Designing the User Experience of Machine Learning Systems

Dr. Boris Adryan
Zühlke Engineering GmbH, Germany
badryan@gmail.com, @BorisAdryan

Proposal for a **presentation** at the AAAI Spring Symposium Series.

Computers don't have a notion of the world around them. Nevertheless, the current generation of personal devices already attempts to hide that fact by providing context-specific information and recommendations that are based on some interpretation of previous input (e.g. search terms) and behaviour (e.g. commute patterns). At this stage, most users don't expect websites, mobile phones or tablets to give useful predictive insight. True-positive predictions ('*I see you're arriving at the cinema - would you like to see a list of movies?*') are often met with positive surprise, false-positive predictions ('*Customers who bought this book about contraception als wanted to know about diapers*') provoke laughter. We usually expect to be disappointed and recommender systems to be broken - it's the reality of machine learning UX.

With the anticipated billions of devices to make up the Internet of Things, it becomes clear that information overload is imminent. We cannot longer digest the vast amount of raw data coming off these devices; i.e. from a practical as well as a UX perspective we have to get away from looking at raw output on dashboards (the proverbial 'app for each device') to intelligent systems that can deal with this data in real-time and provide users with agglomerated context-specific information and relevant, actionable insight. Add speech: Rather than having a nagging voice remind us every minute of an impending energy crisis, we only want to interrupt a journey if it is clear that it cannot be completed without refuelling the car, and that there is a reasonably opportunity to do so nearby. A well-trained machine learning method could be used to infer such 'knowledge' from a set of arbitrary data, based on statistical considerations and properties of previously learned data.

A machine learning method builds a classifier that categorises combinations of incoming data (e.g. amount of gas, distance to target, distance to next gas station, etc) as belonging to groups ('*this is a good opportunity for refuelling*' or '*this is* not *a good moment to annoy the driver*'). Conceptually we can use the classifier at any time, but the initial state of any machine learning system is that of ignorance, i.e. it is unclear whether or not a a prediction is true. While 'on-the-fly' learning exists, ultimately all machine learning is iterative and requires regular feedback to clarify to the computer whether a given set of data really belongs to one or another group: this is the training phase that makes the classifier useful, and more training and more feedback means better classifiers.

In academic machine learning method development, as well as in applications of machine learning in the industrial R&D context, training is a widely accepted, necessary evil. Things become tricky when machine learning and the uninitiated consumer come together. When a user without knowledge of the underlying process is confronted with repeated confirmation requests ('*Do you agree this is a good moment to stop?*'), the training phase can become a UX nightmare that in the worst case makes the user avoid the system at all, before it ever can become any good. We are already seeing websites and apps that use iterative training. Some take the confirmation strategy, but don't communicate why they're doing it.

Others present even objectively bad predictions but allow the user to mark and discard these. Is voice control in respect to providing feedback to machine learning systems more or less intrusive? It seems that systematic A/B testing is required, as some communities (e.g. home automation geeks vs professional drivers) may be more appealed by one or the other strategy.

While providing a metric for the certainty of the reliability of a prediction is a must for engineers, confronting consumers with p-values, false discovery rates or area-under-the-curve is a clear no. What is the best strategy to go about it? People of a certain age will remember how any weather forecast longer than a day was just a random guess, and accepted the very fact. Nowadays, some weather websites feature a reliability score. If an arbitrary 34% reliability provide more 'actionable insight' than the sheer acceptance that predictions are random is unclear.

Can we avoid all this trouble by creating vast training facilities for machine learning algorithms in connected products? Likely not. Good machine learning requires lots of training data. Power comes with large numbers. However, most predictions for the Internet of Things are going to be based on the integration of data across different devices. As everyone might have a different combination of devices that should be taken into consideration, and everyone might have a different scope for using the Internet of Things (the '*What does our user want?*' -- think security, fitness, efficiency), providers of machine learning solutions cannot train their methods without the users themselves. We may want to think about large-scale simulations that draw bootstrapped ensembles of virtual devices and try to infer 'this particular user's need', but ultimately this will only lower the number of classes we're trying to predict – if our features and classification itself are correct, that's still subject to some sort of (human?) supervision.

Coming from the perspective of a machine learning method developer and having experienced bad UX around self-learning devices myself, I cannot provide solutions to the discourse but act as an interpreter between the fields.

Bio: Trained as molecular biologist in the late 1990s, Dr. Boris Adryan pursued studies on the 'systems biology' of embryonic development, a field that aims to model mathematically the processes and emerging properties of cells and tissues in developing animals. Shifting more and more towards computational methods and simulation, his research group at the University of Cambridge was on the forefront of machine learning method development for genome research from 2008 to 2015. His geek interests ultimately led Dr. Adryan to applications of such methods in the Internet of Things. From 2013 he was commercially active with his company thingslearn Ltd., offering expertise and hands-on support to start-up companies in the London IoT scene. As conference speaker he suggested solutions to modelling device relationships with ontologies or how machine learning and voice interactions are going to bring about a real creepy future. In 2016 Dr. Adryan returned to Germany to join Zühlke Engineering as Principal Consultant for IoT and data analytics.

Motivation: I've always been a wanderer between the worlds. My initial training was in biology, most of my work for the past two decades mathematics and computer science. I once tried and failed to get into interaction design school, mostly because the 'undo' button had not been invented yet and I make pencils break. UX and UI are my passion, although professionally in my past roles they were the least concern. However, I believe they are crucial for the success of IoT in the consumer world, and as a specialist in the field I'm completely aware that machine learning training phases are vastly incompatible with what we perceive as good UX. That's why I started talking about it at tech conferences, and I hope to meet like-minded people at your event from whom I can learn.