“FOUNDATIONS OF MACHINE LEARNING SYSTEMS”

- It is the title of my chair… chosen to summarise my (planned) work
- So a good title for a talk!
- I cover one aspect of what I am interested in (the mathematical side)
- I aim to convey *flavour* of work; perhaps a bit different to much ML research

Details are in a few papers I refer to at the end
JOINT WORK WITH TWO PHD STUDENTS

Christian Fröhlich

Rabanus Derr
I think nobody should be certain of anything.
"an element of a structure which connects it to the ground" – Wikipedia

Abstracting just slightly:
An Interface to the World

And what happens if your interface does not respect the properties of the world?
FOUNDATIONS OF MACHINE LEARNING SYSTEMS

- Study the interface of ML systems to the world
- Pay attention to what we assume about the world
- Like other areas of engineering, learn from failures
  - Particular focus: failure of usual models of data

Need to pay attention to the data itself ...

Sabina Leonelli’s remarkable “data journeys”

(Aside: watch her nice talk https://www.youtube.com/watch?v=XYNV1EuNVXk)
MACHINE LEARNING SYSTEMS
\[
\min_{h \in \mathcal{H}} \mathbb{E}(\mathcal{L}_h)
\]

\[\mathcal{L}_h := \ell(\mathcal{X}, h(\mathcal{Z}))\]
PROTOTYPE ML PROBLEM: MINIMISE EXPECTED RISK

The world gives us random variables $X, Y$ with some fixed joint distribution $P_{XY}$

Actually it gives us samples “drawn i.i.d.” from $P_{XY}$

The loss function $\ell$ is given to us (by someone else?)

Goal: minimise (over $h$) the expected value of the indexed family of random variables

\[
R_h(\omega) := \ell(Y(\omega), h(X(\omega)))
\]
LOWER ONE’S SIGHTS, AND FIX A MODEL CLASS \( \mathcal{H} \)

\[
\arg\min_{h \in \mathcal{H}} \mathbb{E} \mathcal{L}(Y, h(X))
\]

\[
\arg\min_{h \in \mathcal{H}} \frac{1}{n} \sum_{i=1}^{n} \mathcal{L}(Y_i, h(X_i))
\]
arg min_{h \in \mathcal{H}} \frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, h(X_i)) Z_i
WHAT TO STUDY?

- **the model class** — the focus of much ML research
- **algorithms** to optimise — the focus of most of the remainder
- **the hypothesis** — focus of “explainability”
- **the loss function**, how performance is judged; see next slide
- **expectation** to aggregate individual losses / encode fairness
- **the set system** (usually a $\sigma$-algebra) — the set of measurable events
- **our real model of the world** — $(X_i, Y_i)$ as iid “samples from a distribution”

$$
\arg \min_{h \in \mathcal{H}} \mathbb{E} \ell(Y, h(X))
$$

$\mathbb{E}$ implies an underlying probability space $(\Omega, \mathcal{S}, \mu)$

$$
\frac{1}{n} \sum_{i=1}^{n} \ell(Y_i, h(X_i))
$$
LOSS FUNCTIONS AND INFORMATION

- **Loss functions:**
  - Traditionally $\ell(y, \hat{p})$; reframe as $\ell: \Delta^n \to \mathbb{R}^n$
  - Parametrise via a convex set $S = \text{spr}(\ell) \subset \mathbb{R}^n$ as $\ell = \partial\sigma_S$, subgradient of support function of $S$
  - Provides new insights and notions; e.g. “inverse loss” $\ell^\circ = \sigma_S$; have $\ell \circ \ell^\circ \circ \ell = \ell$

- **Information:**
  - Not just Shannon; many information measures satisfy an “information processing inequality”
  - Not just binary $I(P\|Q)$, but a general experiment $E: [n] \to \Delta(\mathcal{X})$ (think multi-class class probability estimation)
  - Parametrise information by a convex set $D \subset \mathbb{R}^n$ or $\mathcal{F} \subset (\mathbb{R}^n)^\mathcal{X}$; $I_D(E)$ and $I_\mathcal{F}(E)$; averages of support functions
  - **Bridge:** BayesRisk$_\ell(E, \pi) = -I_{-\pi \cdot \text{spr}(\ell)}(E)$; BayesRisk$_{\ell, \mathcal{H}}(E, \pi) = -I_{-\pi \cdot \mathcal{H}}(E)$
    - Information depends upon the use to which it will be put
  - **Information Processing Equality:** $I_D(RE) = I_{RD}(E)$ and $I_\mathcal{F}(ET) = I_{T\mathcal{F}}(E)$
    - Information is not so much lost, as transformed

  If studying $\ell$ provides such insight, then what if we make a similar effort to study $E$? Will convex sets prevail again?

\[
\arg\min_{h \in \mathcal{H}} \mathbb{E} \ell(Y, h(X))
\]
BEYOND EXPECTATIONS
WHEN $X$, $Y$ REPRESENT PEOPLE

$$\arg\min_{h \in \mathcal{H}} \mathbb{E} \ell(Y, h(X))$$

- We are increasingly asked to be able to explain or justify the results of a ML based decision.
- Much effort given to justifying $\mathcal{H}$ or $\arg\min$
- But justification of $\mathbb{E}$ is also called for!
- Probability theory was developed as a response to (very artificial) “games of chance”.
- It works well there. But why believe the world is a casino?
- Confer the over-emphasis of games in AI research (Go)
MANY PATHS TO ONE DESTINATION

1. Axiomatic approach to risk measures
2. Demanding fairness (f. risk measures)
3. Uncertainty + Ambiguity (economics)
4. Robust Bayes (imprecise prior)
5. Rearrangement invariant norms
6. de Finetti with a bid-ask spread
7. Set systems for probability ($\Omega, \mathcal{S}, \mu$)
8. Generalised frequentism (von Mises)

The remainder of the talk:
- Relations between 1, 5 and 6, and how to stratify the choices ($\mathcal{P}$)
- How generalising $\mathcal{S}$ rather than $\mu$ leads to similar destination (7)
- Can also reach the same destination by starting with the data, but not assuming probabilities (8)

The nett result: multiple compelling reasons to go “beyond expectations”

$R(X) = \sup_{P \in \mathcal{P}} \mathbb{E}_P(X)$
RISK MEASURES AND COHERENT UPPER PROBABILITIES
IMPRECISE PROBABILITY

- \( \omega \in \Omega \) represents a state of the world
- A gamble is a bounded function \( X : \Omega \to \mathbb{R} \) yielding an uncertain loss \( X(\omega) \) when the state \( \omega \) is realised
- Gambles form a vector space \( \mathcal{L} \)
- Posit 4 axioms for the set \( \mathcal{D} \) of desirable gambles:
  1. \( \sup X < 0 \Rightarrow X \in \mathcal{D} \)
  2. \( \inf X > 0 \Rightarrow X \notin \mathcal{D} \)
  3. \( X \in \mathcal{D}, \lambda \in \mathbb{R}_{>0} \Rightarrow \lambda X \in \mathcal{D} \)
  4. \( X \in \mathcal{D}, Y \in \mathcal{D} \Rightarrow X + Y \in \mathcal{D} \)
- The set \( \mathcal{D} \) satisfying 1–4 above is a coherent set of desirable gambles (aka acceptance set)
The upper prevision of $X$ is $\bar{P}(X) := \inf\{\alpha \in \mathbb{R} : X - \alpha \in \mathcal{D}\}$ – the smallest amount of certain loss $\alpha$ that, when subtracted from the uncertain loss $X$, makes the resulting gamble desirable (i.e. the certainty equivalent).

Symmetrically, the lower prevision $\underline{P}(X) = -\bar{P}(-X) = \sup\{\alpha \in \mathbb{R} : \alpha - X \in \mathcal{D}\}$ – the largest certain loss $\alpha$ which we are willing to shoulder in exchange for giving away an uncertain $X$.

If $\bar{P}$ is defined as above on an $X \in \mathcal{D}$ then it satisfies

1. $\bar{P}(X) \leq \sup X$
2. $\bar{P}(\lambda X) = \lambda \bar{P}(X)$
3. $\bar{P}(X + Y) \leq \bar{P}(X) + \bar{P}(Y)$

and is said to be a coherent upper prevision.
Known that any upper prevision which avoids sure loss dominates at least one linear prevision (point wise). 

Thus \( \mathcal{Q} := \{ Q : Q(X) \leq \bar{P}(X) \; \forall X \in \mathcal{L}, \; Q \text{ linear} \} \) is non-empty.

Can construct a canonical coherent extension of \( \bar{P} \) via 

\[
\bar{E} = \sup_{Q \in \mathcal{Q}} Q(X)
\]

known as the natural extension of \( \bar{P} \).

Upper probabilities arise by taking a prevision of an indicator gamble:

\( \bar{P}(A) := \bar{P}(\chi_A) \) and lower probabilities similarly:

\( \underline{P}(A) := 1 - \bar{P}(\chi_{\Omega \setminus A}) \)
COHERENT RISK MEASURES

- Yes, the same word used by different communities...
  - Who doesn’t want to be coherent?

- Treat $X(\omega)$ and $Y(\omega)$ as a random variables on some probability space $(\Omega, \mathcal{S}, \mu)$
  - $R(\lambda X) = \lambda R(X), \forall \lambda \in \mathbb{R}^+$ (positive homogeneity)
  - $R(X + Y) \leq R(X) + R(Y)$ (subadditivity)
  - $R(X + c) = R(X) + c, \forall c \in \mathbb{R}$ (translation equivariance)
  - $X(\omega) \leq Y(\omega) \forall \omega \Rightarrow R(X) \leq R(Y)$ (monotonicity)
In standard probability theory, there is a 1:1 correspondence between probabilities and expectations via Lebesgue integration.

However with imprecise probability there are many coherent upper previsions associated with a coherent upper probability.

Hence Walley focussed upon coherent upper previsions.

Pelessoni and Vicig (2003):

Let $\mathcal{L}$ be a linear space of bounded real-valued random variables, containing all constant functions.

A functional $R$ is a coherent risk measure on $\mathcal{L}$ if and only if it is a coherent upper prevision on $\mathcal{L}$.
Walley does not start with a measure space but just a set of possibilities $\Omega$; one can instead start with a probability space.

Then one can introduce the notion of law invariance — $R(X)$ only depends upon $\text{Law}(X)$.

Spectral risk measures: Given a probability measure $\lambda$ on $[0,1]$, define

$$ R_\lambda(X) = \int_0^1 \text{CVaR}_\alpha(X) d\lambda(\alpha) $$

$$ \text{CVaR}_\alpha(X) := \mathbb{E}(X \mid X \geq q_\alpha(X)) $$

(Conditional value-at-risk)

Convenient to rewrite as $R_w(X) = \int_0^1 F_X^{-1}(q)w(q)dq$

Distortion risk measures: Given $\phi : [0,1] \rightarrow [0,1]$ which is monotonically increasing, concave and satisfies $\phi(0) = 0$ and $\phi(1) = 1$ the distortion risk measure is given by the Choquet integral

$$ R_\phi(X) = \int_{-\infty}^0 [\phi(S_X(x) - 1)]dx + \int_0^\infty \phi(S_X(x))dx, \text{ where } S_X(x) = 1 - F_X(x) = P(X > x) $$

Gzyl and Mayoral (2008): $R_W = R_\phi$ when $\phi'(t) = w(1 - t)$
CONNECTION TO UPPER PROBABILITIES

- Work on a measurable space \((\Omega, \mathcal{F})\).
- Given a distortion \(\phi\) define \(\overline{P}(A) = \phi(P(A))\).
- This forms a capacity — a set function \(\overline{\mu}: \mathcal{F} \rightarrow \mathbb{R}\) satisfying \(\overline{\mu}(\emptyset) = 0, \overline{\mu}(\Omega) = 1\) and \(A \subset B \Rightarrow \overline{\mu}(A) \leq \overline{\mu}(B)\).
- A submodular capacity also satisfies \(\overline{\mu}(A \cup B) + \overline{\mu}(A \cap B) \leq \overline{\mu}(A) + \overline{\mu}(B)\) for all \(A, B \in \mathcal{F}\).
- It turns out (see paper) that for submodular capacities, Walley’s natural extension corresponds with the Choquet integral.
- Thus spectral risk measures are natural extensions of coherent upper probabilities.
THE FUNDAMENTAL FUNCTION

- Rearrangement invariant function norms $R$: just think of functionals of random variables that only depend upon their distribution.

- For each measurable subset $E \subseteq \Omega$ with measure $\mu(E) = t$, we define the fundamental function $\phi_r : [0,1] \rightarrow \mathbb{R}^+$ as $\phi_r(t) = \|\chi_E\|_R = R(\chi_E)$, where $\chi_E$ is the indicator function of $E$.

- Fundamental functions are always "quasi-concave":
  - $\phi$ is non-decreasing and $\phi(0) = 0$
  - $t \mapsto \phi(t)/t$ is decreasing
  - $\phi$ is continuous except perhaps at the origin
  - Little is lost if one demands concavity (and increasingness and anchored at 0)

- e.g. CVaR$_\alpha$: $\phi_\alpha(t) := \frac{t}{1-\alpha} \wedge 1$ for $\alpha \in [0,1)$
THE LORENTZ AND MARCINKIEWICZ NORMS

- Given any concave fundamental function $\phi$, the Lorentz norm of $X$ is
  \[ \|X\|_{\Lambda_\phi} = X^*(0)\phi(0+) + \int_0^1 F_{|X|}^{-1}(1 - \omega)\phi'(\omega)d\omega, \]

- The Marcinkiewicz norm is
  \[ \|X\|_{M_\phi} = \sup_{0 < t \leq 1} \{ \phi(t)\text{CVaR}_{1-t}(\|X\|) \} \]

- Known result: For all concave fundamental functions $\phi$, all $X$, and all ri norms
  \[ \| \cdot \|_{\mathcal{R}} \text{ we have } \|X\|_{M_\phi} \leq \|X\|_{\mathcal{R}} \leq \|X\|_{\Lambda_\phi} \]
Recall $\|X\|_{M_\phi} \leq \|X\|_\mathcal{R} \leq \|X\|_{\Lambda_\phi}$

If additionally we have $\phi'(0) < \infty$ then $\|X\|_{\Lambda_\phi} \leq K \cdot \|X\|_{M_\phi}$ with $K = \frac{1}{\phi(1/\phi'(0))}$.

Thus when $\phi'(0) < \infty$, all ri norms are equivalent.

When $\phi'(0) = \infty$, $\|\cdot\|_{\Lambda_\phi}$ and $\|\cdot\|_{M_\phi}$ are not equivalent.
Recall the definition of the fundamental function: $\phi_\mathcal{R}(t) = \|\chi_{[0,t]}\|_\mathcal{R}$

This is the upper probability of the set $[0,t]$

Provides new insight to coherent upper probabilities
ETHICAL INTERPRETATION

- Ethical interpretation: interpret as how ethically bad for a fraction $t$ of the population to suffer loss 1.
  - $\mathbb{E}(X)$ corresponds to $\phi(t) = t$;
  - $\max X$ corresponds to $\phi(t) = \chi_{(0,1]}(t)$.
  - Harsanyi vs Rawls… (see Fairness Risk Measures for an elucidation)

- But there’s still a problem: if you choose $\phi_1$ and I choose $\phi_2$, how might we come to some agreement about a compromise $\phi$ somehow “in between” $\phi_1$ and $\phi_2$?
  Want $\| \cdot \|_{\text{compr}} = \mathcal{F}(\| \cdot \|_1, \| \cdot \|_2)$

- Turns out that suitable functors $\mathcal{F}$ also have “fundamental functions” $\psi_{\mathcal{F}}$ and $\phi_{\text{compr}} = \psi_{\mathcal{F}}(\phi_1, \phi_2)$, and $\{\psi_{\mathcal{F}}\} \cong \{\phi\}$

- The hard ethical choice remains – there is no cheap fix by going meta…
SYSTEM OF PRECISION
EVENTS \((\Omega, \mathcal{S}, \mu)\)

When posing problems in probability calculus, it should be required to indicate for which events the probabilities are assumed to exist

– Andrei Nikolaevich Kolmogorov 1927

Traditionally \(\mathcal{S}\) is taken to be a \(\sigma\)-algebra – a set system closed under complementation and arbitrary countable unions

This is rarely questioned (apart from the \(\sigma\))
It turns out that the “natural” set system to consider for precise events is a pre-Dynkin system which is only closed under finite disjoint unions.

Imprecise probabilities are precise on a pre-Dynkin system.

Hence “the system of precision”

When one defines a measure on a pre-Dynkin system and extends it to an algebra, one essentially recreates the theory of coherent upper previsions – newly “measurable” events have an imprecise probability.

Allows one to model intersectionality – think of what it means that all intersections of events have probabilities when one tries to reason with finite data – why assume every compound event should be ascribed a (precise) probability?
NON-STOCHASTIC SEQUENCES
There is nothing more deceptive than an obvious fact.
— Arthur Conan Doyle, *The Boscombe Valley Mystery*

“Data as fact”

The foundation of the “discipline” of statistics:

The prospectus of the Statistical Society of London (1838) stated: “The Statistical Society will consider it the first and most essential rule of its conduct to exclude carefully opinions from transactions and publications.”

Their motto was *aliis exterendum* — “to be threshed out by others”

The wanted to sever any connection between the data and its use

Nowadays: “benchmark data sets”; but what gets lost in this view of data?
DATA AS "RANDOM VARIABLES"

- The canonical model of "data"
- Two small difficulties from a mathematical perspective:
  - They are not "random"; they do not "vary"
    - Because they are simply (measurable) functions!
  - Interpreting "random" and "variable" is hard!
    - Bertrand Russell reckoned the notion of a "variable" to be "one of the most difficult to understand" notions in mathematics
- Deep learning researchers are of little help...
- But we have a well accepted mathematical theory of probability. *Surely the answer is known?*
- Indeed! Based upon the Kolmogorov's axiomatisation. So what does he have to say?
§ 2. The Relation to Experimental Data

The reader who is interested in the purely mathematical development of the theory only, need not read this section, since the work following it is based only upon the axioms in § 1 and makes no use of the present discussion. Here we limit ourselves to a simple explanation of how the axioms of the theory of probability arose and disregard the deep philosophical dissertations on the concept of probability in the experimental world. In establishing the premises necessary for the applicability of the theory of probability to the world of actual events, the author has used, in large measure, the work of R. v. Mises, [1] pp. 21-27.
Suppose \((X_i)_{i \in \mathbb{N}}\) is a iid sequence of Bernoulli random variables with \(\mathbb{P}(X_i = 1) = p \in [0,1]\).

- Let \(S_n := \sum_{i=1}^{n} X_i\) for \(n \in \mathbb{N}\).
- Then \(\mathbb{P}(\lim_{n \to \infty} S_n / n = p) = 1\)
REPEAL OF THE “LAW” OF LARGE NUMBERS

- Let $L^{1/2}$ denote the set of binary sequences with limiting relative frequency $1/2$.
- SLLN: $\lambda(L^{1/2}) = 1$. Thus $L^{1/2}$ is a very large subset of $\{0,1\}^\infty$.
- Oxtoby: $L^{1/2}$ is meagre in $\mathcal{T}^\infty$. Thus $L^{1/2}$ is a very small subset of $\{0,1\}^\infty$.
- Many even stronger variants; bottom line: maths won’t solve this…
BUT WON’T THIS UNDERMINE PROBABILITY?

- Yes, it undermines probability theory’s *claim for universality* - for being the only theory of uncertainty you need

- But the grander theory that is needed for “nonstochastic” randomness is a strict generalisation of probability theory

---

In everyday language we call random these phenomena where we cannot find a regularity allowing us to predict precisely their results. Generally speaking there is no ground to believe that a random phenomenon should possess any definite probability. Therefore, we should have distinguished between randomness proper (as absence of any regularity) and stochastic randomness (which is the subject of the probability theory).
VON MISES’ PROGRAM: DERIVE KOLMOGOROV’S AXIOMS FROM MORE BASIC ONES

- Von Mises was endeavouring to create a scientific theory of probability – not just a mathematical one.

  - Axiom 1: relative frequencies converge.
  - Axiom 2: They remain invariant under sub-selection.

- What if axiom 1 is not satisfied?
Bruno De Finetti opened his book on probability by stating that: “Probability Does Not Exist” (i.e. did not exist independent of observer).

“Thus” it is a wholly subjective notion...

WHEN THE RELATIVE FREQUENCIES DON’T CONVERGE…

- Then there is no “probability” (or more precisely, no “the probability”)
  - Instead there are multiple cluster points
- Have a sequence \( x: \mathbb{N} \rightarrow [k] \)
- Relative frequency of \( i \)th class: \( r_i^x(n) := \frac{1}{n} | \{ j \in [n]: x_j = i \} | \)
- Stack all these into a \( k \)-vector to get the relative frequency \( r^x(n) := r^x_{[k]}(n) \)
- Let \( \text{CP}(r^x) \) denote the set of cluster points of \( r^x \); if a singleton, then limit exists
NON-CONVERGENCE AT INFINITY
BUT CONVERGENCE TO “INFINITY”

- Suppose $C$ is a rectifiable closed curve in $\Delta^k$. Then there exists $x$ such that the set of cluster points of $r^x$ is $C$.
- From this one can naturally recover risk measures / upper previsions
- Every sequence can be reasoned with in terms of an upper prevision
- And every upper prevision can be generated by the relative frequencies of some sequence
IN ADDITION…

- Interpolation between Knightian risk and uncertainty
- Can also develop unstable conditional probability
  - And recover a “generalised Bayes rule”
- And define a nice notion of independence
  - Ends up being a bit tricky to do (one needs to worry about the set-system)
- But this is early days
  - Yet to explore estimators and the use in practice
  - Intriguing that one can completely recover Walley’s theory (based as it is on the de Finetti subjective framework) in a strictly frequentist setting
LOOKING AHEAD
CURRENT / FUTURE QUESTIONS

- Make it practical: estimating sets of cluster points of relative frequencies
- Applications in insurance – intersectionality and imprecision
- Relate to general measures of information
  - Both are support functions of convex sets...
- Non-stochastic sequences and traditional models
  - Distribution shift, non-stationarity, selection bias, etc
- Relation to other “black swan” theories
- Non-stochastic sequences and performative prediction

The foundations of statistics with black swans
Graciela Chichilnisky
Many roads lead to upper previsions $\overline{R}_\mathcal{P}(X) = \sup_{P \in \mathcal{P}} \mathbb{E}_P(X)$

Mathematically nice: a support function with $\langle X, P \rangle := \mathbb{E}_P(X)$; thus $\overline{R}_{\text{coP}}(X) = \overline{R}_\mathcal{P}(X)$

Imprecise probability of an event $A$ is $\overline{P}(A) = \overline{R}(\chi_A)$

Fundamental function $\phi(t) = \overline{R}(\chi_{A_t})$, where $\mu(A_t) = t$, stratifies $\{\overline{R}\}$

Offers ethical insight and tail control

System of precision provides a different parametrisation, and offers an approach to modelling intersectionality

From “almost all” to “all”: every sequence $x: \mathbb{N} \rightarrow [k]$ induces an $\overline{R}$, and vice versa

This provides strictly frequentist semantics for imprecise probability

“The probability” does not necessarily exist; something richer always does
REFLECTIONS

▸ Challenge what is taken for granted
▸ Seeking many paths is not redundant
▸ Knowledge is a relation, not a thing
▸ Foundations are an interface to the world
Loss functions and Information
The Geometry and Calculus of Losses
Information Processing Equalities and the Information-Risk Bridge

Generalised Expectations
Risk Measures and Upper Probabilities: Coherence and Stratification
Tailoring to the Tails: Risk Measures for Fine-Grained Tail Sensitivity

The System of Imprecision
The Set Structure of Precision: Coherent Probabilities on Pre-Dynkin-Systems

Non-stochastic Sequences
A Strictly Frequentist Theory of Imprecise Probability

Independence*
Fairness and Randomness in Machine Learning: Statistical Independence and Relativization

Nonlinear Expectations & Fairness*
Fairness Risk Measures (ICML2019)

* Not covered in the talk