Rajeev Verma / University of Amsterdam



DELTA LAB







Alexander Timans

Rajeev Verma / University of Amsterdam



DELTA LAB





Statistical Science 2001, Vol. 16, No. 3, 199–231

Statistical Modeling: The Two Cultures

Leo Breiman



Abstract. There are two cultures in the use of statistical modeling to reach conclusions from data. One assumes that the data are generated by a given stochastic data model. The other uses algorithmic models and treats the data mechanism as unknown. The statistical community has been committed to the almost exclusive use of data models. This commitment has led to irrelevant theory, questionable conclusions, and has kept statisticians from working on a large range of interesting current problems. Algorithmic modeling, both in theory and practice, has developed rapidly in fields outside statistics. It can be used both on large complex data sets and as a more accurate and informative alternative to data modeling on smaller data sets. If our goal as a field is to use data to solve problems, then we need to move away from exclusive dependence on data models and adopt a more diverse set of tools.

Statistical Science 2001, Vol. 16, No. 3, 199–231

Statistical Modeling: The Two Cultures

Leo Breiman





Statistical Science 2001, Vol. 16, No. 3, 199-231

Statistical Modeling: The Two Cultures

Leo Breiman





The data-modelling culture

The role of statistical inference in machine learning





Machine Learning





Model validation. Measured by predictive accuracy.







Model validation. Measured by predictive accuracy.

Machine Learning: is this enough?







Model validation. Measured by predictive accuracy.

Machine Learning: is this enough?









Machine Learning: Risk Controlling frameworks



 $g(\hat{f}(x),\,\cdot\,)$

Machine Learning: Risk Controlling frameworks



 $g(\hat{f}(x), \cdot)$

Machine Learning: Risk Controlling frameworks





 $g(\hat{f}(x),\psi)$

Machine Learning: Risk Controlling frameworks





Machine Learning: Risk Controlling frameworks



 $\hat{f}_{\psi}(x) := g(\hat{f}(x), \psi)$

e.g. false positive rate



Machine Learning: Risk Controlling frameworks



e.g. false positive rate



Machine Learning: Risk Controlling frameworks

 $\mathscr{R}(\psi) = \mathbb{E}_P \left[\mathscr{C}(\hat{f}_{\psi}(X), Y) \right]$ control this risk





Conformal Risk Control

Anastasios N. Angelopoulos¹, Stephen Bates¹, Adam Fisch², Lihua Lei³, and Tal Schuste

¹University of California, Berkeley ²Massachusetts Institute of Technology ³Stanford University ⁴Google Research

Abstract

We extend conformal prediction to control the expected value of any monotone loss function. The algorithm generalizes split conformal prediction together with its coverage guarantee. Like conformal

Learn then Test: Calibrating Predictive Algorithms to Achieve Risk Control

Anastasios N. Angelopoulos, Stephen Bates, Emmanuel J. Candès, Michael I. Jordan, Lihua Lei

October 3, 2022

Abstract

We introduce a framework for calibrating machine learning models so that their predictions satisfy explicit,

Machine Learning: Risk Controlling frameworks

Distribution-Free, Risk-Controlling Prediction Sets

Stephen Bates, Anastasios Angelopoulos, Lihua Lei, Jitendra Malik, Michael I. Jordar

August 6, 2021

Abstract

While improving prediction accuracy has been the focus of machine learning in recent years, this alone does not suffice for reliable decision-making. Deploying learning systems in consequential settings

Conformal Risk Control

Anastasios N. Angelopoulos¹, Stephen Bates¹, Adam Fisch², Lihua Lei³, and Tal Schuste

¹University of California, Berkeley ²Massachusetts Institute of Technology ³Stanford University ⁴Google Research

Abstract

We extend conformal prediction to control the expected value of any monotone loss function. The algorithm generalizes split conformal prediction together with its coverage guarantee. Like conformal

Learn then Test: Calibrating Predictive Algorithms to Achieve Risk Control

Anastasios N. Angelopoulos, Stephen Bates, Emmanuel J. Candès, Michael I. Jordan, Lihua Lei

October 3, 2022

Abstract

We introduce a framework for calibrating machine learning models so that their predictions satisfy explicit,

Machine Learning: Risk Controlling frameworks

Distribution-Free, Risk-Controlling Prediction Sets

Stephen Bates, Anastasios Angelopoulos, Lihua Lei, Jitendra Malik, Michael I. Jordar

August 6, 2021

Abstract

While improving prediction accuracy has been the focus of machine learning in recent worrs, this alone does ^rAlgorithmic learning in a random world

ettings

by <u>Vladimir Vovk</u>, <u>Alex Gammerman</u>, and <u>Glenn Shafer</u>

Springer, 2005 (first edition), 2022 (second edition)



The main topic of this book is conformal prediction, a method machine learning, and unlike other state-of-the-art methods, the

The book integrates mathematical theory and revealing experir are applied to independent and identically distributed data, and results to models called repetitive structures, which originate in existing methods of machine learning, including newer method

Topics and Features:

- Describes how conformal predictors yield accurate and reliable
- Handles both classification and regression problems
- Explains how to apply the new algorithms to real-world data se
- Demonstrates the infeasibility of some standard prediction task
- Explains connections with Kolmogorov's algorithmic randomn
- Develops new methods of probability forecasting and shows he

Researchers in computer science, statistics, and artificial intelli machine learning. Practitioners and students in all areas of rese

e.g. false positive rate



 $\hat{f}_{\psi}(x) := g(\hat{f}(x), \psi)$

$$\mathcal{R}(\psi) = \mathbb{E}_{P} \left[\ell\left(\hat{f}_{\psi}(X), Y\right) \right]$$

control this risk
Goal:find threshold(s) $\hat{\psi}$ such that
$$\mathbb{P} \{ \mathcal{R}(\hat{\psi}) \leq \epsilon \} \geq 1 - \delta$$

treat the patient



 $\{(x_i, y_i)\}_{i=1}^N \quad (x, y) \sim P_0$

calibration set

Risk Controlling frameworks: conformal prediction

$$\mathcal{R}(\psi) = \mathbb{E}_P\left[\ell\left(\hat{f}_{\psi}(X), Y\right)\right]$$

control this risk

 $\{(x_i, y_i)\}_{i=1}^N \quad (x, y) \sim P_0$

calibration set

$s: X \times Y \rightarrow [0,B]$

compatibility score

Risk Controlling frameworks: conformal prediction

$$\mathcal{R}(\psi) = \mathbb{E}_P\left[\ell\left(\hat{f}_{\psi}(X), Y\right)\right]$$

control this risk

 $\{(x_i, y_i)\}_{i=1}^N \quad (x, y) \sim P_0$ calibration set $s: X \times Y \rightarrow [0,B]$ compatibility score $\mathscr{C}: \mathbb{I}\{s(x, y) \le \psi\}$ loss function

$$\mathcal{R}(\psi) = \mathbb{E}_P\left[\ell\left(\hat{f}_{\psi}(X), Y\right)\right]$$

control this risk

 $\{(x_i, y_i)\}_{i=1}^N \quad (x, y) \sim P_0$ calibration set $s: X \times Y \rightarrow [0,B]$ compatibility score $\mathscr{C}: \mathbb{I}\{s(x, y) \le \psi\}$ loss function $\mathscr{R}(\psi) = \mathbb{P}\{s(X, Y) \le \psi\}$ **Risk function**

$$\mathcal{R}(\psi) = \mathbb{E}_P\left[\ell\left(\hat{f}_{\psi}(X), Y\right)\right]$$

control this risk

 $\{(x_i, y_i)\}_{i=1}^N \quad (x, y) \sim P_0$ calibration set $s: X \times Y \rightarrow [0,B]$ compatibility score $\mathscr{C}: \mathbb{I}\{s(x, y) \le \psi\}$ loss function $\mathscr{R}(\psi) = \mathbb{P}\{s(X, Y) \le \psi\}$ **Risk function**

empirical CDF function





Goal:find threshold(s) $\hat{\psi}$ such that

 $\mathbb{P}\{\mathscr{R}(\hat{\psi}) \leq \epsilon\} \geq 1 - \delta$



empirical CDF function





Goal:find threshold(s) $\hat{\psi}$ such that

 $\mathbb{P}\{\mathscr{R}(\hat{\psi}) \leq \epsilon\} \geq 1 - \delta$

e.g. false positive rate



$$\mathcal{R}(\psi) = \mathbb{E}_P \left[\ell \left(\hat{f}_{\psi}(X), Y \right) \right]$$

control this risk
Goal:find threshold(s) $\hat{\psi}$ such that
 $\mathbb{P} \{ \mathcal{R}(\hat{\psi}) \leq \epsilon \} \geq 1 - \delta$

Static batch setting: $\hat{\psi}$ is computed once using hold-out calibration set,

When accurate prediction models yield harmful self-fulfilling prophecies

Wouter A.C. van Amsterdam, MD, PhD*

Department of Data Science and Biostatistics Julius Center of Health Sciences and Primary Care University Medical Center Utrecht, Utrecht, the Netherlands University of Utrecht, Utrecht, the Netherlands Heidelberglaan 100, 3584 CX Utrecht, the Netherlands corresponding author

Nan van Geloven, PhD

Department of Biomedical Data Sciences Leiden University Medical Center, Leiden, the Netherlands

Jesse H. Krijthe, PhD

Pattern Recognition & Bioinformatics Delft University of Technology, Delft, the Netherlands

Rajesh Ranganath, PhD

Courant Institute of Mathematical Science, Department of Computer Science Center for Data Science New York University, New York City, USA

Giovanni Cinà*, PhD

Department of Medical Informatics Amsterdam University Medical Center, Amsterdam, the Netherlands Institute for Logic, Language and Computation University of Amsterdam, Amsterdam, the Netherlands Pacmed, Amsterdam, the Netherlands

W.A.C.VANAMSTERDAM-3@UMCUTRECHT.NL

G.CINA@AMSTERDAMUMC.NL

¹UvA-Bosch Delta Lab, University of Amsterdam ²Department of Computer Science, Johns Hopkins University

Abstract

Machine learning systems deployed in the real world must operate under dynamic and often unpredictable distribution shifts. This challenges the validity of statistical safety assurances on the system's risk established beforehand. Common risk control frameworks rely on fixed assumptions and lack mechanisms to continuously monitor deployment reliability. In this work, we propose a general framework for the real-time monitoring of systems has the potential to thwart any 'quality assurance' stamp these methods derive from their static inference. Challenges like outliers, distribution shifts and feedback

loops are commonplace [Koh et al., 2021]. In fact, you

terdam et al. [2025] argue that an effective machine learning model should *actively* affect the real-world—distribution shift is then not merely an artifact or deployment challenge, but rather a manifestation of a successfully operating system. Hence, any decision-making parameters necessitate *continuous monitoring* during deployment, and the user should be notified when statistical reliability is faltering.

.

There is a need to continuously monitor the risk control guarantees on the predictive systems.

¹UvA-Bosch Delta Lab, University of Amsterdam ²Department of Computer Science, Johns Hopkins University

Abstract

Machine learning systems deployed in the real world must operate under dynamic and often unpredictable distribution shifts. This challenges the validity of statistical safety assurances on the system's risk established beforehand. Common risk control frameworks rely on fixed assumptions and lack mechanisms to continuously monitor deployment reliability. In this work, we propose a general framework for the real-time monitoring of systems has the potential to thwart any 'quality assurance' stamp these methods derive from their static inference. Challenges like outliers, distribution shifts and feedback

loops are commonplace [Koh et al., 2021]. In feet, year

terdam et al. [2025] argue that an effective machine learning model should *actively* affect the real-world—distribution shift is then not merely an artifact or deployment challenge, but rather a manifestation of a successfully operating system. Hence, any decision-making parameters necessitate *continuous monitoring* during deployment, and the user should be notified when statistical reliability is faltering.

.







On Continuous Monitoring of Risk Violations under Unknown Shift $Z = \ell(\hat{\psi}, \hat{f}, X, Y)$ $(\mathbf{x}_1,\mathbf{y}_1)$ $(\mathbf{x}_t, \mathbf{y}_t)$ P_t automobil airplane airplane automobile bird froa horse Data stream $t \in \mathcal{T}$ t = 1• • • • • •

$$\mathbb{E}_{P_1}[Z_1] \le \epsilon$$

 $\mathbb{E}_{P_t}[Z_t] \leq \epsilon$



 $\mathbb{E}_{P_T}[Z_T] \leq \epsilon$

$$Z = \ell(\hat{\psi}, \hat{f}, X, Y)$$

$$(\mathbf{x}_1,\mathbf{y}_1)\sim P_1$$
 $(\mathbf{x}_t,\mathbf{y}_t)$

t = 1Data stre . . .

$$\mathbb{E}_{P_1}[Z_1] \le \epsilon \qquad \qquad \mathbb{E}_{P_t}[Z_t]$$

Goal: for the considered threshold $\hat{\psi}$, decide whether it controls the instantaneous risk by ideally sample access at each time step.

 $_{t})\sim P_{t}$

 $(\mathbf{x}_T, \mathbf{y}_T) \sim P_T$

eam $t\in\mathcal{T}$	• • •	t = T	
$] \leq \epsilon$		$\mathbb{E}_{P_T}[Z_T] \leq \epsilon$	
		- 1 -	





$$Z = \ell(\hat{\psi}, \hat{f}, X, Y)$$

$$(\mathbf{x}_1,\mathbf{y}_1)\sim P_1$$
 $(\mathbf{x}_t,\mathbf{y}_t)$

$$t=1$$
 ... Data stre

$$\mathbb{E}_{P_1}[Z_1] \le \epsilon \qquad \qquad \mathbb{E}_{P_t}[Z_t]$$

Approach: deploy a risk tracker $M_t(\psi)$ to monitor risk violations.

 $_t)\sim P_t$

 $(\mathbf{x}_T, \mathbf{y}_T) \sim P_T$

eam $t \in \mathcal{T}$	•••	t=T	
$] \leq \epsilon$		$\mathbb{E}_{P_T}[Z_T] \leq \epsilon$	



Properties of risk tracker: if the risk violations happen, the tracker should grow. If the tracker does grow, it should signal risk violations with high probability.

Approach: deploy a risk tracker $M_t(\psi)$ to monitor risk violations.



$$\begin{split} H_0(\psi) &: \mathbb{E}_{P_t}[Z_t | \mathcal{F}_{t-1}] \leq \epsilon \quad \forall t \in \mathcal{T} \\ H_1(\psi) &: \exists t \in \mathcal{T} \quad \mathbb{E}_{P_t}[Z_t | \mathcal{F}_{t-1}] > \epsilon \end{split}$$



$$\begin{split} H_0(\psi) &: \mathbb{E}_{P_t}[Z_t | \mathcal{F}_{t-1}] \leq \epsilon \quad \forall t \in \mathcal{T} \\ H_1(\psi) &: \exists t \in \mathcal{T} \quad \mathbb{E}_{P_t}[Z_t | \mathcal{F}_{t-1}] > \epsilon \end{split}$$

How to design a tracker $M_t(\psi)$?





How to design a tracker $M_t(\psi)$?





Data stream $t \in \mathcal{T}$ t = 1• • •

A sequential forecasting game.



Forecaster

π_{t} estimate of the risk at the next time step: *t*







t=1 Data	strea

A sequential forecasting game.



Forecaster

\mathcal{T}_{t} estimate of the risk at the next time step: *t*







t=1	•••	Data stream

Forecaster incurs e

A sequential forecasting game.



Forecaster

π_t estimate of the risk at the next time step: t

am
$$t \in \mathcal{T}$$
 \cdots $t = T$

rror:
$$\delta_t = z_t - \pi_t$$



Forecaster incurs error: $\delta_t = z_t - \pi_t$

the forecaster would incur diminishing errors.

A sequential forecasting game.



Forecaster

estimate of the risk at the next time step: *t* $\mathcal{I}_{\mathbf{f}}$

am
$$t \in \mathcal{T}$$
 \cdots $t = T$

If the forecaster is playing their best move: $\pi_t = \mathbb{E}_{P_t}[Z_t | \mathcal{F}_{t-1}]$, then

V



Forecaster incurs error: $\delta_t = z_t - \pi_t$

the forecaster won't incur error, as $\mathbb{E}_{P_t}[Z_t - \pi_t | \mathscr{F}_{t-1}] = 0.$

A sequential forecasting game.



Forecaster

estimate of the risk at the next time step: *t* $\mathcal{I}_{\mathbf{f}}$

am
$$t \in \mathcal{T}$$
 ... $t = T$

If the forecaster is playing their best move: $\pi_t = \mathbb{E}_{P_t}[Z_t | \mathcal{F}_{t-1}]$, then

A sequential forecasting game.

Forecaster incurs error: $\delta_t = z_t - \pi_t$

$$t=1$$
 ... Data stream $t\in \mathcal{T}$... $t=T$





Forecaster

estimate of the risk at the next time step: *t* \mathcal{I}_{+}

The error process $(\delta_t)_{t \in \mathcal{T}}$ can be used to construct the tracker.

V

$$M_t(\psi) = \prod_{i=1}^t (1 + \lambda_i \cdot \delta_i) = \prod_{i=1}^t (1 + \lambda_i(z_i - \epsilon))$$

If the risk is controlled, then the tracker will not grow.

$\mathbb{E}[M_t(\psi) | \mathcal{F}_{t-1}] = M_t$

$$_{t-1} \cdot \mathbb{E}_{P_t}[\lambda_t(z_t - \epsilon) | \mathcal{F}_{t-1}]$$

$$M_t(\psi) = \prod_{i=1}^t (1 + \lambda_i \cdot \delta_i) = \prod_{i=1}^t (1 + \lambda_i(z_i - \epsilon))$$

If the risk is controlled, then the tracker will not grow.

$\mathbb{E}[M_t(\psi) | \mathcal{F}_{t-1}] = M_t$

Test supermartingale

$$t_{t-1} \cdot \mathbb{E}_{P_t}[\lambda_t(z_t - \epsilon) | \mathcal{F}_{t-1}]$$

Submitted to Statistical Science

Game-Theoretic Statistics and Safe Anytime-Valid Inference

Aaditya Ramdas, Peter Grünwald, Vladimir Vovk and Glenn Shafer

Abstract. Safe anytime-valid inference (SAVI) provides measures of statistical evidence and certainty—e-processes for testing and confidence sequences for estimation—that remain valid at all stopping times, accommodating con-

Testing by betting:

$M_t(\psi)$ is the wealth process of an agent actively betting against the null.

Submitted to Statistical Science

Game-Theoretic Statistics and Safe Anytime-Valid Inference

Aaditya Ramdas, Peter Grünwald, Vladimir Vovk and Glenn Shafer

Abstract. Safe anytime-valid inference (SAVI) provides measures of statistical evidence and certainty—e-processes for testing and confidence sequences for estimation—that remain valid at all stopping times, accommodating continuous monitoring and analysis of accumulating data and optional stopping or continuation for any reason. These measures crucially rely on test martin-



Properties of risk tracker: if the risk violations happen, the tracker should grow. If the tracker does grow, it should signal risk violations with high probability.

Approach: deploy a risk tracker $M_t(\psi)$ to monitor risk violations.



Lemma 4.2 (False alarm guarantee). For any $\psi \in \Psi$ such that $\mathbb{E}_{P_t}[z_t \mid \mathcal{F}_{t-1}] \leq \epsilon \ \forall t \in \mathcal{T}$ satisfies the null, it holds that $\mathbb{P}(\exists t \in \mathcal{T} : M_t(\psi) \geq 1/\delta) \leq \delta$.

If the tracker does grow, it should signal risk violations with high probability.

 $\lambda_t = \arg \max_{\lambda \in [0, 1/\epsilon)} \mathbb{E}_{H_1}[\log M_t(\psi)].$

If the risk violations happen, the tracker should grow.

On Continuous Monitoring of Risk Violations under Unknown Shift

Definition 4.4 (Growth rate optimality (GRO)). The betting rate λ_t is growth rate optimal if it satisfies the condition

Empirical demonstration



have B = 1, S = 50 and $t_{out} = 200$, with results evaluated over R = 50 trials (mean and std. deviation).

Figure 2: Results for outlier detection with a stepwise shift (§ 6.1). From left to right: Visuals of the growing risk and wealth process behaviour with respective rejection thresholds ϵ and $1/\delta$, for a single threshold candidate (here $\psi = 0.50$); the behaviour of the valid threshold set ψ -CS (Eq. 5), which eventually shrinks to zero signalling a model update; and the empirical distributions of detection delays $\tau(\psi) - \tau_*(\psi)$ across all $\psi \in \Psi$, including the false alarm region (FP). We also

Empirical demonstration



Figure 3: Results for set prediction with a temporal shift on FMoW (§ 6.2). From left to right: Visuals of the growing risk and wealth process behaviour with respective rejection thresholds ϵ and $1/\delta$, for a single threshold candidate (here $\psi = 0.08$); the behaviour of the valid threshold set ψ -CS (Eq. 5), which eventually tends to zero signalling a model update; and the empirical distributions of detection delays $\tau(\psi) - \tau_*(\psi)$ across all $\psi \in \Psi$, including the false alarm region (FP). We also have B = 1 and S = 365 (one year), with results evaluated over R = 50 trials (mean and std. deviation).

More results in the paper:

Confidence sets, asymptotic consistency and detection delay bound, betting strategie



Questions?