Research Statement

Manuel Gomez Rodriguez

January 10, 2024

My main research interest lies in the development of human-centric machine learning, a rapidly growing field of research that seeks to maximize the societal benefits of machine learning systems and minimize their potential harms, risks and burdens.

During the last years, my main focus has been on developing human-centric machine learning models and algorithms for evaluating, supporting and enhancing decision making processes where algorithmic and human decisions feed and influence each other. To this end, my research has introduced conceptual innovations and technical breakthroughs along three different dimensions:

1. Probabilistic, causal, and game-theoretic models of decision making in specific contexts.
2. Algorithms that leverage these models to enhance decision making with provable guarantees.
3. Observational and interventional studies to evaluate such models and algorithms in practice.

Moreover, these conceptual innovations and technical breakthroughs have often uncovered previously unexplored connections between fields, as exemplified by several of my current achievements and my vision for the future.

Current Achievements

My research contributions to human-centric machine learning can be categorized in several distinctive research themes. Since each of these themes entails their own technical challenges and application domains, in what follows, I discuss each of them separately.

Human-AI Teaming. In recent years, there has been an increasing interest in developing machine learning systems especially designed to team up with human experts in a wide range of critical domains, from medicine and drug discovery to candidate screening and criminal justice. The main promise is that, by working together, human experts and machine learning systems will achieve a considerably better performance than each of them would achieve on their own. In the last years, together with students and postdocs in my group at MPI-SWS, we have pursued two lines of research to fulfill this promise on prediction tasks.

In a first line of research, we have pursued the idea of algorithmic triage. Under algorithmic triage, a machine learning model does not predict all instances but instead defers some of the instances to human experts. As a result, one does not only have to find a machine learning model but also a triage policy which determines who predicts each instance. Here, one of the main challenges is that, for each potential triage policy, there is an optimal machine learning model, however, the triage policy is also something one seeks to optimize. In a sequence of papers, we have developed some of the first algorithms with theoretical guarantees to learn under algorithmic triage in regression [1], classification [2, 3] and reinforcement learning [4] settings. In these pieces
of work, we have conducted observational experiments showing that, by using algorithmic triage, human experts and machine learning models consistently achieve better average performance than each of them would achieve on their own.

In a second line of research, we have pursued the design of machine learning models that adaptively limit experts’ level of agency \[5, 6\]. We have advocated for machine learning models which, rather than providing single predictions, provide sets of predictions, namely prediction sets, and forcefully ask human experts to predict label values from these prediction sets.\[1\] The key rationale here is that, by using the theory of conformal prediction \[7, 8\] to construct the above prediction sets, we can precisely trade-off the probability that the ground truth label is not in the prediction set, which determines how frequently the systems will mislead human experts, and the size of the prediction set, which determines the difficulty of the prediction task the experts need to solve using the system. Further, we have developed several bandit algorithms that leverage the nested structure of the prediction sets provided by any conformal predictor and a natural counterfactual monotonicity assumption on the experts’ predictions to find the conformal predictor under which experts would benefit the most from using such system very efficiently. Finally, we have conducted a large-scale human subject study that suggest that machine learning models that adaptively limit experts’ level of agency may offer greater performance than those allowing experts to always exercise their own agency.

**Fairness in Machine Learning.** As algorithmic decisions become more consequential to individuals and society, there have been increasing concerns about the potential for unfairness of algorithmic decision making. These concerns have been supported by a number of empirical studies, which have provided, e.g., evidence of racial discrimination in criminal justice \[9\], health \[10\] or advertisement \[11\]. As a result, there has been a growing interest in the field of fairness in machine learning, which aims to develop machine learning models whose outcomes do not have a disproportionately large adverse impact on particular groups of people sharing certain sensitive traits such a race or sex.

Together with students, postdocs and collaborators at MPI-SWS, we have been at the forefront of the field since its early days. In a sequence of papers, we were among the first to tackle the design of (margin-based) classifiers with fairness guarantees \[12–15\]. This work received immediate international recognition by means of a best paper award honorable mention at the 26th International World Wide Web Conference and, since then, it has stimulated a very large amount of follow-up work (\(~3,000\) citations). In addition, Bilal Zafar—the PhD student who led these sequence of papers—won an Otto Hahn Medal from the Max Planck Society for outstanding scientific achievements in their doctoral thesis research.

More recently, together with students, postdocs and collaborators at MPI-SWS and MPI-IS, we have focused on settings in which there is a feedback loop between algorithmic and human decisions, which influence the data generation and collection process. In one piece of work \[16\], we have focused on learning accurate predictive models in scenarios where labels only exist conditional on certain decisions—if a loan is denied, there is not even an option for the individual to pay back the loan. We have shown that, in this selective labels setting, learning a predictor directly only from available labeled data is suboptimal in terms of both fairness and utility. To avoid this undesirable behavior, we have proposed to directly learn decision policies that maximize utility under fairness constraints

---

\[1\] There are many systems used everyday by experts that, under normal operation, limit experts’ level of agency. For example, think of a pilot who is flying a plane. There are automated, adaptive systems that prevent the pilot from taking certain actions based on the monitoring of the environment.
and thereby take into account how decisions affect which data is observed in the future. In another piece of work [17], we have focused on designing ranking models that understand the long-term consequences of their proposed rankings and, more importantly, are able to avoid the undesirable ones. More specifically, we introduced a joint representation of rankings and user dynamics using Markov decision processes and, building upon this representation, introduced an efficient gradient-based algorithm to learn parameterized ranking models that trade off the immediate utility and the long-term welfare.

Finally, in a very recent piece of work, together with a student in my group at MPI-SWS [18], we have focused on selection processes in which an often intractable number of candidates is reduced to a shortlist of the most promising candidates using a screening classifier. We have shown that, even if a screening classifier is well-calibrated calibrated [19, 20], any threshold decision rule that uses such classifier may be biased against qualified candidates within demographic groups of interest. More specifically, it may shortlist one or more candidates from a group who are less likely to be qualified than one or more rejected candidates from the same group. As a consequence, it may perpetuate historical biases against minority groups by precluding the best candidates within these groups—the candidates who are more likely to be qualified—to be shortlisted. Then, we have introduced an efficient post-processing algorithm to minimally modify any given calibrated classifier so that it does not suffer from this type of within-group unfairness.

**Strategic Machine Learning.** As decision making is increasingly informed by data-driven predictive models, there is an increasing pressure on the decision makers to be transparent about the decision policies, the predictive models, and the features they use. However, individuals may be incentivized to use this knowledge to invest effort strategically in order to receive a beneficial decision. For example, in loan decisions, if a bank discloses that it will use credit card debt to decide whether it offers a loan to a customer, she may feel compelled to avoid credit card debt overall. Motivated by this observation, there has been a flurry of work in the emerging field of strategic machine learning in very recent years and, together with students, postdocs and collaborators at MPI-SWS, we have carried out some of the early work.

In a first piece of work [21], we were among the first to address the problem of finding decision policies that incentivize individuals to invest in forms of effort that increase the utility of the policy. This was in contrast with most, if not all, of the contemporary work, which had focused on the design of accurate machine learning models in the above mentioned strategic setting. One of our key ideas was the realization that individuals’ investment of effort induces a change in their features and, under some technical assumptions, this change can be characterized analytically at a population level. Building upon this characterization, we have studied the hardness of the problem and identified a natural monotonicity assumption on the cost individuals pay to change features that allows for a highly effective polynomial time heuristic search algorithm to find optimal policies.

In a second piece of work [22], we have uncovered a previously unexplored connection between strategic machine learning and counterfactual explanations. In short, counterfactual explanations aim to help individuals subject to decisions informed by machine learning models understand what would have to change for these decisions to be beneficial ones. In this work, we have investigated how individuals may use the knowledge gained by counterfactual explanations to invest effort strategically and maximize their chances of receiving a beneficial decision. More specifically, we have developed several polynomial-time algorithms with approximation guarantees to find near-optimal policies and counterfactual explanations in such a strategic setting. Moreover, we have also shown that, by incorporating a matroid constraint into the problem formulation, one can increase the
diversity of the near-optimal set of counterfactual explanations and incentivize individuals across
the whole spectrum of the population to self improve.

**Machine Learning for Counterfactual Reasoning.** There is empirical evidence that humans
improve their decision making skills by means of counterfactual reasoning—reasoning about what
might have been had they made alternative decisions to those they actually took [23–24]. However,
in sequential decision making processes where multiple, dependent decisions are made sequentially
over time, the number of alternatives a human may need to reason about can be intractably large,
particularly if there is uncertainty on the dynamics of the environment. In the last years, together
with students and postdocs in my group at MPI-SWS, we have initiated the development of machine
learning models and algorithms to help humans conduct counterfactual reasoning in such settings.

In a first line of work, we have focused on Markov decision processes and developed algorithms
to identify optimal sequences of alternative decisions that, in comparison with the factual decisions,
would have counterfactually led to better outcomes. In a first piece of work [25], we have focused on
discrete state spaces and developed an algorithm based on dynamic programming that is guaranteed
to solve the problem in polynomial time. In a second piece of work [26], we have shown that, in
continuous state spaces, we cannot generally expect to solve the problem in polynomial time.
However, under a natural form of Lipschitz continuity of the environment’s dynamics, we have
developed a practical $A^*$ algorithm that is guaranteed to return the optimal solution to the problem.
In both pieces of work, using real data from the medical domain, we have shown that the alternative
sequences found by these algorithms can provide valuable insights to enhance sequential decision
making.

In a second line of work, we have focused on temporal point processes, a popular type of processes
for modeling discrete event data in continuous time, and developed a first-of-a-kind temporal point
process model that, in contrast with existing models, can be used to answer counterfactual questions
about these type of processes [27]. For example, in epidemiology, assume that, during a pandemic,
a government decides to implement business restrictions every time the weekly incidence—the
(relative) number of new cases—is larger than certain threshold but unfortunately the incidence
nevertheless spirals out of control. Our model could help the government understand retroactively
to what extent the incidence would have grown had a lower threshold been implemented.

**Other achievements.** Around the time I received tenure at MPI-SWS, the COVID-19 pandemic
started and I quickly branched out from my current focus at that time and, together with students,
postdocs and collaborators from multiple MPIs, EPFL and ETH, we worked on several projects
related to COVID-19 at a furious pace. We have developed an epidemiological model based on
temporal point processes that can be used to predict the spread of epidemics at an unprecedented
spatiotemporal resolution [28], a privacy-preserving and inclusive system for epidemic risk assess-
ment and notification [29], and a group testing method based on dynamic programming that is
specifically designed to use the information provided by contact tracing [30].

**Previous Achievements**

During my PhD and my postdoctoral work, my research focused on understanding, predicting
and controlling information diffusion over the Web and social media. This led to a series of pa-
pers [31–43], which significantly advanced the state of the art in the network inference and influence
maximization problems. Two of these papers [32, 37] received immediate international recognition
by means of a best paper award honorable mention at KDD, the flagship conference in data min-
ing, and an outstanding best paper award at NeurIPS, the flagship conference in machine learning. Since then, these series of papers have stimulated a large amount of follow-up work (>3,000 citations) and have been the methodological basis for two journal papers on malaria in collaboration with epidemiologists at Imperial College and others [44, 45].

After I joined MPI-SWS as a tenure-track faculty, I realized that my doctoral and postdoctoral work on network inference and influence maximization leveraged particular instances of a more general and powerful type of random processes, marked temporal point processes, which could be potentially used to design a new generation of models and algorithms to predict and optimize the functioning of social, information and networked systems. In the years that followed, I leveraged this realization to lead the design of:

(i) probabilistic models based on marked temporal point process to predict information propagation [46–48], product competition [49], opinion dynamics [50], information reliability [51–53], knowledge content [54], and spatiotemporal processes [55, 56]. In all cases, by exploiting fine grained user data, the models provide more accurate predictions than the state of the art.

(ii) a series of efficient off-line and online algorithms with provable guarantees to steer information dissemination [57–63], detect and precent the spread of misinformation [64, 65], and design spaced repetition algorithms for efficient memorization [66–68]. These algorithms exploit an alternative representation of marked temporal point processes using SDEs with jumps and establish a previously unexplored connection between optimal control of SDEs with jumps and marked temporal point processes.

At the beginning of 2020, my work on marked temporal point processes made my case for tenure at MPI-SWS. However, around the same time, I started to shift focus spearheaded by an ERC Starting Grant on “Human-Centric Machine Learning”.

**Vision for the Future**

Had the physician initiated the antibiotic treatment for sepsis a day earlier, the patient would have recovered. Had they taken an earlier train to the airport, they would not have missed their flight. Had I clicked on the attachment of that strange email, my computer would have been hacked. These are examples of counterfactual reasoning, a type of reasoning that is epitomized by the phrase “what might have been,” which implicates a juxtaposition of an imagined versus factual reality [23, 69].

Counterfactual reasoning is tightly connected to the way we attribute causality and responsibility [70], and it has been shown to play a significant role in the ability that humans have to learn from limited past experience [24] and improve their decision making skills [71]. Is counterfactual reasoning a human capacity that machines cannot have? Surprisingly, recent advances at the interface of causality and machine learning have demonstrated that it is possible to build machines that perform and benefit from counterfactual reasoning, in a way similarly as humans do [72, 73]. However, these advances have predominantly comprised machine learning systems designed to operate autonomously, without human supervision. In the incoming years, my goal is to develop human-centric machine learning models and algorithms for automated decision support that are able to perform and benefit from counterfactual reasoning. In pursuit of its goal, together with students and collaborators, we will introduce several fundamental innovations and technical breakthroughs, which I discuss next.
**Human-AI Complementarity.** In a decision making process, whenever a machine learning model is used to predict the value of an outcome of interest, it has been widely agreed that the model should also provide a confidence score along with each prediction \[19, 74\]. Then, the decision maker is supposed to use the confidence score to calibrate how much to trust the prediction. However, multiple lines of empirical evidence have recently shown that decision makers have difficulties at developing a good sense on when to trust a prediction using confidence scores, based on the way they are computed today \[75, 76\]. As an immediate consequence, it is not yet clear how to ensure that, after receiving automated decision support from a machine learning model, the average quality of the decisions made by decision makers does not worsen. In my research, we will use counterfactual reasoning to first understand why and then design automated decision support systems that can only increase and never decrease the average quality of human decisions. Our starting point will be our recent work on human-aligned calibration \[77\], where we have shown that, on settings with binary decisions and outcomes, a (rational) decision maker can only make optimal decisions if the confidence scores satisfy a natural counterfactual monotonicity property.

**Computational and Data Requirements.** Using counterfactual reasoning, we will reduce the computational and data requirements of machine learning models underpinning automated decision support systems. To this end, we will view each machine learning model as a different (causal) intervention in the decision making process. Under this view, given decision making data gathered under one intervention, we will use the structural similarity and shared properties between this intervention and other alternative interventions to generate counterfactual decision making data. Finally, we will leverage this counterfactual decision making data to find the optimal machine learning model much more efficiently. Our starting point will be our on-going work on counterfactual prediction sets \[6\], where we have demonstrated that, for automated decision support systems based on conformal prediction, it is possible to achieve an exponential gain in terms of computational and data efficiency by leveraging counterfactual decision making data.

**Algorithmic Harm.** The concept of harm is a central tenet of ethical principles, codes and laws. For example, the bioethical principle “first, do no harm” \[78\], asserts that a doctor’s moral responsibility to benefit patients is superseded by their responsibility not to harm them \[79\]. In this context, we do not find any reason to make an exception with automated decision support systems based on machine learning systems. Motivated by this observation, we will develop mechanisms to measure and control how much harm an automated decision support system based on a machine learning model may cause. Building upon the counterfactual comparative account of harm from the field of philosophy \[80\], we will say that an automated decision support system is harmful on a specific decision making instance if and only if the decision maker would have made a better decision on their own. Here, we will focus on automated decision support systems for multiclass classification tasks \[5, 81\] and matching tasks \[82, 83\].

To showcase and evaluate the above machine learning models and algorithms, we will go beyond the status quo, which relies only on observational experiments for evaluation, and conduct human subject studies with laypersons using Prolific, an online research platform that facilitates the recruitment and management of human participants. By doing so, we will demonstrate that counterfactual reasoning can bring practical benefits to machine learning for decision support.
References


