting: 1) the learning-theoretic complexity of the algorithm selector, 2) the size of the portfolio, and 3) the learning-theoretic complexity of the algorithm’s performance as a function of its parameters. We prove end-to-end bounds in terms of all three elements simultaneously. The multitude of factors impacting generalization differentiates this paper from prior research on generalization in algorithm configuration (e.g., Gupta and Roughgarden 2017; Balcan et al. 2017; Garg and Kalai 2018; Liu et al. 2020).

That research focuses on learning a single good configuration rather than a portfolio together with an algorithm selector. In the former case, generalization error only grows with (3)—just one of the sources of error we must contend with. Our bounds apply to the widely-applicable setting where on any fixed input, algorithmic performance is a piecewise-constant function of its parameters with at most \( t \) pieces, for some \( t \in \mathbb{Z} \). This structure has been observed in algorithm configuration for integer programming, greedy algorithms, clustering, and computational biology (Gupta and Roughgarden 2017; Balcan et al. 2017, 2018, 2021; Balcan 2020). Given a training set of size \( N \), we prove that the generalization error is bounded\(^1\) by \( \tilde{O}\left(\sqrt{\left( d + \kappa \log t \right) / N }\right) \), where

\(^1\)Here we assume that algorithmic performance is a quantity in
\( \kappa \) is the size of the portfolio and \( \hat{d} \) measures the intrinsic complexity of the algorithm selector, as we define in Section 3. We also prove that this bound is tight up to logarithmic factors: the generalization error can be as large as \( \Omega \left( \sqrt{\left( \frac{\hat{d} + \kappa}{N} \right)} \right) \). This implies that even if the algorithm selector is extremely simple (\( \hat{d} \) is small), overfitting cannot be avoided in the worst case when the portfolio size \( \kappa \) is large. Moreover, we instantiate our guarantees for several commonly-used families of algorithm selectors.

Finally, via experiments in the context of integer programming configuration, we illustrate the inherent tradeoff our theory exposes: as we increase the portfolio size, we can hope to include a high-performing parameter setting for any given instance, but it becomes increasingly difficult to avoid overfitting. We incrementally increase the size of the portfolio and with each addition we train an algorithm selector using regression forest performance models. As the portfolio size increases, the algorithm selector’s training performance continues to improve, but there comes a point where the test performance begins to worsen, meaning that the algorithm selector is overfitting to the training set.

**Additional related research.** Gupta and Roughgarden (2017) also provide generalization guarantees for algorithm configuration. They primarily analyze the problem of learning a single parameter setting with high expected performance. They do provide guarantees for the more general problem of learning a mapping from instances to parameter settings in a few special cases, but do not study the problem of learning a portfolio in conjunction with learning a selector, which we do. They study settings where for each problem instance, a domain expert has defined a number of relevant features, as do we in Section 4. Their first result applies to learning an algorithm selector when the set of features is finite. In contrast, our results apply to infinite feature spaces. Their second set of results is tailored to the problem of learning empirical performance models. An empirical performance model is meant to predict how long a particular algorithm will take to run on a given input. An algorithm selector can use an empirical performance model by selecting the parameter setting with best predicted performance. Gupta and Roughgarden (2017) provide guarantees that bound the difference between the empirical performance model’s expected error and average error over the training set. Their guarantees can be applied once the portfolio is already chosen. They do not study the problem of learning the portfolio itself, whereas we study the composite problem of learning the portfolio and the algorithm selector.

### 2 Problem Formulation and Road Map

**Notation.** Our theoretical guarantees apply to algorithms parameterized by a real value \( \rho \in \mathbb{R} \). We use the notation \( \mathcal{Z} \) to denote the set of problem instances the algorithm may take as input. For example, \( \mathcal{Z} \) might consist of integer programs (IPs) if we are configuring an IP solver. There is an unknown distribution \( \mathcal{D} \) over problem instances in \( \mathcal{Z} \).

To describe the performance of a parameterized algorithm, we adopt the notation of prior research (Balcan et al. 2021). For every parameter setting \( \rho \in \mathbb{R} \), there is a function \( u_{\rho} : \mathcal{Z} \rightarrow [0,1] \) that measures, abstractly, the performance of the algorithm parameterized by \( \rho \) given an input \( z \in \mathcal{Z} \). For example, \( u_{\rho} \) might measure runtime or the quality of the algorithm’s output. We use the notation \( \mathcal{U} = \{ u_{\rho} : \rho \in \mathbb{R} \} \) to denote the set of all performance functions.

**Problem formulation.** A portfolio-based algorithm selection procedure relies on two key components: a portfolio and an algorithm selector. A portfolio is a set \( \mathcal{P} = \{ \rho_1, \ldots, \rho_\kappa \} \subseteq \mathbb{R} \) of \( \kappa \) parameter settings. An algorithm selector is a mapping \( f : \mathcal{Z} \rightarrow \mathcal{P} \) from problem instances \( z \in \mathcal{Z} \) to parameter settings \( f(z) \in \mathcal{P} \). In practice (Xu, Hoos, and Leyton-Brown 2010; Kadioglu et al. 2010; Sandholm 2013), the portfolio and algorithm selector are typically learned using the following high-level procedure:

1. Choose a class \( \mathcal{F} \) of algorithm selectors, each of which maps \( \mathcal{Z} \) to \( \mathbb{R} \). (In Section 4, we provide several examples of classes \( \mathcal{F} \) used in practice.)
2. Draw a training set \( \mathcal{S} = \{ z_1, \ldots, z_N \} \sim \mathcal{D}^N \) of problem instances from the unknown distribution \( \mathcal{D} \).
3. Use \( \mathcal{S} \) to learn a portfolio \( \mathcal{P} = \{ \rho_1, \ldots, \rho_\kappa \} \subseteq \mathbb{R} \).
4. Use \( \mathcal{S} \) to learn an algorithm selector \( \hat{f} \in \mathcal{F} \) that maps to parameter settings in the portfolio \( \mathcal{P} \).

Given an instance \( z \in \mathcal{Z} \), the performance of the parameter setting selected by \( \hat{f} \) is \( u_{f(z)}(z) \). We bound the expected quality \( \mathbb{E}_{z \sim \mathcal{D}} \left[ u_{f(z)}(z) \right] \) of the learned algorithm selector.

**Road map.** We first analyze the extent to which the average performance of the selector \( \hat{f} \) over the training set generalizes to its expected performance. We then use this analysis to relate the performance of \( \hat{f} \) and the optimal selector under the optimal choice of a portfolio. Specifically, we bound the difference between \( \mathbb{E}_{z \sim \mathcal{D}} \left[ u_{f(z)}(z) \right] \) and \( \max_{\mathcal{P} : |\mathcal{P}| \leq \kappa} \mathbb{E}_{z \sim \mathcal{D}} \left[ \max_{\rho \in \mathcal{P}} u_{\rho}(z) \right] \). (If our goal is to minimize \( u_{\rho}(z) \), we may replace each \( \max \) with a \( \min \).)

### 3 Sample Complexity Bounds

In this section, we bound the difference between the average performance of any selector \( f \in \mathcal{F} \) over the training set \( \mathcal{S} \sim \mathcal{D}^N \) and its expected performance. Formally, we bound

\[
\frac{1}{N} \sum_{z \in \mathcal{S}} u_{f(z)}(z) - \mathbb{E}_{z \sim \mathcal{D}} \left[ u_{f(z)}(z) \right]
\]

for any choice of an algorithm selector \( f \in \mathcal{F} \). This will serve as a building block for our general analysis of portfolio-based algorithm selection.

Our bounds apply in the widely-applicable setting where on any fixed input, algorithmic performance is a piecewise-constant function of the algorithm’s parameters. This structure has been observed in algorithm configuration for integer

---


programmed, greedy algorithms, clustering, and computational biology (Gupta and Roughgarden 2017; Balcan et al. 2017, 2018, 2021; Balcan 2020). To describe this structure more formally, for a fixed input \( z \in \mathcal{Z} \), we use the notation \( u^*_z : \mathbb{R} \to \mathbb{R} \) to denote algorithmic performance as a function of the parameters (whereas the functions \( u_p \) defined in Section 2 measure performance as a function of the input \( z \)). Naturally, \( u^*_z(\rho) = u_p(z) \). We refer to \( u^*_z \) as a dual function (as opposed to \( u_p \), which is a primal function). We assume algorithmic performance is a piecewise-constant function of the parameters, or more formally, that each function \( u^*_z \) is piecewise constant with at most \( t \) pieces, for some \( t \in \mathbb{Z}^+ \).

Our bounds depend on both the number of pieces \( t \) and on the intrinsic complexity of the class of algorithm selectors \( \mathcal{F} \). We use the following notion of the multi-class projection of \( \mathcal{F} \) to define the class’s intrinsic complexity.

**Definition 3.1.** Given a selector \( f \in \mathcal{F} \), let \( \rho_1 < \rho_2 < \cdots < \rho_t \) be the parameter settings \( f \) maps to, with \( \tilde{\kappa} \leq \kappa \).

The function \( f \) defines a partition \( Z_1, \ldots, Z_{\tilde{\kappa}} \) of the problem instances \( \mathcal{Z} \) where for any \( z \in \mathcal{Z} \), if \( f(z) = \rho_i \), then \( z \in Z_i \). For each function \( f \in \mathcal{F} \) there is therefore a corresponding multi-class function \( \tilde{f} : \mathcal{Z} \to [\tilde{\kappa}] \) that indicates which set of the partition the instance \( z \) belongs to: \( \tilde{f}(z) = i \) when \( z \in Z_i \). We use the notation \( \tilde{\mathcal{F}} = \{ \tilde{f} : f \in \mathcal{F} \} \) to denote the set of all such multi-class functions.

Defining this set of multi-class functions allows us to use classic tools from multi-class learning to reason about the algorithm selectors \( \mathcal{F} \). In particular, our bounds depend on the Natarajan (1989) dimension of the class \( \mathcal{F} \), which is a natural extension of the classic VC dimension (Vapnik and Chervonenkis 1971) to multi-class functions.

**Definition 3.2 (Natarajan dimension).** The set \( \tilde{\mathcal{F}} \) multi-class shatters a set of problem instances \( z_1, \ldots, z_N \) if there exist labels \( y_1, \ldots, y_N \in [\kappa] \) and \( y'_1, \ldots, y'_N \in [\kappa] \) such that:

1. For every \( i \in [N] \), \( y_i \neq y'_i \), and
2. For any subset \( C \subseteq [N] \), there exists a function \( \tilde{f} \in \tilde{\mathcal{F}} \) such that \( \tilde{f}(z_i) = y_i \) if \( i \in C \) and \( \tilde{f}(z_i) = y'_i \) otherwise.

The Natarajan dimension of \( \tilde{\mathcal{F}} \) is the cardinality of the largest set that can be multi-class shattered by \( \tilde{\mathcal{F}} \).

In Section 4, we bound the Natarajan dimension of \( \tilde{\mathcal{F}} \) for several commonly-used classes of algorithm selectors \( \mathcal{F} \). We use Natarajan dimension to quantify the intrinsic complexity of the class of selectors, which in turn allows us to bound Equation (1) for every function \( f \in \mathcal{F} \). To do so, we relate the Natarajan dimension of \( \tilde{\mathcal{F}} \) to the pseudo-dimension of the function class \( \mathcal{U}_\mathcal{F} \) = \( \{ z \mapsto u_{f(z)}(z) : f \in \mathcal{F} \} \). Every function in \( \mathcal{U}_\mathcal{F} \) is defined by an algorithm selector \( f \in \mathcal{F} \). On input \( z \in \mathcal{Z} \), \( u_{f(z)}(z) \) equals the utility of the algorithm parameterized by \( f(z) \) on input \( z \). Pseudo-dimension (Haussler 1992) is a classic learning-theoretic tool for measuring the intrinsic complexity of a class of real-valued functions (whereas Natarajan dimension applies to multi-class functions). Both Natarajan dimension and pseudo-dimension are extensions of the classic VC dimension, so they bear some resemblance. Below, we define the pseudo-dimension of the class \( \mathcal{U}_\mathcal{F} \).

**Definition 3.3 (Pseudo-dimension).** The set \( \mathcal{U}_\mathcal{F} \) shatters a set of instances \( z_1, \ldots, z_N \in \mathcal{Z} \) if there exist witnesses \( w_1, \ldots, w_N \in \mathbb{R} \) such that for any subset \( C \subseteq [N] \), there exists an algorithm selector \( f \in \mathcal{F} \) such that \( u_{f(z_i)}(z_i) \leq w_i \) if \( i \in C \) and \( u_{f(z_i)}(z_i) > w_i \) otherwise. The pseudo-dimension of \( \mathcal{U}_\mathcal{F} \), denoted \( \text{Pdim}(\mathcal{U}_\mathcal{F}) \), is the size of the largest set of instances that can be shattered by \( \mathcal{U}_\mathcal{F} \).

Classic learning-theoretic results allow us to provide generalization bounds once we calculate the pseudo-dimension. For example (Haussler 1992), with probability \( 1 - \delta \) over the draw of the set \( \{ z_1, \ldots, z_N \} \sim D^N \), for any selector \( f \in \mathcal{F} \),

\[
\frac{1}{N} \sum_{i=1}^{N} u_{f(z_i)}(z_i) - \mathbb{E}_{z \sim D} \left[ u_{f(z)}(z) \right] = \mathcal{O} \left( H \sqrt{\frac{1}{N} \left( \text{Pdim}(\mathcal{U}_\mathcal{F}) + \log \frac{1}{\delta} \right)} \right).
\]

We provide a general bound on \( \text{Pdim}(\mathcal{U}_\mathcal{F}) \), which allows us to bound Equation (1). The proof is in the full version (Balcan, Sandholm, and Vitercik 2020).

**Theorem 3.4.** Suppose each dual function \( u^*_z \) is piecewise-constant with at most \( t \) pieces. Let \( d \) be the Natarajan dimension of \( \mathcal{F} \). Then \( \text{Pdim}(\mathcal{U}_\mathcal{F}) = \tilde{O} \left( \sqrt{d + \kappa \log \frac{1}{\delta}} \right) \).

At a high level, the \( \tilde{O} (d) \) term accounts for the intrinsic complexity of the algorithm selectors \( \mathcal{F} \). The \( O (\kappa \log t) \) term accounts for the complexity of composing selectors \( f \) with the performance functions \( u_p \). In Theorem 3.5, we prove this bound is tight up to logarithmic factors.

**Proof sketch of Theorem 3.4.** Let \( z_1, \ldots, z_N \in \mathcal{Z} \) be an arbitrary set of problem instances. Since each dual function \( u^*_z \) is piecewise-constant with at most \( t \) pieces, there are \( M \leq Nt \) intervals \( I_1, \ldots, I_M \) partitioning \( \mathbb{R} \) where for any interval \( I_j \) and any instance \( z_i \), \( u^*_z(\rho) \) is constant across all \( \rho \in I_j \). Given these intervals, we partition the algorithm selectors in \( \mathcal{F} \) into at most \( M^K \) sets so that within any one set, all selectors map to the same \( \kappa \) (or fewer) intervals. Focusing on the selectors within one set \( \mathcal{F}_0 \) of the partition, we prove that the number of ways the utility functions \( u_f \) across \( f \in \mathcal{F}_0 \) can label the instances \( z_1, \ldots, z_N \) is upper bounded by the number of ways the multi-class projection functions \( f \) across \( f \in \mathcal{F}_0 \) can label the instances. We can then use the Natarajan dimension of \( \tilde{\mathcal{F}} \) to bound the number of ways the functions in \( \mathcal{U}_\mathcal{F} \) label the instances \( z_1, \ldots, z_N \).

Theorem 3.4 and Equation (2) imply that with probability \( 1 - \delta \) over the draw \( S \sim D^N \), for any selector \( f \in \mathcal{F} \),

\[
\frac{1}{N} \sum_{z \in S} u_{f(z)}(z) - \mathbb{E}_{z \sim D} \left[ u_{f(z)}(z) \right] = \tilde{O} \left( H \sqrt{\frac{1}{N} \left( d + \kappa \log \frac{1}{\delta} \right)} \right).
\]

This theorem quantifies a fundamental tradeoff: as the portfolio size increases, we can hope to obtain better and better empirical performance \( \sum_{z \in S} u_{f(z)}(z) \) but the generalization error \( \tilde{O} \left( H \sqrt{d + \kappa} / \sqrt{N} \right) \) will worsen.
We now prove that Theorem 3.4 is tight up to logarithms. The following theorem illustrates that even if the class of algorithm selectors is extremely simple (in that the Natarajan dimension of $F$ is 0), if the portfolio size (that is, the number $\kappa$ of parameters mapped to) is large, we cannot hope to avoid overfitting. The full proof is in the full version (Balcan, Sandholm, and Vitercik 2020).

**Theorem 3.5.** For any $\kappa, \bar{d} \geq 2$, there is a class of functions $\mathcal{U} = \{ u_\rho : \rho \in \mathbb{R} \}$ and a class of selectors $F$ such that:

1. Each selector $f \in F$ maps to $\leq \kappa$ parameter settings.
2. Each dual function $u^*_\rho$ is piecewise-constant with $I$ discontinuity.
3. The Natarajan dimension of $F$ is at most $\bar{d}$, and
4. The pseudo-dimension of $\mathcal{U}_F$ is $\Omega(\kappa + \bar{d})$.

**Proof sketch.** Let $Z = (0, 1]$. For each parameter setting $\rho \in \mathbb{R}$, define $u_\rho(z) = 1(z \leq \rho)$. Let $\kappa, \bar{d} \geq 2$ be two arbitrary integers. We split this proof into two cases: $\bar{d} \geq \kappa$ and $\kappa > \bar{d}$. In both cases, we construct a class of selectors $F$ that satisfies the properties in the theorem statement and we prove that $\text{Pdim}(\mathcal{U}_F) \geq \max\{\kappa, \bar{d}\} = \Omega(\kappa + \bar{d})$. We sketch the proof of the case where $\kappa > \bar{d}$.

We begin by partitioning $Z = (0, 1]$ into $\kappa$ intervals $Z_1, \ldots, Z_\kappa$, where $Z_i = (\frac{i-1}{\kappa}, \frac{i}{\kappa}]$. For each set $C \subseteq [\kappa]$, we define an selector $f_C : Z \rightarrow \mathbb{R}$ as follows. For any $z \in Z_i$, let $i$ be the index of the interval $z$ lies in, i.e., $z \in Z_i$. If $i \in C$, we map $f_C(z) = \frac{i}{\kappa}$ and if $i \notin C$, we map $f_C(z) = \frac{i}{\kappa} - \frac{1}{\kappa}$. Let $F = \{ f_C : C \subseteq [\kappa] \}$. The multi-class partitioning of $F$ is extremely simple: its Natarajan dimension is 0. Moreover, the set $S = \left\{ \left\{ \frac{1}{\kappa}, \frac{2}{\kappa}, \ldots, \frac{\kappa-1}{\kappa}, 1 \right\} \right\}$ is shattered by $\mathcal{U}_F$ because—at a high level—each selector $f_C$ maps each element $z \in S$ to a parameter just above $z$ or just below $z$, which allows the function class $\mathcal{U}_F$ to shatter $S$. 

In the proof of Theorem 3.5, each performance function $u_\rho$ maps to $\{0, 1\}$, so we effectively prove a lower bound on the VC dimension of $\mathcal{U}_F$. Classic results from learning theory imply the generalization error of learning a selector $f \in F$ can therefore be as large as $\tilde{\Omega}\left(H\sqrt{(\bar{d} + \kappa)/N}\right)$, which matches Equation (3) up to logarithmic factors.

### 4 Application of Theory to Algorithm Selectors

We now instantiate Theorem 3.4 for several commonly-used classes of algorithm selectors. In each of the case studies, there is a feature mapping $\phi : Z \rightarrow \mathbb{R}^m$ that assigns feature vectors $\phi(z) \in \mathbb{R}^m$ to problem instances $z \in Z$.

#### 4.1 Linear Performance Models

We begin by providing guarantees for algorithm selectors that use a linear performance model. These have been used extensively in computational research (Xu et al. 2008; Xu, Hoos, and Leyton-Brown 2010). To define this type of selector, let $\rho = (\rho_1, \ldots, \rho_\kappa)$ be a set of $\kappa$ distinct parameter settings. For each $i \in [\kappa]$, define a vector $w_i \in \mathbb{R}^m$ and let $W = \begin{pmatrix} w_1 & \cdots & w_\kappa \end{pmatrix}$ be a matrix containing all $\kappa$ weight vectors. The dot product $\phi(z) \cdot w_i$ is meant to estimate the performance of the algorithm parameterized by $\rho_i$ on instance $z$. We define the algorithm selector $f_{\rho, W}(z) = \rho_i$ where $i = \arg\max_{j \in [\kappa]} \{ \phi(z) \cdot w_j \}$, which selects the parameter setting with best predicted performance.

We define the class of algorithm selectors $F_L = \{ f_{\rho, W} : W \in \mathbb{R}^{m \times \kappa}, \rho \in \mathbb{R}^\kappa \}$. To define the class $F_L$, for each matrix $W \in \mathbb{R}^{m \times \kappa}$, let $g_W : Z \rightarrow [\kappa]$ be a function where $g_W(z) = \arg\max_{i \in [\kappa]} \{ \phi(z) \cdot w_i \}$. By definition, $F_L = \{ g_W : W \in \mathbb{R}^{m \times \kappa} \}$ is the well-studied $m$-dimensional linear class which has a Natarajan dimension of $O(m \kappa)$ (Shalev-Shwartz and Ben-David 2014). This fact implies the following corollary.

**Corollary 4.1.** Suppose the dual functions are piecewise-constant with at most $t$ pieces. The pseudo-dimension of $\mathcal{U}_{F_L} = \{ z \rightarrow u_{f(z)} : f \in F_L \}$ is $O(km \log(km) + \kappa \log t)$.

#### 4.2 Regression Tree Performance Models

We now analyze algorithm selectors that use a regression tree as the performance model. These have proven powerful in computational research (Hutter et al. 2014). A regression tree $T$’s leaf nodes partition the feature space $\mathbb{R}^m$ into disjoint regions $R_1, \ldots, R_{\kappa}$. In each region $R_i$, a constant value $c_i$ is used to predict the algorithm’s performance on instances in the region. The internal nodes of the tree define this partition: each performs an inequality test on some feature of the input. We use the notation $h_T(z)$ to denote tree $T$’s prediction of the algorithm’s performance on instance $z$.

Formally, $h_T(z)$ equals the constant value corresponding to the region of the tree’s partition to which $\phi(z)$ belongs.

An algorithm selector can be defined using a regression tree performance model as follows. Let $\rho = (\rho_1, \ldots, \rho_\kappa)$ be a set of $\kappa$ parameter settings. For each $\rho_i$, let $T_i$ be a tree that is meant to predict the performance of the algorithm parameterized by $\rho_i$, and let $T = (T_1, \ldots, T_{\kappa})$ be the set of all $\kappa$ trees. We define the algorithm selector $f_{\rho, T}(z) = \rho_i$ where $i = \arg\max_{j \in [\kappa]} \{ h_{T_j}(z) \}$. The class of algorithm selectors $F_R$ consists of all functions $f_{\rho, T}$ across all parameter vectors $\rho \in \mathbb{R}^\kappa$ and all $\kappa$-tuples of regression trees $T = (T_1, \ldots, T_{\kappa})$. The full proof of the following lemma is in the full version (Balcan, Sandholm, and Vitercik 2020).

**Lemma 4.2.** Suppose we limit ourselves to building regression trees with at most $t$ leaves. Then the Natarajan dimension of $F_R$ is $O(\kappa t \log(k \kappa m))$.

**Proof sketch.** For each $\kappa$-tuple of regression trees $T = (T_1, \ldots, T_{\kappa})$, let $g_T : Z \rightarrow [\kappa]$ be a function where $g_T(z) = \arg\max_{j \in [\kappa]} \{ h_{T_j}(z) \}$. By definition, the set $F_R$ consists of the functions $g_T$ across all $\kappa$-tuples of regression trees $T$ with at most $t$ leaves. Let $z_1, \ldots, z_N \in Z$ be a set of problem instances. Our goal is to bound the number of ways the
functions \( g_T \) can label these instances. A single regression tree induces a partition of these \( N \) problem instances defined by which leaf each instance is mapped to as we apply the tree’s inequality tests. The key step in this proof is bounding the total number of partitions we can induce by varying the tree’s inequality tests. We then generalize this intuition to bound the number of partitions \( \kappa \) regression trees can induce as we vary all their parameters. Once the partition of each regression tree is fixed, the tree with the largest prediction error of each problem instance depends on the relative ordering of the constants at the trees’ leaves. There is a bounded number of possible relative orderings, and we aggregate all of these bounds to prove the lemma statement.

Corollary 4.3. Suppose the dual functions are piecewise-constant with at most \( t \) pieces and we limit ourselves to building regression trees with at most \( \ell \) leaves. Then \( \text{Pdim} (\Upsilon_{\mathcal{R}_n}) = O(\ell \kappa \log(\ell \kappa m) + \kappa \log t) \).

This pseudo-dimension bound reflects the end-to-end nature of our analysis, since the guarantee bounds the generalization error of both selecting the portfolio and training the regression tree performance model. This is why the bound grows with both the size of the portfolio \( \langle \kappa \rangle \) and the complexity of the regression trees \( \langle \ell \rangle \) and \( \langle m \rangle \).

4.3 Clustering-Based Algorithm Selectors

We now provide guarantees for clustering-based algorithm selectors (Kadioglu et al. 2010). This type of selector clusters the feature vectors \( \phi(z_1), \ldots, \phi(z_N) \in \mathbb{R}^m \) and chooses a good parameter setting for each cluster. On a new instance \( z \), the selector determines which cluster center is closest to \( \phi(z) \) and runs the algorithm using the parameter setting assigned to that cluster. More formally, let \( \rho = (\rho_1, \ldots, \rho_\kappa) \) be a set of parameter settings and let \( x_1, \ldots, x_\kappa \in \mathbb{R}^m \) be a set of vectors. We define the matrix

\[
X = \begin{pmatrix}
  | & \cdots & | \\
  x_1 & \cdots & x_\kappa \\
  | & \cdots & | 
\end{pmatrix},
\]

where each \( x_i \) represents a cluster center. We define the selector \( f_{\rho, X}(z) = \rho_i \) with \( i = \text{argmin}_{j \in [\kappa]} \{ ||x_j - \phi(z)||_p \} \) for some \( \ell_p \)-norm with \( p \geq 1 \), and the class \( \mathcal{F}_C = \{ f_{\rho, X} : \rho \in \mathbb{R}^\kappa, X \in \mathbb{R}^{m \times \kappa} \} \). This lemma’s proof is in the full version (Balcan, Sandholm, and Vitercik 2020).

Lemma 4.4. For any \( p \in [1, \infty) \), the Natarajan dimension of \( \mathcal{F}_C \) is \( O(m \kappa \log(m \kappa p)) \).

Proof sketch. For each matrix \( X \), let \( g_X : Z \to [\kappa] \) be defined such that \( g_X(z) = \text{argmin}_{i \in [\kappa]} \{ ||x_i - \phi(z)||_p \} \). By definition, \( \mathcal{F}_C = \{ g_X : X \in \mathbb{R}^{m \times \kappa} \} \). Let \( z_1, \ldots, z_N \in Z \) be a set of problem instances. Our goal is to bound the number of ways the functions \( g_X \) can label these instances as we vary \( X \in \mathbb{R}^{m \times \kappa} \). We do so by analyzing, for each instance \( z_i \), the boundaries in \( \mathbb{R}^{m \times \kappa} \) where if we shift \( X \) from one side of the boundary to the other, the column in \( X \) closest to \( \phi(z_i) \) changes. We show that these boundaries are defined by multi-dimensional polynomials. We bound the total number of regions these boundaries induce in \( \mathbb{R}^{m \times \kappa} \), which implies a bound on the Natarajan dimension of \( \mathcal{F}_C \).

Lemma 4.4 and Theorem 3.4 imply the following bound.

Corollary 4.5. If the dual functions are piecewise-constant with at most \( t \) pieces, then \( \text{Pdim} (\Upsilon_{\mathcal{R}_C}) = \tilde{O}(m \kappa + \kappa \log t) \).

5 Learning Procedure with Guarantees

We use the results from the previous section to provide guarantees for the high-level learning procedure from Section 2:  

1. Draw a training set of problem instances \( S \sim \mathcal{D}^N \).
2. Use \( S \) to select a set of at most \( \kappa \) configurations \( \mathcal{P} \subseteq \mathbb{R} \).
3. Use \( S \) to learn an algorithm selector \( \hat{f} \in \mathcal{F} \) that maps problem instances \( z \in Z \) to parameter settings \( \hat{f}(z) \in \mathcal{P} \).

Our guarantees depend on the quality of the portfolio \( \mathcal{P} \) and selector \( \hat{f} \), as formalized by the following definition.

Definition 5.1. Given a training set \( S \subseteq Z^N \) and parameters \( \alpha \in (0, 1], \beta \in [0, 1], \) and \( \epsilon \in [0, 1] \), we say the portfolio \( \mathcal{P} \) and the algorithm selector \( \hat{f} \) are \( (\alpha, \beta, \epsilon) \)-optimal if:

1. The portfolio \( \mathcal{P} \) is nearly optimal over the training set:

\[
\frac{1}{N} \sum_{z \in S} \max_{\rho \in \mathcal{P}} u_\rho(z) \geq \alpha \max_{\mathcal{P} \subseteq \mathbb{R} \mid |\mathcal{P}| \leq \kappa} \frac{1}{N} \sum_{z \in S} \max_{\rho \in \mathcal{P}} u_\rho(z) - \beta.
\]

(The maximization means that performance is measured with respect to an oracle that selects an optimal algorithm parameter \( \rho \) from the portfolio for each instance.)

2. The algorithm selector \( \hat{f} \) returns high-performing parameter settings from the set \( \mathcal{P} \) in the sense that

\[
\frac{1}{N} \sum_{z \in S} u_{\hat{f}(z)}(z) \geq \frac{1}{N} \sum_{z \in S} \max_{\rho \in \mathcal{P}} u_\rho(z) - \epsilon.
\]

For example, when algorithmic performance as a function of the parameters is piecewise constant, there are only a finite number of meaningfully different parameter values to choose among—one per piece. Then, since \( \sum_{z \in S} \max_{\rho \in \mathcal{P}} u_\rho(z) \) is a submodular function of the portfolio \( \mathcal{P} \), we can use a greedy algorithm to select \( \mathcal{P} \), and we obtain \( \alpha = 1 - \frac{1}{e} \) and \( \beta = 0 \), as we prove in the full version (Balcan, Sandholm, and Vitercik 2020). Alternatively, integer programming could be used to select the optimal portfolio from the finite set of candidate parameter values, in which case we would obtain \( \alpha = 1 \) and \( \beta = 0 \). Moreover, the value \( \epsilon \) can be calculated directly from the training set.

The following theorem bounds the difference between the expected performance of the selector \( \hat{f} \) and an oracle that selects an optimal selector and an optimal portfolio. The proof is in the full version (Balcan, Sandholm, and Vitercik 2020).

Theorem 5.2. Suppose that each dual function \( u^*_p \) is piecewise constant with at most \( t \) pieces. Given a training set \( S \subseteq Z \) of size \( N \), suppose we learn an \( (\alpha, \beta, \epsilon) \)-optimal
portfolios \( \mathcal{P} \subset \mathbb{R} \) and algorithm selector \( \hat{f} : \mathcal{Z} \rightarrow \mathcal{P} \) in \( \mathcal{F} \). With probability \( 1 - \delta \) over the draw \( \mathcal{S} \sim \mathcal{D}^N \),
\[
\mathbb{E}_{z \sim \mathcal{D}} \left[ u_{\hat{f}(z)}(z) \right] \\
\geq \alpha \max_{P : |P| \leq \kappa} \mathbb{E} \left[ \max_{\rho \in P} u_{\rho}(z) \right] - \epsilon - \hat{O} \left( H \sqrt{\frac{d + \kappa}{N}} \right),
\]
where \( \hat{d} \) is the Natarajan dimension of \( \mathcal{F} \).

**Proof sketch.** First, let \( \mathcal{P}^* \) be the optimal portfolio in the sense that \( \mathcal{P}^* = \arg\max_{P \subset \mathbb{R} : |P| \leq \kappa} \mathbb{E}_{z \sim \mathcal{D}} \left[ \max_{\rho \in P} u_{\rho}(z) \right] \). We use a Hoeffding bound to relate the expected performance of \( \mathcal{P}^* \) under the oracle algorithm selector and its average performance over the training set. We then use Definition 5.1 to relate the latter quantity to the average performance of the learned selector \( \hat{f} \) over the training set. Finally, we use Theorem 3.4 to relate the average performance of \( \hat{f} \) to its expected performance. Putting all of these bounds together, we prove the theorem statement.

We can obtain symmetric guarantees when our goal is to minimize rather than maximize a performance measure.

## 6 Experiments

We provide experiments that illustrate the tradeoff we investigated from a theoretical perspective in the previous sections: as we increase the portfolio size, we can hope to include a well-suited parameter setting for any problem instance, but it becomes increasingly difficult to avoid overfitting. We illustrate this in the context of integer programming algorithm configuration. We configure CPLEX, one of the most widely used commercial solvers. CPLEX uses the branch-and-cut (B&C) algorithm (branch-and-bound with cutting planes, primal heuristics, preprocessing, etc.) to solve integer programs (IPs). We tune a parameter \( \rho \in [0, 1] \) of CPLEX that controls its variable selection policy and has been studied extensively in prior research (Gauthier and Ribiére 1977; Bénichou et al. 1971; Beale 1979; Linderoth and Savelsbergh 1999; Ackterberg 2009; Balcan et al. 2018). We leave CPLEX’s other techniques on and unchanged. We provide a more detailed overview of CPLEX and the parameter we tune in the full version (Balcan, Sandholm, and Vitercik 2020). B&C partitions the IP’s feasible region, finding locally optimal solutions within the sets of the partition, and eventually verifies that the best solution found so far is globally optimal. It organizes this partition as a tree. As in prior research (Balcan et al. 2018; Gupta et al. 2020; Zarpelon et al. 2020), our goal is to find parameter settings leading to small trees—and thereby fast run time—so we define \( u_{\rho}(z) \) to be the size of the tree B&C builds. We aim to learn a portfolio \( \hat{P} \) and selector \( \hat{f} \) resulting in small expected tree size \( \mathbb{E} \left[ u_{\hat{f}(z)}(z) \right] \).

**Distribution over IPs.** We analyze a distribution over IPs formulating the combinatorial auction winner determination problem, which we generate using the Combinatorial Auction Test Suite (Leyton-Brown, Pearson, and Shoham 2000). We use the “arbitrary” generator with 200 bids and 100 goods, resulting in IPs with around 200 variables, and the “regions” generator with 400 bids and 200 goods, resulting in IPs with around 400 variables. We define a heterogeneous distribution \( \mathcal{D} \) as follows: with equal probability, we draw an instance from the “arbitrary” or “regions” distributions. To assign features to these IPs, we use all the features developed in prior research by Leyton-Brown, Pearson, and Shoham (2000) and Hutter et al. (2014), resulting in 140 features.

**Experimental procedure.** We first learn a portfolio of size 10 in the following way. We draw a training set of \( M = 1000 \) IPs \( z_1, \ldots, z_M \sim \mathcal{D} \) and solve for the dual functions \( u_{\rho_1}^1, \ldots, u_{\rho_M}^M \)—which measure tree size as a function of the parameter \( \rho \)—using the algorithm described in Appendix D.1 of the paper by Balcan et al. (2018). These functions are piecewise-constant with at most \( t \) pieces, for some \( t \in \mathbb{N} \). Therefore, there are at most \( Mt \) parameter settings leading to different algorithmic performance over the training set. Let \( \mathcal{P} \) be this set of parameter settings. We use a greedy algorithm to select 10 parameter settings from \( \mathcal{P} \). First, we find a parameter setting \( \rho_1 \) which minimizes average tree size over the training set: \( \rho_1 \in \arg\min_{\rho \in \mathcal{P}} \sum_{i=1}^M u_{\rho}^i(z) \). Then, we find a parameter setting \( \rho_2 \) that minimizes average tree size when the better of \( \rho_1 \) or \( \rho_2 \) is used: \( \rho_2 \in \arg\min_{\rho \in \mathcal{P}} \min_{i=1}^M \left\{ u_{\rho}^i(z) \right\} \). We continue greedily until we have a portfolio \( \mathcal{P} = \{\rho_1, \ldots, \rho_{10}\} \).

We then use a regression forest to select among parameter settings in the portfolio \( \mathcal{P} \). Prior research (Hutter et al. 2014) has illustrated that regression forests can be strong predictors of B&C runtime. Here, we use them to predict B&C tree size. A regression forest is a set \( F = \{T_1, \ldots, T_M\} \) of regression trees (reviewed in Section 4.2). On an input IP \( z \), the regression forest’s prediction, denoted \( h_F(z) \), is the average of the trees’ predictions: \( h_F(z) = \frac{1}{M} \sum_{i=1}^M h_{T_i}(z) \). We train regression forests \( T_1, \ldots, T_{10} \) for each of the 10 parameter settings in the portfolio \( \mathcal{P} \). Then we define the algorithm selector \( \hat{f}(z) = \rho_i \) where \( i = \arg\min_{j \in [10]} \left\{ h_{T_j}(z) \right\} \).

To learn the regression forest, we draw a training set \( z_1, \ldots, z_N \sim \mathcal{D} \) of IPs (with \( N \) specified below). For each parameter setting \( \rho_i \) in \( \mathcal{P} \) and IP \( z_j \), we compute \( u_{\rho_i}(z_j) \), the size of the tree B&C builds using the parameter setting \( \rho_i \). We then train the forest \( F_i \) corresponding to the parameter setting \( \rho_i \) using the labeled training set \( \{(z_1, u_{\rho_i}(z_1)), \ldots, (z_N, u_{\rho_i}(z_N))\} \). We use Python’s default scikit-learn regression forest (Pedregosa et al. 2011).

In Figure 1a, we plot the performance of the regression forests as both the training set and portfolio grow. For a fixed training set size \( N \), we train the regression forests \( F_1, \ldots, F_{10} \) using the method described above. We then evaluate performance as a function of the portfolio size \( \kappa \). Specifically, for each \( \kappa \in [10] \), we define a selector \( f_\kappa(z) = \rho_i \) where \( i = \arg\min_{j \in [\kappa]} \left\{ h_{T_j}(z) \right\} \). We draw \( N_t = 10^4 \) test
instances $S_t \sim D^{N_t}$. The test performance of $\hat{f}_\kappa$ is

$$\hat{v}_\kappa = \frac{1}{N_t} \sum_{z \in S_t} u_{\hat{f}_\kappa(z)}(z). \quad (5)$$

In Figure 1a, we plot the multiplicative performance improvement we obtain as we increase $\kappa$. Specifically, we plot $\hat{v}_\kappa / \hat{v}_1$. These are the blue solid ($N = 10^3$), orange dashed ($N = 10^3$), green dotted ($N = 10^4$), and purple dashed ($N = 2 \cdot 10^5$) lines. By the iterative fashion we constructed the portfolio, $\hat{v}_1$ is the performance of the best single parameter setting, so $\hat{v}_1$ is already highly optimized.

We plot a similar curve for the test performance of the oracle algorithm selector which always selects the optimal parameter setting from the portfolio. Specifically, for each portfolio size $\kappa \in [10]$, let $f^*_\kappa$ be the oracle algorithm selector $f^*_\kappa(z) = \arg\min_{p_1, \ldots, p_5} u_{p_1}(z)$. Given a test set $S_t \sim D^{N_t}$, we define the average test performance of $f^*_\kappa$ as

$$v^*_\kappa = \frac{1}{N_t} \sum_{z \in S_t} u_{f^*_\kappa(z)}(z).$$

The blue dotted line equals $v^*_\kappa / v^*_1$ as a function of $\kappa$.

Finally, when the training set is of size $N = 2 \cdot 10^5$, we provide a similar curve for the training performance of the learned algorithm selectors $\hat{f}_\kappa$. Letting $z_1, \ldots, z_N$ be the training set, we denote the average training performance as

$$\hat{v}_\kappa = \frac{1}{N} \sum_{i=1}^N u_{\hat{f}_\kappa(z_i)}(z_i).$$

The yellow solid line is $\hat{v}_\kappa / \hat{v}_1$ as a function of $\kappa$.

In Figure 1c, we plot $\hat{v}_\kappa / \hat{v}_1$ as a function of the portfolio size $\kappa$ for larger portfolio sizes ranging from 1 to 20. We greedily extend the portfolio $P$ to include an additional 20 parameter settings. We then train 20 regression forests using freshly drawn training sets of size 100 and 1000. This plot illustrates the fact that as we increase the portfolio size, overfitting causes test performance to worsen.

**Discussion.** Focusing first on test performance using the largest training set size $N = 2 \cdot 10^5$, we see that test performance continues to improve as we increase the portfolio size, though training and test performance steadily diverge. This illustrates the tradeoff we investigated from a theoretical perspective in this paper: as we increase the portfolio size, we can hope to include a well-suited parameter setting for every instance, but the generalization error will worsen. Figure 1c shows that for a given training set size, there is a portfolio size after which test performance actually starts to get strictly worse, as our theory predicts. In other words, we observe overfitting: the selector has strong average performance over the training set but poor test performance.

**7 Conclusions**

We provided guarantees for learning a portfolio of parameter settings in conjunction with an algorithm selector for that portfolio. We provided a tight (up to log factors) bound on the number of samples sufficient and necessary to ensure that the selector’s average performance on the training set generalizes to its expected performance on the real unknown problem instance distribution. Our guarantees apply in the widely-applicable setting where the algorithm’s performance on any input problem instance is a piecewise-constant function of its parameters. Our theoretical bounds indicate that even with an extremely simple algorithm selector, we cannot hope to avoid overfitting in the worst-case if the portfolio is large. Thus, there is a tradeoff when increasing the portfolio size, since a large portfolio allows for the possibility of including a strong parameter setting for every instance, but this potential for performance improvement is overshadowed by a worsening propensity towards overfitting. We concluded with experiments illustrating this tradeoff in the context of integer programming. A direction for future research is to understand how the diversity of a portfolio impacts its generalization error, since algorithm portfolios are often expressly designed to be diverse.
Acknowledgments

This material is based on work supported by the National Science Foundation under grants CCF-1535967, CCF-1733556, CCF-1910321, IIS-1617590, IIS-1618714, IIS-1718457, IIS-1901403, and SES-1919453; the ARO under awards W911NF1710082 and W911NF2010081; the Defense Advanced Research Projects Agency under cooperative agreement HR00112020003; an AWS Machine Learning Research Award; an Amazon Research Award; a Bloomberg Research Grant; a Microsoft Research Faculty Fellowship; an IBM PhD fellowship; and a fellowship from Carnegie Mellon University’s Center for Machine Learning and Health.

References


Shalev-Shwartz, S.; and Ben-David, S. 2014. Understanding machine learning: From theory to algorithms. Cambridge University Press.


