Optimization with Trained Machine Learning Models Embedded

Artur M. Schweidtmann\textsuperscript{1}, Dominik Bongartz\textsuperscript{2,3}, Alexander Mitsos\textsuperscript{2,*}

\textsuperscript{1} Delft University of Technology, Department of Chemical Engineering, Van der Maasweg 9, Delft 2629 HZ, The Netherlands
\textsuperscript{2} Process Systems Engineering (AVT.SVT), RWTH Aachen University, Forckenbeckstr. 51, 52074 Aachen, Germany.
\textsuperscript{3} Department of Chemical Engineering, KU Leuven, Celestijnenlaan 200F, 3001 Leuven, Belgium

MSC2000: 90C26 90C30 90C90 68T01 60-04

Keywords: Machine learning; Surrogate modeling; Regression; Supervised learning; Deterministic global optimization; Artificial neural networks; Deep learning; Gaussian processes; Reduced-space formulation; Full-space formulation; McCormick relaxations; Bayesian optimization; Hybrid modeling

1 Introduction

Machine learning (ML) gives computers the ability to learn from data without being explicitly programmed. Cases where the data includes input vectors (in $\mathbb{R}^n_d$) and corresponding target vectors (in $\mathbb{R}^n_t$) are known as supervised learning. Regression problems learn continuous variables as targets whereas classification problems learn discrete categories as targets. While linear regression goes back to the least-squares method by Gauss and Legendre in the early 19th century, recent advances in computing led to the breakthrough performance of ML in various domains even surpassing human performance.

Across many engineering and science domains, ML models are trained on data and are subsequently optimized. In chemistry, for instance, ML models are commonly fitted to experimental data. This training usually constitutes an optimization problem where model parameters are varied to minimize the model error on the training data. Then, a subsequent optimization problem can be solved to identify the experimental conditions (i.e., inputs of the ML model) that maximize the experimental performance (i.e., the output of the ML model). We refer to this subsequent optimization problem as optimization with trained ML models embedded. Notably, the ML model parameters are optimization variables during the training and fixed parameters during the optimization with trained ML models embedded. Vice versa, the inputs of the ML model are fixed parameters (determined by the training data) during the training and optimization variables during the optimization with trained ML models embedded. While other chapter in this book deal with the training of ML models (c.f. Section ??), this chapter focuses on the (deterministic global) optimization with trained ML models embedded. Also, this chapter covers the optimization of hybrid models where ML models are combined with mechanistic models.

2 Formulations

As illustrated in Figure 1, there exists a broad variety of ML models ranging from linear regression models to deep artificial neural networks (ANNs).

Once a ML regression model has been trained (and validated) on input data from $\mathcal{D} \subset \mathbb{R}^n_d$ and target data from $\mathbb{R}^n_t$, the trained model usually represents an explicit function $m : \mathcal{D} \rightarrow \mathbb{R}^n_t$. Depending on the chosen model, this function may have different properties, e.g., it may be

- discontinuous (e.g., for ensemble tree models) or continuous (e.g., ANNs),
- nonsmooth (e.g., for ANNs with ReLU activation function) or smooth (e.g., for ANNs with hyperbolic tangent activation function),
- linear or convex nonlinear or nonconvex.

Corresponding author: *A. Mitsos, E-mail: amitsos@alum.mit.edu
2.1 Reduced-Space and Full-Space Model Formulations

For most ML models, there are multiple approaches of embedding the function $m$ in the optimization problem to be solved. One way to classify these approaches is to distinguish between reduced-space formulations and full-space formulations. 

In reduced-space formulations, the ML model is used directly as the function $m$. For example, if the problem to be solved consists in minimizing the output of the ML model over a compact input set $X \subset \mathcal{D}$, the corresponding reduced-space formulation would read

$$\min_{x \in X} m(x).$$

Thus, the only variables are the $n_d$ inputs of the model, and there are no constraints beyond those imposed by the set $X$. If the ML model is combined with other functions, e.g., in a hybrid model containing both ML and mechanistic parts, the problem could take the form

$$\min_{x \in X, y \in \mathcal{Y}} f(x, y, m(x))$$

$$\text{s.t. } h(x, y, m(x)) = 0$$

$$g(x, y, m(x)) \leq 0,$$

where $y \in \mathcal{Y} \subset \mathbb{R}^{n_y}$ are additional optimization variables, and $f$, $h$, and $g$ are some objective function, equality constraints, and inequality constraints, respectively, all of which may depend on the outputs of the ML model as well as the variables $x$ and $y$. Alternatively, the inputs of the ML model may not be optimization variables themselves, but rather outputs of some other function $i : \mathcal{Y} \to X$:

$$\min_{y \in \mathcal{Y}} f(y, m(i(y)))$$

$$\text{s.t. } h(y, m(i(y))) = 0$$

$$g(y, m(i(y))) \leq 0.$$

In a full-space formulation, internal variables of the ML models become part of the optimization problem as optimization variables, and equations defining the ML model become constraints. In this case, the function $m$ does not occur in the problem as a single function that can be evaluated to obtain outputs for given inputs, but instead, the evaluation becomes part of solving the optimization problem. Note that typically a range of full-space formulations exists that differ in how many and which internal variables and equations become part of the optimization problem. These can also be considered as intermediate versions between full- and reduced-space formulations. Similar to the reduced-space formulation, more complex problems can of course be constructed where the ANN is combined with other functions, e.g., in a hybrid mechanistic/data-driven model.
From a modeling perspective, reduced-space formulations are very intuitive and easy to implement in procedural environments such as e.g., when modeling in Python. In these environments, the ML models are naturally implemented as functions that can just be used in the optimization problem. In contrast, when modeling in an equation-oriented environment such as, e.g., GAMS or AMPL, the reduced-space formulation is often much more challenging to implement. For example, to write an ANN in a reduced-space formulation, one would have to symbolically substitute the outputs of each layer into the activation function of the next layer in order to ultimately obtain an expression for the outputs of the ANN (i.e., those of the last layer) as a function of its inputs (i.e., the inputs of the first layer). In such an environment, it is more natural to write a full-space formulation that merely requires defining the outputs of all layers as variables and writing the corresponding equations as constraints.

From a computational perspective, the chosen formulation can have a considerable impact on the effort for solving the problem, because the problem looks very different to the optimizer: The reduced-space formulations have much fewer variables and equality constraints than the full-space formulations but contain potentially very complicated functions. In particular, the number of variables and constraints in the optimization problem is independent of the type of ML model used or the amount of data used for training it. In the full-space formulation, the number of optimization variables and constraints may increase with the complexity of the ML model (e.g., for an ANN, it may increase with the number of hidden layers, or with the number of neurons per layer\(^{21}\)), or even with the amount of data that was used for training the model (e.g., for Gaussian processes\(^{19}\)). As discussed in the following, it may depend on the optimization algorithm how efficiently either formulation can be solved.

An alternative classification of ways of incorporating ML models in optimization problems is given by Lombardi & Milano\(^{14}\) who distinguish embedding an ML model by expanding the language as opposed to encoding the ML model using the native language. This first case entails defining a new function representing the ML model that can then be used when formulating the optimization problem. If this is done for an entire ML model, this would correspond to a reduced-space formulation as defined above. This approach may, however, only introduce certain components of an ML model as new functions, e.g., activation functions of ANNs. The second case entails representing the ML model via functions that are already available in the chosen optimization environment. This could in fact be done for both full space and reduced space formulations. In full space formulations, the ML model consists of a number of variables and constraints in the optimization problem, while in RS formulations, the functions encoding the ML model are a composition of existing functions.

### 2.2 Modeling Nonsmooth Functions

For some ML models such as ANNs with ReLU activation function, there is an additional distinction regarding the way the nonsmoothness is handled. On the one hand, the ReLU activation function can be formulated with the max function. This enables a reduced-space formulation of the ANN, meaning that the network can be expressed as an explicit function mapping the inputs to the outputs of the network. However, this function is usually nonconvex and nonsmooth and thus challenging to solve to global optimality. On the other hand, the max function can be reformulated as a piecewise linear function modeled with a binary variable that determines which of the linear pieces is active (c.f. Section 3.4). This avoids the use of nonsmooth functions in the model at the expense of adding one binary variable per neuron with ReLU activation function. Furthermore, this makes a reduced-space formulation as described above impossible, because the optimizer now needs to control the binary variables, which are part of the internals of the ANN. Typically, this also entails the use of additional constraints, e.g., in the form of a Big-M formulation. Similarly, the nonsmoothness of tree models can be reformulated using binary variables (c.f. Section 3.3).

### 2.3 Validity Domain Modeling

An additional aspect is related to the domain of the function \(m\). Since the ML model has been trained on a limited number of data points \((x_i, t_i) \in \mathbb{R}^{n_d} \times \mathbb{R}^{n_t}\), it can not be expected to give a good description of the underlying, “true” input-output relationship for arbitrary inputs \(x \in \mathbb{R}^{n_d}\). If \(x\) is far from the inputs of the training data, the model needs to extrapolate, which can give unreliable results. In this sense, it may be prudent to add constraints to the optimization problem that restrict the inputs of the ML model
to values that are not too far from its training data. Such constraints could take the form of the convex hull of the training data points as in the convex region surrogate model, or an approximation of the possibly nonconvex region covered by the training data points, e.g., obtained by one-class classifiers. Also, the distance to training data points can be included as a penalty to the objective function.

3 Machine Learning Models

In this section, we discuss a few common ML models and possible optimization formulations with these ML models embedded.

3.1 Convex region surrogate models

Convex region surrogate models were proposed by Zhang et al. They consist of affine functions defined over a number of convex polytopes that are constructed to contain the training data. They can approximate nonlinear (potentially discontinuous) functions over nonconvex regions. Given the regions into which the domain is divided according to the model, evaluating the model at a point amounts to identifying which region this point lies in and evaluating the affine function defined on this region.

The models are originally devised in a Generalized Disjunctive Programming (GDP) setting, but they can be reformulated as MILPs, e.g., via the hull reformulation. This representation is particularly suitable for the optimization problem in which the model is to be embedded is already a MILP. According to the above classification, this is a full-space formulation of the model, because the optimization solver controls additional variables and constraints.

To our knowledge, a reduced-space formulation of this model has not been attempted yet. In its purest form, this would entail expressing the model as a piecewise-defined function of \( x \). In this case, the challenge lies in the fact that the function may be discontinuous, and that the constraints on the input values need to be accounted for explicitly.

3.2 Gaussian processes

Gaussian processes, also known as Kriging, are infinite-dimensional generalizations of multivariate Gaussian distributions. Their predictions follow Gaussian distributions and thus include an estimate and a variance. Formally, Gaussian processes are defined by its mean function \( \mu(x) := \mathbb{E}[f(x)] \) and covariance function \( k(x, x') := \mathbb{E}[ (y(x) - \mu(x)) (y(x') - \mu(x'))^T ] \), where \( y \) is an observation from \( f(x) \). The most common covariance function is the squared exponential covariance function, \( k_{SE}(r) := \exp(-\frac{1}{2} r^2) \), where \( r := \sqrt{(x - x')^T \Lambda (x - x')} \) is a Euclidean distance with weighting factors \( \Lambda := \text{diag}(\lambda_1^2, \ldots, \lambda_n^2) \). The hyperparameters \( \theta = [\lambda_1, \ldots, \lambda_n] \) are adjusted during training to maximize the probability that the Gaussian process fits the training data. The Gaussian process posterior distribution is obtained by conditioning the prior distributions on training data \( (\mathbf{X}, \mathbf{Y}) \), \( f(x) \sim \mathcal{GP}(\mu(x), k(x, x'))|\mathbf{X}, \mathbf{Y} \). The estimate and variance of the posterior can be calculated by

\[
\begin{align*}
    m_D(x) &= K_{x,X} (K_{XX})^{-1} y, \\
    k_D(x) &= K_{x,x} - K_{x,X} (K_{XX})^{-1} K_{X,x},
\end{align*}
\]

where \( K_{X,X} := [k(x_i, x_j)] \in \mathbb{R}^{N \times N} \) is the covariance matrix of the data, \( K_{x,X} := \left[ k(x, x_1), \ldots, k(x, x_N) \right] \in \mathbb{R}^{1 \times N} \) is the covariance vector between the candidate point \( x \) and the training data, and \( K_{x,x} := k(x, x) \).

Trained Gaussian processes are commonly embedded in optimization problems for iterative planning of (computational) experiments through Bayesian optimization. Therein, an acquisition function is maximized to identify an optimal tradeoff between exploration and exploitation. One common example is the maximization of the expected improvement acquisition function. Furthermore, Gaussian processes are commonly used as surrogate models when only limited data is available. Optimization problems with trained Gaussian processes embedded are NLPs as the covariance function is nonlinear. Moreover, the optimization of acquisition functions are known to exhibit a large number of (suboptimal) local optima. In the previous literature, optimization problems with trained Gaussian processes embedded have mostly been solved using...
full space formulations (e.g.,\textsuperscript{15}) while recent work indicated that the reduced space formulation can be advantageous.\textsuperscript{19} Notably, tailored convex and concave relaxations of covariance and acquisition functions can improve the solution times for these problems significantly.\textsuperscript{19}

### 3.3 Decision tree ensembles

Decision tree ensembles are popular models for representing nonlinear relationships in large-scale, noisy data sets including both continuous and discrete inputs. They consist of multiple decision trees, where a decision tree predicts the output based on a sequence of queries involving the inputs (e.g., if $x > c$, where $c$ is a constant parameter, follow branch 1 of the tree, if $x \leq c$ follow branch 2 of the tree). For given values of the inputs, the output is computed by following the tree based on the answers to those queries from the root to a certain leaf, which then contains the output value. In a tree ensemble, the output of multiple trees is averaged (in the case of regression) to yield the output of the overall model to improve the prediction accuracy. The most popular models of this type are gradient boosted trees, where the trees are built sequentially by learning the residual between the data and the previous tree, and random forests, which consist of trees trained on random subsets of the data as well as the inputs used in the queries.

By construction, tree ensemble models predict the output as a piecewise constant function of the inputs. As such, they are inherently discontinuous, which makes the optimization of problems with trained ensemble models embedded difficult to optimize. Recently, Misic\textsuperscript{19} and Biggs et al.\textsuperscript{4} presented mixed-integer formulations for representing ensemble tree models in optimization problems. They encode the results of the queries as binary variables and introduce constraints that enforce the selection of the correct leaf node based on these variables. The approach of Biggs et al.\textsuperscript{4} has the advantage that additional (linear) constraints are easier to incorporate.

Misener and co-workers recently extended these approaches by incorporating an uncertainty measure as a penalty term in the objective. This term penalizes large deviation of inputs from the training data, either considering the distance to the nearest (clusters of) data points\textsuperscript{23} or the distance to a subspace of the input space containing the data.\textsuperscript{17} The former approach was also used in the opposite sense for application in Bayesian optimization, i.e., to enhance exploration rather than restrict the search to the vicinity of the training data.\textsuperscript{23}

Optimization with tree ensembles embedded becomes particularly challenging when the ensembles get large (e.g., several thousand trees) or when the trees contain many queries. Therefore, dedicated approaches for large models have been proposed. These are based on Benders decomposition\textsuperscript{11,16}, truncation of the tree depth\textsuperscript{16}, considering subsets of the trees\textsuperscript{4,17}, or dedicated B&B procedures.\textsuperscript{17,24}

### 3.4 Artificial neural networks

ANNs are one of the most common ML models and they are an essential block of deep learning architectures (see also, e.g.,\textsuperscript{5,13}). Feed-forward ANNs, also known as multilayer perceptrons, consist of $N$ (hidden) layers including $D^{(k)}$ neurons. Generally, ANNs can be viewed as directed acyclic graphs connecting neurons that are organized in layers. The first layer corresponds to the inputs of the ANN and the last layer corresponds to its outputs. For each layer $k \geq 2$, the output vector $z^{(k)}$ of the layer $k$ is given by $z^{(k)} = h_k\left(W^{(k-1)}z^{(k-1)} + b^{(k-1)}\right)$ where $h_k(\cdot)$ is an activation function, $W^{(k-1)}$ is a weight matrix and $b^{(k-1)} \in \mathbb{R}^{D^{(k)}}$ a bias vector. Notably, the weights ($W^{(k)}$) and bias vectors ($b^{(k)}$) are known constant parameters in optimization problems with trained ANNs embedded. For regression problem, the hyperbolic tangent function, $h_k(x) = \tanh(x)$, has been the most common activation function in ANNs. Also, the rectified linear unit (ReLU) activation function, $h_k(x) = \max(x, 0)$, is increasingly common for deep ANNs as it is more effectively trainable.\textsuperscript{19}

Given the nonlinear activation functions, optimization problems with ANNs embedded are generally nonlinear optimization problems (NLPs). As discussed in Section\textsuperscript{2.1} ANNs can be modeled using full space or reduced space formulations. Previous studies indicate that the reduced space formulation has a favorable performance compared to the full space formulation for deterministic global optimization with trained ANNs embedded.\textsuperscript{23} This is mostly due to the increased problem size of full space formulations and the difficulty to solve large-scale NLPs to global optimality.
As the ReLU function is a piecewise linear function, it can also be reformulated through binary variables and linear constraints. This allows formulating optimization problems with trained ReLU ANNs as mixed-integer linear programs (MILPs). As intermediate variables are introduced to the optimization problem, these MILP formulations are essentially full space formulations. While most previous works use big-M formulations for ReLU ANNs, recent works also proposed sharp or ideal formulations as well as hybrids. Moreover, most previous works employ specialized bound tightening techniques. Recently, open-source modeling tools for ReLU ANNs as MILP have been proposed bridging established ML and optimization tools.

To the best of our knowledge, a comparison between the nonlinear reduced space formulation and the MILP full space formulation has not yet been published in the literature. Thus, it still remains unclear what the most efficient problem formation is. While the reduced space formation has significantly smaller problem sizes, the MILP formulation is linear. Irrespective of the formulation, it appears that the problem size of previous studies has been limited by high computational times.

4 Conclusions

Trained ML models are commonly embedded in optimization problems. In many cases, this leads to large-scale NLPs that are difficult to solve to global optimality. While ML models frequently lead to large problems, they also exhibit homogeneous structures and repeating patterns (e.g., layers in ANNs). Thus, specialized solution strategies can be used for large problem classes. Recently, there have been some promising works proposing specialized reformulations using mixed-integer programming or reduced space formulations. However, further work is needed to develop more efficient solution approaches and keep up with the rapid development of new ML model architectures.

References

[1] R. Anderson, J. Huchette, W. Ma, C. Tjandraatmadja, and J. P. Vielma. Strong mixed-integer programming formulations for trained neural networks. *Mathematical Programming*, pages 1–37, 2020.

[2] R. Arora, A. Basu, P. Mianjy, and A. Mukherjee. Understanding deep neural networks with rectified linear units. *arXiv preprint arXiv:1611.01491*, 2016.

[3] D. Bergman, T. Huang, P. Brooks, A. Lodi, and A. U. Raghunathan. Janos: An integrated predictive and prescriptive modeling framework. *INFORMS Journal on Computing*, 2021.

[4] M. Biggs, R. Hariss, and G. Perakis. Optimizing objective functions determined from random forests. *Available at SSRN 2986630*, 2017.

[5] C. M. Bishop. *Pattern recognition and machine learning*. Information science and statistics. Springer, New York, NY, 8 edition, 2009.

[6] D. Bongartz and A. Mitsos. Deterministic global flowsheet optimization: Between equation-oriented and sequential-modular methods. *AIChE Journal*, 65(3):1022–1034, 2019.

[7] F. Boukouvala and C. A. Floudas. Argonaut: Algorithms for global optimization of constrained grey-box computational problems. *Optimization Letters*, 11(5):895–913, 2017.

[8] J. A. Caballero and I. E. Grossmann. Rigorous flowsheet optimization using process simulators and surrogate models. In *Computer Aided Chemical Engineering*, volume 25, pages 551–556. Elsevier, 2008.

[9] C.-H. Cheng, G. Nührenberg, and H. Ruess. Maximum resilience of artificial neural networks. In *International Symposium on Automated Technology for Verification and Analysis*, pages 251–268. Springer, 2017.

[10] M. Fischetti and J. Jo. Deep neural networks and mixed integer linear optimization. *Constraints*, 23(3):296–309, 2018.
[11] D. R. Jones, M. Schonlau, and W. J. Welch. Efficient global optimization of expensive black-box functions. *Journal of Global optimization*, 13(4):455–492, 1998.

[12] J. Kim and S. Choi. On local optimizers of acquisition functions in bayesian optimization. *arXiv preprint arXiv:1901.08350*, 2019.

[13] Y. LeCun, Y. Bengio, and G. Hinton. Deep learning. *Nature*, 521(7553):436–444, 2015.

[14] M. Lombardi and M. Milano. Boosting combinatorial problem modeling with machine learning. *arXiv preprint arXiv:1807.05517*, 2018.

[15] L. Lueg, B. Grimstad, A. Mitsos, and A. M. Schweidtmann. relumip: Open source tool for milp optimization of relu neural networks. Oct 2021.

[16] V. V. Mišić. Optimization of tree ensembles. *Operations Research*, 68(5):1605–1624, 2020.

[17] M. Mistry, D. Letsios, G. Krennrich, R. M. Lee, and R. Misener. Mixed-integer convex nonlinear optimization with gradient-boosted trees embedded. *INFORMS Journal on Computing*, 2020.

[18] C. E. Rasmussen. Gaussian processes in machine learning. In *Advanced lectures on machine learning*, pages 63–71. Springer, 2004.

[19] A. M. Schweidtmann, D. Bongartz, D. Grothe, T. Kerkenhoff, X. Lin, J. Najman, and A. Mitsos. Deterministic global optimization with gaussian processes embedded. *Mathematical Programming Computation*, 13(3):553–581, 2021.

[20] A. M. Schweidtmann, E. Esche, A. Fischer, M. Kloft, J.-U. Repke, S. Sager, and A. Mitsos. Machine learning in chemical engineering: A perspective. *Chemie Ingenieur Technik*, 93(12):2029–2039, 2021.

[21] A. M. Schweidtmann and A. Mitsos. Deterministic global optimization with artificial neural networks embedded. *Journal of Optimization Theory and Applications*, 180(3):925–948, 2019.

[22] A. M. Schweidtmann, J. M. Weber, C. Wende, L. Netze, and A. Mitsos. Obey validity limits of data-driven models through topological data analysis and one-class classification. *Optimization and Engineering*, pages 1–22, 2021.

[23] S. M. Stigler. Gauss and the invention of least squares. *the Annals of Statistics*, pages 465–474, 1981.

[24] A. Thebelt, J. Kronqvist, M. Mistry, R. M. Lee, N. Sudermann-Merx, and R. Misener. Entmoot: A framework for optimization over ensemble tree models. *Computers & Chemical Engineering*, 151:107343, 2021.

[25] V. Tjeng, K. Xiao, and R. Tedrake. Evaluating robustness of neural networks with mixed integer programming. *arXiv preprint arXiv:1711.07356*, 2017.

[26] C. Tsay, J. Kronqvist, A. Thebelt, and R. Misener. Partition-based formulations for mixed-integer optimization of trained relu neural networks. *arXiv preprint arXiv:2102.04373*, 2021.

[27] M. Von Stosch, R. Oliveira, J. Peres, and S. F. de Azevedo. Hybrid semi-parametric modeling in process systems engineering: Past, present and future. *Computers & Chemical Engineering*, 60:86–101, 2014.

[28] Q. Zhang, I. E. Grossmann, A. Sundaramoorthy, and J. M. Pinto. Data-driven construction of convex region surrogate models. *Optimization and Engineering*, 17(2):289–332, 2016.