all men count with you, but none too much: Information Aggregation and Learning in Prediction Markets

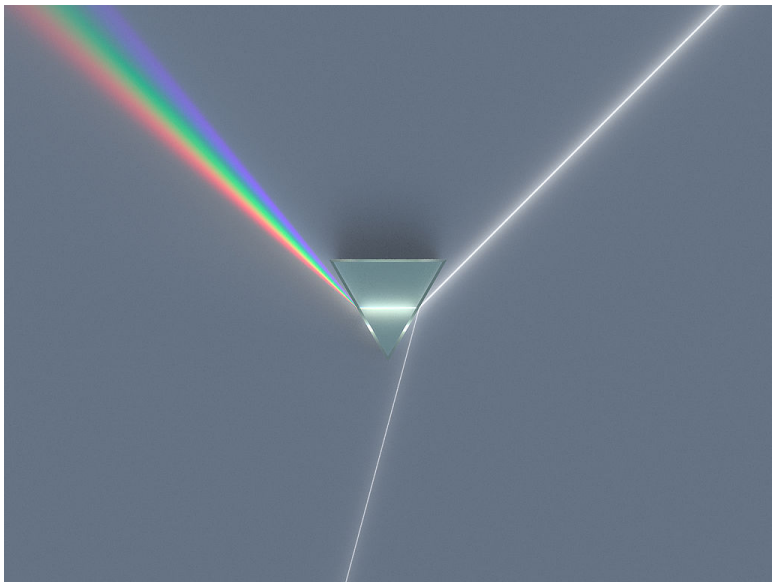
by

Sindhu Krishnan Kutty

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Computer Science and Engineering)
in The University of Michigan
2015

Doctoral Committee:

Assistant Professor Jacob D. Abernethy, Chair
Professor Paul J. Resnick
Rahul Sami, Google Inc.
Professor Michael P. Wellman



for my nilesh
तू असा जवळी रहा

ACKNOWLEDGEMENTS

They say it takes a village to raise a child, and this baby of mine has been nurtured and helped along by several wonderful people along the way!

First, I'd like to acknowledge my amazing advisor, Prof. Jacob D. Abernethy for making the last year and a half of my time at UM the most enjoyable and memorable. His exceptional ability to tease out intuitive explanations for the most abstract concepts makes working with him tremendously exciting. He very generously took me under his wing and introduced me to the larger vibrant research community in this area. He encouraged me to have a little more faith and be a little bolder. His influence on my way of thinking and writing have been great and is, I hope, reflected in this thesis. And as if all that weren't enough, he's also funny, warm and loads of fun to hang out with! And, Jake, I owe you a homemade Indian meal!

Dr. Rahul Sami introduced me to the idea of prediction markets. Some of our work on learning in recommender systems is what got me interested in the idea of connections between machine learning and prediction markets. Thank you for leaving me free to explore and learn the ropes of this area and for funding my initial foray into research.

I'd also like to thank my wonderful collaborators Dr. Sébastien Lahaie and (more recently) Dr. Rafael Frongillo and my other committee members Prof. Paul Resnick and Prof. Michael Wellman (and previously Prof. Satinder Singh Baveja and Provost Martha Pollack) for their input at various points along the way. I'd like to particularly acknowledge Prof. Michael Wellman for recognizing the significance of a side result

in my proposal that eventually led to an exciting project and Provost Martha Pollack for being so encouraging during my initial years at UM. Early on, I had tons of fun being a Graduate Student Instructor for Prof. Seth Pettie, Prof. Martin Strauss and Prof. Kevin Compton; Seth also managed to convince the powers that be to bestow a runner-up teaching award for which this GSI is particularly grateful! Also in the CSE department, I'd like to thank (perhaps the nicest) grad chair Prof. Benjamin Kuipers, the walking encyclopedia of anything related to grad school, Dawn Freysinger, the super helpful and warm Karen Liska and my fellow grad students and friends Chansoo Lee and Travis Martin.

I got my first taste of research at Villanova University while working with Prof. Mary-Angela Papalaskari and Prof. Giorgi Japaridze both of whom were incredibly supportive and encouraging; Prof. Papalaskari continues to be a close friend and mentor and I'm very grateful to have her in my life.

On a more personal note, I'd like to gratefully acknowledge Dr. Sonya Freiband for helping me navigate some complicated events of the past few years, and Katelyn Cooper for being so awesome with both my boys.

Somehow, I had the incredible luck to be born to Sudha and Krishnan Kutty. Through the ups and downs, their love and faith has been unwavering and their support absolute. In addition, I'm so thankful for my father's delight and supreme pride in my smallest accomplishments and my mother's ability to find the minutiae of my life so incredibly fascinating (for which, by the way, she has the rather dubious privilege of being on the receiving end of descriptions of said minutiae). I hope they have an inkling of how special they are to me.

I am very fortunate to be able to spend my days with three of the most delightful characters in the world. Many thanks go to my puppy, Roscoe, for warming my feet and my heart through many cold days and nights (you're still not officially allowed on the bed, by the way!). My heartfelt gratitude to my son, Dhruv, for bringing me

such joy and for being a constant reminder of all that's wonderful and important in Life. (And I don't care how old you are when you read this, you'll always be my snuggle puppy!) And finally, and perhaps most importantly, for always expecting the best of and for me, I give my undying love to my best friend, my staunchest supporter, my source of strength, wisdom and confidence (and an endless supply of quirky humor!): Nilesh D. Mankame. More than fifteen years since we first met, I still can't believe that someone as smart, funny, kind and decent, cherishes me so! He teaches me daily, by example, how to live a life of gratitude and generosity. Simply being in his company makes me a better version of myself. Babu, as we get ready to embark on our next adventure together, I feel safe in the knowledge of this truth[1]:

and this is the wonder that's keeping the stars apart,

i carry your heart(i carry it in my heart).

[1]lines shamelessly borrowed from e e cummings

TABLE OF CONTENTS

ABSTRACT

all men count with you, but none too much:
Information Aggregation and Learning in Prediction Markets

by

Sindhu Kutty

Chair: Jacob D. Abernethy

Prediction markets are markets that are set up to aggregate information from a population of traders in order to predict the outcome of an event. In this thesis, we consider the problem of designing prediction markets with discernible *semantics* of aggregation whose *syntax* is amenable to analysis. For this, we will use tools from computer science (in particular, machine learning), statistics and economics. First, we construct generalized log scoring rules for outcomes drawn from high-dimensional spaces. Next, based on this class of scoring rules, we design the class of exponential family prediction markets. We show that this market mechanism performs an aggregation of private beliefs of traders under various agent models. Finally, we present preliminary results extending this work to understand the dynamics of related markets using probabilistic graphical model techniques.

We also consider the problem in reverse: using prediction markets to design machine learning algorithms. In particular, we use the idea of sequential aggregation from prediction markets to design machine learning algorithms that are suited to situations where data arrives sequentially. We focus on the design of algorithms for

recommender systems that are robust against cloning attacks and that are guaranteed to perform well even when data is only partially available.

CHAPTER I

Introduction

1.1 The Backstory

Consider the following question: can we harness collective human intelligence to predict the outcome of future events with a high degree of accuracy?

The problem of predicting future outcomes has wide applicability and the idea of harnessing the "wisdom of crowds" has been explored even in popular culture (*Surowiecki*, 2005). Consider, for instance, the following prediction problems. A government might want to assess the probability of outbreak of an infectious disease in the country, or a campaign manager might want to have a current assessment of the likelihood of her candidate's success, or a company may want to assess the likelihood of timely product delivery. Depending on these assessments, the organizations might decide to act differently. For instance, the government might want to shore up its supply of vaccines, the campaign might want to reassess its strategies (like choosing an appropriate vice president) or the company might want to revise its delivery date. To understand how the wisdom of crowds might help us make these estimates, let's take a closer look at the first of these examples.

Suppose that we are charged with predicting the probability of an outbreak this year (of a particular magnitude) of the disease *du jour*. There are many parties who have information of interest to us including the media, doctors, people in the aviation

industry, people who have flown to an area with the disease, people who know (of) such people etc. We are now living in a world where communication is easier than ever and subsequently we have the means to contact the relevant individuals and collect their responses. However, it's one thing to have the ability to *access stated opinions* and quite another to be privy to *internal beliefs* and have a sense of the *aggregate* opinion – and, in fact, part of the problem is to define aggregation more precisely.

Perhaps it is not surprising that one way to incentivize participation is to have people "put their money where their mouth is". That is, provide a *financial* incentive for *truthful participation*. But what mechanism should we use for this? It has been observed that financial markets prove to be surprisingly good predictors. For instance, orange juice futures turn out to be a better predictor of future weather (yes, the *weather*!) than statistical data (for a fascinating analysis of this see *Roll* (1984)). So it came to pass that economists started asking why not set up markets whose *goal*, rather than consequence, is information aggregation with a view to prediction.

Prediction markets are market mechanisms where you can trade on your perceived likelihood of an event. The market issues contracts (called *securities*) that correspond to each outcome of the event; going back to the disease example, this could correspond to a contract that pays off some amount if the outbreak comes to pass this year and nothing otherwise. The market will also set some price on this contract. Clearly, if you believe that the disease outbreak is imminent, you would want to buy this contract if your expected payoff is more than the current price. To make this easier to reason about, the contract is usually set up to pay off \$1 if the event occurs and \$0 otherwise[1]. This allows us to interpret prices as probabilities; the price at which a (risk neutral) trader would be indifferent between buying and selling this security would exactly match his belief probability of the event occurrence.

[1] these are called Arrow-Debreu securities

Notice that, while we have argued that the price would correspond to a *risk neutral* trader's belief, we have said nothing about *aggregation process* which, by the way, is the main point of the market mechanism! Also, an astute reader would have noticed that if we propose to issue a security for each outcome, we are restricting ourselves to scenarios with finite (and a reasonable number of) outcomes. Clearly, these are pressing issues and, excitingly, ones that we explore here.

Because of complicated anti-betting laws and uncertain legal ramifications, prediction markets haven't been as widely deployed as they are applicable. Corporate prediction markets are known to be increasingly used to assess viability of projects and timeliness of software delivery (*Cowgill et al.*, 2009); typically these markets are run within the firm using play money (see, for instance, *Bell* (2009) for an analysis of legal ramifications of running corporate prediction markets). Iowa Electronic Markets[2] allow the public to trade on political outcomes (among other things) using (a limited amount of) real money. Since these markets are run by the University of Iowa Tippie College of Business and the markets are run for educational and research purposes, the IEM has been granted conditional legal status by the US government[3]. Robin Hanson, among others, made the case for deploying prediction markets more widely both for information aggregation as well as to study what works and what doesn't (*Hanson*, 1999). But, as scientists, we are not satisfied in simply knowing *that* these markets work well, but also *why* they do, whether these results are *repeatable* and to *what degree*. In other words, we would like to build a model to explain the process and thence construct sound prediction market machinery from the ground up.

It has been known since the 1950s (*Brier*, 1950) that it is possible to incentivize a single person to truthfully report his belief (the context again, believe it or not, was

[2]available at `https://tippie.uiowa.edu/iem/`

[3]it received no-action letters from the Division of Trading and Markets of the Commodity Futures Trading Commission

the weather!). *Hanson* (2003a) had the brilliant insight of using these proper scoring rules sequentially in order to allow elicitation from *groups* of people. Due to some desirable properties (for instance, the way LMSR responds to bets on conditional probabilities), Hanson particularly advocated the use of the logarithmic scoring rule which in its sequential prediction market variant is called the Logarithmic Market Scoring Rule (LMSR) (*Hanson*, 2007).

This sequential formulation of LMSR turns out to be equivalent (under mild conditions) to a more natural *cost function based market maker* (*Hanson*, 2007; *Chen and Pennock*, 2007). In this case, the market maker charges traders for buying shares of issued contracts, which are themselves Arrow-Debreu securities, using a potential function evaluated on the total number of shares of all securities purchased thus far. More generally, *Chen and Vaughan* (2010) established a one-to-one correspondence between strictly proper market scoring rules and convex cost-function-based market makers. In a surprising twist, *Abernethy et al.* (2013) showed that, in fact, if you design your market maker axiomatically to satisfy some intuitive and desirable properties, you *must* actually price your securities using cost functions.

In this thesis, we focus on building *cost-function-based prediction markets*. We design a prediction market mechanism (over possibly *infinite outcome* spaces) using tools from statistics and under various models of trader behavior, including *risk aversion* and *budget constraints*. We show that, under reasonable assumptions, the behavior of rational traders can be understood as the result of implementing a *learning algorithm* on their private beliefs. Similarly, the market state can be interpreted as a distribution over the outcome space. Of particular interest is the market equilibrium: the market state at which no trader is motivated to make any more trades. Interestingly, our market design results in a market equilibrium that corresponds to a *weighted mixture of traders' private beliefs*. We draw connections between the aggregation of data performed by learning algorithms and the information aggregation

done in prediction markets. We are also able to tease out a surprising correspondence between financial exposure in a market and privately held beliefs.

Let's go back to the running disease example. In fact, the same sets of people in a neighboring country (doctors, media, travelers, etc.) may also have relevant information. Suppose the government of this neighboring country has also been similarly obsessed with estimating the probability of an outbreak in the first country using prediction markets. This exposure to different trading populations might lead to different estimates – how should they be collated? We consider this problem as the *interactions between markets*. That is, we consider scenarios where markets for predicting the outcome of a *single event* were deployed in *multiple venues*. Suppose now, that the neighboring country actually deployed a separate prediction market to estimate the probability of an outbreak *at home*. In this case, the markets are not on the same event, but on *related* ones; the probability of outbreak in a country would affect the probability of the outbreak in its neighbors (borders being what they are). Is this effect something that can be accurately quantified? How should markets on related events be designed? Should trades in one market be reflected in related ones? If so, how? We explore these questions in this thesis.

We also consider how ideas from prediction markets may be incorporated into designing learning algorithms for social computing. Consider internet-based recommendation systems like those in the movie rental service provider Netflix, Inc.[4] and the electronic commerce company Amazon.com, Inc.[5], or the crowd-sourced reviews for restaurants and other local businesses in Yelp[6]. Nearly everyone has had a moment where a review for a product or service appears suspiciously gushing or otherwise obviously fake. How does one weed out these fake reviewers? A clever attack on these systems is the *cloning* attack where one of these fake reviewers artificially boosts their

[4]available at `https://www.netflix.com/`
[5]available at `http://www.amazon.com/`
[6]available at `http://www.yelp.com/`

standing in the system by copying previous reviews and then exploiting their reputation to later mislead the recommendation system. We use the idea of sequential aggregation from prediction markets to design new algorithms for these internet-based recommendation and forecasting systems. We identify that on the one hand, these domains have genuine, helpful and informative forecasters whose information is crucial for accurate predictions; on the other hand, there may also be malicious agents who provide strategically misleading predictions to the system. The domain also allows for erratically arriving information and possible non-availability of feedback. We present a model that captures the major characteristics of this domain and use a *prediction market metaphor* to design and analyze high performance algorithms in this model.

1.2 Structure of the thesis

In the next chapter, we provide some background and a brief overview of the models and results discussed in this thesis.

In Chapter III we define a scoring rule-based prediction market mechanism for belief aggregation. Background for this chapter is covered in Sections 2.1 and 2.2.

We provide results on modeling interactions between prediction markets in Chapter IV using graphical models.

In Chapters V and VI we design online learning algorithms for recommender systems; we provide a brief review of these systems in Section 2.4.

We end the thesis by summarizing our results and by outlining avenues for further exploration in Chapter VII.

1.3 Summary of Contributions

We now highlight the main contributions of this thesis.

Maximum Entropy Scoring Rules When you are faced with making a prediction about a (reasonably sized) finite outcome space, you are free to construct a scoring rule that elicits the entire distribution and score people accordingly. But what if you intend to predict the outcome of an event from a high-dimensional or even infinite outcome space? Jacob Abernethy, Sébastien Lahaie, Rahul Sami and I show that arguably, under such circumstances, *the* generalization of the proper log scoring rule to general statistics and outcome spaces can be constructed from exponential families (*Abernethy et al.*, 2014b). Exponential family distributions are a class of distributions that arise out of picking the maximum entropy distribution that agrees with agent beliefs. Intuitively, these maximum entropy distributions maximize uncertainty in (or assume the least about) the data. This is striking; it means that the agents are free to have *any* belief distribution but that in order to maximize their score they will be incentivized to be truthful about the expected value of the statistics under that belief.

Exponential Family Markets Based on these proper scoring rules, we design a class of *cost-function-based prediction markets* over possibly *infinite outcome* spaces using tools from statistics. We analyzed the market evolution under various models of trader behavior, including *risk aversion* and *budget constraints* (*Abernethy et al.*, 2014b) and showed that, under reasonable assumptions, the behavior of rational traders can be understood as the result of implementing a *learning algorithm* on their private beliefs. Similarly, the market state can be interpreted as a distribution over the outcome space. Our market design results in a market equilibrium that corresponds to a *weighted mixture of traders' private beliefs*. The semantics of prices at *equilibrium* in binary outcome prediction markets have been analyzed before (*Wolfers and Zitzewitz*, 2006; *Manski*, 2004). In our more general exponential family market, we drew connections between

the aggregation of data performed by learning algorithms and the equilibrium market state. We were also able to tease out a correspondence between financial exposure in a market and privately held beliefs.

Graphical Models for Prediction Markets We are interested in explicitly characterizing the interaction between markets on the same and on related events by drawing on results from graphical models. In one instance, we are able to show that a trader in such a market behaves as if he were *implementing a learning algorithm*, even though his *incentives are purely financial*.

Learning Algorithms for Recommender Systems One of the challenges in recommender systems is to implicitly identify the non-informative or malicious agents so that the recommendations can be based on the truly informative agents' predictions. This domain also allows for erratically arriving information. Additionally the true outcome is not always revealed to the algorithm. We cast this as a *general online learning problem* that captures the information as arriving sequentially, the agents as either stochastic processes or adversarial entities and feedback as only conditionally available and design an algorithm that makes recommendation predictions that are *nearly* accurate.

CHAPTER II

Background

This chapter provides some of the technical background for the ideas we explore in this thesis. We start with the core concept – that of prediction markets.

2.1 Prediction Markets

Prediction markets are markets that allow traders to bet on contracts (also known as *securities*) whose value depends on the outcome of some future event. For example, to predict the outcome of a presidential election one could imagine a contract that pays off \$1 if the Republican candidate wins the election and \$0 otherwise. The price on this contract, which could vary between \$0 and \$1, can be interpreted as the probability of that candidate winning the election.

The reason that we typically think of prediction markets as representing aggregate information of a population is tied to the observation that any trader who believes that the probability of an outcome is p for a security that pays off \$1 should be willing to *buy* (respectively sell) a security priced at *less* (respectively more) than p. It stands to reason then that if the market is "stationary" then the traders have somehow reached a consensus at probability p.

The prediction market could be implemented in a number of ways including as continuous double auctions, pari-mutuel markets and automated market makers (see, for

instance *Pennock and Sami* (2007), for details). If you design your automated market maker to satisfy some intuitive axioms like path independence and no-arbitrage, it turns out that the pricing rule can always be defined in terms of a *cost function* that takes the number of outstanding shares of all securities as argument.

Cost Function Prediction Market One popular form of the prediction market mechanism for finite outcomes is the logarithmic market scoring rule (LMSR) (*Hanson*, 2003b). In this case, the market maker issues a contract associated with each of n outcomes; each of these contracts pays off \$1 iff the associated outcome $i \in \{1, \ldots, n\}$ occurs and nothing otherwise. The market state is defined by the total number of outstanding shares of each security that have been purchased so far in the market. If the current market state is $\mathbf{q} = (q_1, \ldots, q_n)$ for n securities and a trader wishes to purchase $\boldsymbol{\delta}$ security shares in this market, the automated market maker implementing the log market scoring rule will charge $C(\mathbf{q}+\boldsymbol{\delta})-C(\mathbf{q})$ dollars, where $C(\mathbf{q}) = \log \sum_{i=1}^{n} \exp q_i$. In this case, $\nabla C(\mathbf{q})$ gives you the *instantaneous price* of the securities. This price can be interpreted as a predicted distribution on the outcomes. Typically this price corresponds to the last trader's belief in this market, who is assumed to update his belief to incorporate all previous trades in the market. In this thesis, we present a cost function based market maker that demonstrably performs belief aggregations of *all* traders in the market.

2.2 Exponential Families of Distributions

We will now switch gears to talk about a popular family of probability distributions that turn out to be instrumental in generalizing the LMSR mechanism we described above. Suppose we are given access to empirical averages of some function of data. A natural question to ask is if we can find a distribution whose *expected* statistics match these observations. Exponential family distributions arise as the *unique* solution to

match these while maximizing (the Shannon entropy notion of) uncertainty. The *exponential family of distributions* includes many of the commonly used distributions including the *Gaussian*, the *multinomial*, the *Poisson*, etc.

Consider the Gaussian distribution on a single real variable x. Typically the distribution is parameterized in terms of mean μ and variance σ^2. If we instead define *natural* parameters $\theta = \left(\frac{\mu}{\sigma^2}, \frac{-1}{2\sigma^2}\right)$, and a vector function $\phi(x) := (x, x^2)$, we see that the probability density function of the Gaussian

$$p_{\mu,\sigma}(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp -\frac{(x-\mu)^2}{2\sigma^2}$$

can be rewritten as

$$p_\theta(x) = \exp(\theta \cdot \phi(x) - \psi(\theta)) \tag{2.1}$$

where $\psi(\theta)$ is a normalization term (that does not depend on the data x) that ensures that the pdf integrates to 1. Thus

$$\begin{aligned} \int_x \exp(\theta \cdot \phi(x) - \psi(\theta))\, dx &= 1 \\ \text{Or} \quad \psi(\theta) &= \log \int_x \exp(\theta \cdot \phi(x))\, dx \end{aligned}$$

It turns out that Equation 2.1 describes the general form of exponential family distributions. Here $\psi(\theta)$ is called the log partition function and $\phi(x)$ are the sufficient statistics. Recall that a statistic is just a function of the data. If the data is drawn from some distribution parameterized by θ then a statistic is called *sufficient* if no other statistic that can be computed from the data gives you more information about θ. For instance, the number of heads in a set of Bernoulli trials gives you a everything you need in order to compute a distribution on the trial outcomes. In particular, if there are n trials and k heads, it is not necessary to know exactly when the heads

occurred in order to compute the probability of that sequence (which is always $\frac{1}{\binom{n}{k}}$ regardless of the success probability or the particular order of the sequence.).

It turns out that an equivalent alternate parameterization of exponential family distributions is via its *mean parameters* $\mu_\theta := \mathrm{E}_{\mathrm{x}\sim\mathrm{p}_\theta}[\phi(\mathrm{x})]$. The mean parameters can be obtained via differentiation of the log partition function; that is, for any θ we have $\nabla\psi(\theta) = \mu_\theta$. We describe exponential families in greater detail in Chapter III. For now, we will look at Bayesian updates in exponential families which provides a way to reason about estimating natural parameters given access to data points.

2.2.1 Bayesian Updates in Exponential Families

Parameter estimation involves specifying a particular value or distribution over values of parameters given access to data points.

Example: Estimating the Bias of a Coin

Consider the following simple example. Suppose we want to estimate the probability of heads p on a coin toss. One way would be to provide a maximum likelihood estimate of the probability p after a number of independent trials T as

$$\frac{\text{number of heads in } T \text{ trials}}{T} = \frac{h}{T}$$

This is the frequentist view of parameter estimation. Another way to estimate parameters would be to assume a prior distribution on p, say $\pi(p)$. The posterior distribution on p, $\pi(p|h)$, would then be determined by the number of heads h we saw in T trials as well as the prior distribution. In fact, Bayes theorem allows you to compute the posterior distribution as follows:

$$\Pr(p|h) = \frac{\Pr(h|p)\Pr(p)}{\Pr(h)}$$

$\Pr(h)$ the probability of observing h heads in T tosses can be viewed as a normalization constant since it is independent of p, which can be seen as having been marginalized out. So the posterior distribution can be written as

$$\Pr(p|h) \propto \Pr(h|p)\pi(p)$$

Since we are considering the probability of heads in a coin toss, it is reasonable to assume a Binomial form on the likelihood function $\Pr(h|p)$. Note that $\Pr(h|p)$ is a function of p with a particular value for h. Thus,

$$\Pr(h|p) = \mathrm{Bin}(h|p) = \binom{T}{h} p^h (1-p)^{T-h}$$

It turns out that given a likelihood function, for particular choices of the form of the prior distribution, the posterior distribution will have the same functional form. This functional form is then called the *conjugate prior* of the likelihood function. For the Binomial distribution the conjugate prior is the Beta distribution, which is defined as follows (*Diaconis and Ylvisaker*, 1979).

$$\mathrm{Beta}_{\alpha,\beta}(x) \stackrel{\text{def}}{=} \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}$$

where the gamma function $\Gamma(x) \stackrel{\text{def}}{=} \int_0^\infty u^{x-1}e^{-u}du$. The parameters α and β are called hyperparameters because they control the distribution of the parameter to be estimated p.

Thus if $\pi(p) = \mathrm{Beta}_{\alpha,\beta}(p)$, then the posterior distribution on p when there have been T coin tosses with h heads is

$$\Pr(p|h) = \mathrm{Beta}_{\alpha',\beta'}(p)$$

where $\alpha' = \alpha + h$ and $\beta' = \beta + (T - h)$.

Both Binomial and Beta distributions are particular forms of exponential family distributions. One nice feature of the exponential family of distributions is that the family of conjugate priors are themselves members of the exponential family.

Conjugate Priors in Exponential Families

Let $p(x;\theta)$ denote a probability density function of an exponential family with sufficient statistic $\phi : \mathcal{X} \to \mathbf{R}^d$, where θ is the natural parameter:

$$p(x;\theta) = \exp\left[\langle\theta, \phi(x)\rangle - \psi(\theta)\right],$$

and

$$\psi(\theta) = \log \int_{\mathcal{X}} \exp\langle\theta, \phi(x)\rangle dx.$$

Here $\langle\theta, \phi(x)\rangle$ represents the inner product of the vectors θ and $\phi(x)$.

The family of conjugate priors is also an exponential family and takes the form

$$p(\theta; n, \nu) = \exp\left[\langle n\nu, \theta\rangle - n\psi(\theta) - \hat{\psi}(\nu, n)\right].$$

This prior distribution is the distribution on the natural parameters θ on the distribution on $\mathcal{X}$. The sufficient statistics of the prior distribution are a function of θ defined as $\hat{\psi}(\theta) = (\theta, -\psi(\theta))$. The natural parameters of the prior distribution are $(n\nu, n)$ where $n \in \mathbf{R}$ and $\nu \in \mathbf{R}^d$. The function $\hat{\psi}(\nu, n)$ normalizes the pdf so that it integrates to 1 and is convex in $(n\nu, n)$. It is helpful to think of the prior as being based on a phantom sample of size n and mean ν. The justification for this is that

$$\mathbf{E}_\theta\left[\mathbf{E}_x\left[\phi(x)|\theta\right]\right] = \mathbf{E}_\theta\left[\nabla\psi(\theta)\right] = \nu.$$

For a proof see *Diaconis and Ylvisaker* (1979).

Suppose we draw a sample $X = (x_1, \ldots, x_m)$ of size m, and denote the empirical mean by $\mu[X] = \sum_{i=1}^{m} \phi(x_i)$. The posterior distribution is then

$$p(\theta|X) \propto p(X|\theta)p(\theta|n,\nu) \propto \exp\left[\langle \mu[X] + n\nu, \theta\rangle - (m+n)\psi(\theta)\right],$$

and so the posterior mean is

$$\frac{m\mu[X] + n\nu}{m+n}. \tag{2.2}$$

Thus the posterior mean is a convex combination of the prior and empirical means, and their relative weights depend on the phantom and empirical sample sizes.

2.2.2 Graphical Models

Exponential family distributions are used widely and across a number of fields, but they have found prominent usage for probabilistic models that involve several variables with complex codependence relationships. These relationships are captured efficiently using (*probabilistic*) *graphical models*. Exponential family distributions are especially amenable to analysis using graphical models (*Wainwright and Jordan*, 2008). In Chapter IV we will model the interaction between related prediction markets using graphical models. We will show how the exponential market mechanism allows you to precisely characterize the effect of a trade in a market on a related market. We will also draw connections to learning algorithms for markets with latent variables.

2.3 Exponential Family Prediction Markets

Recall that the LMSR market maker is defined on finite outcome spaces. Using the exponential family distributions, we design a class of continuous outcome space market makers that demonstrably perform meaningful aggregations. We detail this work in Chapter III.

The log partition function $\psi(\theta)$ of the exponential family distribution can be used

to define a generalized LMSR cost function. If you further define securities whose payoffs correspond to the sufficient statistics $\phi(x)$ then the outstanding share vector corresponds exactly to the natural parameters of the exponential family. This means that the market state now defines an exponential family distribution over the outcome space. In terms of the market semantics, the mean parameters of the distribution may be interpreted as the instantaneous prices of the securities.

Modeling Trader Behavior We analyze trader interactions with the market under various models of their behavior.

- Typically, traders interacting with prediction markets are assumed to be risk neutral. Thus, they continue buying (or selling) shares in this market until the cost of purchase of a security exactly matches its payoff. We can use concave utility functions to describe risk aversion in traders. We will focus on the exponential utility function which grows as the negative exponential in wealth; the degree of risk aversion is a parameter of this utility function. We will show that an exponential utility trader moves the market state to a mixture of the current state and his belief. In fact, as the trader grows more risk averse, the final state stays closer to the current market state.

- We could also consider Bayesian traders who treat the current market estimate as a prior and compute the likelihood function based on their own private data to move the market state so as to maximize their expected payoff. These traders essentially move the market state to the corresponding maximum a posteriori estimate on the natural parameters of the posterior distribution.

- If traders have budget constraints, then it will affect how far they can move the market state to match their beliefs. We will analyze the interaction of both malicious and informative budgeted traders in the market. We characterize a

malicious trader as one who moves the market state arbitrarily (as opposed to matching his own private belief). We are interested in analyzing the accuracy of the market as characterized by the negative logarithmic loss of the prediction. In this market, change in budget of a trader is exactly the (myopic) loss he induces in the market. Further, an informative trader with positive budget, who moves the market state closer to the true distribution from which the outcome is drawn, can expect to make a profit. Over participation in multiple exponential family markets, we can show that total incremental loss due to a malicious trader is bounded by his initial budget.

- The market evolution when there are multiple traders who have exponential utility is particularly striking. The market at equilibrium would essentially correspond to the average of the agent beliefs weighted by their risk aversion parameters. There is also a surprising equivalence between beliefs and trades in this market. An exponential utility trader engaging in a trade in this market can be thought of as essentially updating his belief. This means that the cost function market exposes a deep connection between beliefs and financial transactions: an agent with some exposure in the market is in effect equivalent to an agent with a different belief.

2.4 Learning in Recommender Systems

In Chapters V and VI of this thesis, we focus on the model of machine learning, called online learning. In batch machine learning, the algorithm designer has access to training data against which the algorithm's learning takes place. The algorithm's performance is then measured on predictions made against test data. In contrast, in online learning both learning and prediction proceed simultaneously. Learning proceeds in rounds, and in each of $t = 1, 2, \ldots, T$ rounds the goal of the algorithm is

to predict based on its input and then learn from feedback obtained on its predictions. Typically, this feedback is in terms of a loss function that measures how much the algorithm's prediction differed from the actual outcome. Often in online learning, it is not possible to characterize this outcome as being generated from a stationary stochastic distribution. The outcome is then said to be adversarially generated. This is in contrast to the traditional statistical models where the outcome is the realization of a stationary statistical process (*Cesa-Bianchi and Lugosi*, 2006). In this case the properties of the distribution may be estimated from the data and the *risk* may be defined as the expected difference between the losses due to the predicted value and true outcome.

The lack of this simplifying stochastic assumption on outcomes not only makes prediction harder, but it is also unclear how to measure the performance of an algorithm in this setting. Consider, for instance, a simple model where the algorithm's prediction and actual outcome are both binary with an adversarially generated outcome. Consider a loss function that simply counts the number of mistakes of the algorithm over all rounds. This simple 0/1 loss measure per round is called a *mistake bound model* (*Littlestone and Warmuth*, 1994). *Any* algorithm can be shown to behave badly when measured in this model using simple worst case analysis. In fact, in this case, an unbiased coin toss would provide the best performance, giving an expected loss of $T/2$, where expectation is taken with respect to the random coin toss. This motivates the need for a better measure of performance in this model.

2.4.1 Online Learning with Expert Advice

In order to provide a more meaningful benchmark, we move to a model that provides comparators against which to measure the algorithm's performance.

In this model, the algorithm has access to *expert advice* in terms of additional information to aid in its predictions. The algorithm is provided with an input in the

form of advice from experts who are typically assumed to have unforgeable identities. The algorithm makes its prediction by either combining or choosing amongst this advice usually based on historical performance of the experts. In this case, we measure *regret* as the loss of the algorithm against the loss of some predefined benchmark, which is typically the best expert in hindsight or some fixed optimal weighted average of the experts' advice. The goal of the algorithm is to minimize regret. Throughout this exposition we assume that there are T rounds in total and n experts.

We take note of one peculiarity of this definition of regret. In this case, the comparison is not against the best expert or combination of experts in *each* round but rather across all rounds *in hindsight*. Again let us consider the mistake bound model. If we allow our benchmark to vary as the best expert *in each round*, any algorithm can incur $\geq T(1 - 1/n)$ expected regret. This could be achieved by simply assigning minimal (i.e., 0) loss to the expert who has least probability (i.e., $\leq 1/n$) of being chosen (*Blum and Mansour*, 2007a).

Now that we have established that our goal in online learning with expert advice is to do (almost) as well as the best expert in hindsight, let us consider a simple problem in this model. Keeping with the mistake bound model, suppose we have a scenario where the best expert in hindsight makes *no mistakes*. In their seminal work, *Littlestone and Warmuth* (1994) use the Halving Algorithm for this scenario. The Halving Algorithm utilizes a majority vote strategy as proposed in *Angluin* (1988). In every subsequent round, all those experts that have made a mistake in previous rounds are eliminated. This guarantees a regret, which in this case is also a true loss, of $O(\log n)$. If we now modify the model so as to allow the best expert to make mistakes, the same strategy will not work. The key insight in *Littlestone and Warmuth* (1994) however, is that we can replace this binary view of expert errors ('one mistake and you're out'!) by a more flexible notion of weights on experts. These weights essentially concretize the trustworthiness of an expert's advice based on

their historical performance when compared against the true outcomes. The resulting algorithm guarantees a regret of $O(\log n)$. Note that this regret is logarithmic in the number of experts and *independent of the number of rounds*.

So far, we have only considered models where the comparator was a single best expert. The next class of comparators is using a combination of expert advice as benchmark. In particular, *Littlestone et al.* (1991) use the best fixed linear combination of expert advice as benchmark. The key idea here is that rather than implementing weight updates on each expert in isolation, their weights are adjusted as a function of their marginal impact on the algorithm prediction; updating more aggressively for worse algorithm predictions. This allows them to achieve a bound of $O(\log n)$.

2.4.2 Online Learning Models for Recommender Systems

The models of online learning that we have proposed in Chapters V and VI were motivated by internet applications, especially recommender systems.

Consider an application where the expert advice arrives sequentially. This means that some dishonest experts may imitate the advice of earlier informative ones. It also means that the advice of later experts cannot be copied by earlier ones. In such applications, weeding out such cloning attacks is crucial to preserving the integrity of the system. Particularly, we want to weed out experts who may look artificially informative by cloning informative agents during initial rounds, and may exploit this trust in later rounds, thus causing large loss to the algorithm.

In particular, we consider the following recommendation problem in Chapter V: Consider a system that has to predict how attractive each of a set of items will be to a target user (or group of users). The system has access to advice from a set of experts, some of whom may actually be controlled by an attacker. Not all experts provide predictions on every item, and they need not provide them in a fixed order for every item. Importantly, the system has limited access to feedback on recommendations:

items that are not recommended highly might never be inspected by the target user. In Chapter V, we formally model this problem, and develop a prediction market-based learning algorithm for it. A full-information version of this problem has been studied by *Resnick and Sami* (2007). The algorithm we present is similar in structure to their algorithm (*Resnick and Sami*, 2007), but modified to get around the limitations of the partial monitoring feedback model. This chapter considers a myopic view of regret: we do not account for earlier dishonest experts misleading later informative ones. More formally, we assume that the aggregation of advice of a sequence of experts is lossless in that no information is lost in this aggregation. Note that this still allows for loss due to cloning, or bad predictions from malicious experts; however this is a strong assumption that we relax in our later work. We show that the algorithm we develop can achieve a myopic regret bound of $O(n\sqrt{T}\log T)$ as opposed to the regret bound of $O(n)$ in the full feedback case.

Motivated by real-world considerations of active attackers and passive community members, our model features a hybrid of adversarial attackers and stochastic community members. Since we separately bound damage caused by adversarial attackers and the information lost from informative members, we may be able to use this to our advantage. In particular, considerations of the experts' incentives to enter the system may drive the trade-off: it may be reasonable to assume that potential attackers will not enter the system unless they have significant influence. In this case, we might seek to keep the damage bound under this limit, while minimizing the information loss.

Prediction Market-based Learning Algorithms In internet applications, data can be modeled as arriving sequentially. We will now make a case for constructing prediction market-based learning algorithms in these settings.

Expert forecasts and recommendations in internet settings present the following

challenges: First, the motives of the individual experts are not always known. Some forecasters may provide best-effort forecasts, but in some cases the experts may have vested interests in manipulating the system. For such attackers, it is often easy to create a sizeable number of clones in order to manipulate the system. Thus a single malicious identity may control multiple experts. We argue that, for these domains, the best formal model of the set of experts is neither purely adversarial, nor purely stochastic, but a hybrid of the two. For experts with unknown motives, assuming that their advice is governed by a stochastic generative process would be unrealistic. On the other hand, for genuine best-effort experts, a stochastic model of predictions and associated loss is appropriate, and may lead to stronger performance guarantees.

Second, for any given item, advice from different experts often arrive haphazardly over time, and not all experts produce forecasts for each item. Critically, later forecasters may have access to information from earlier forecasts about the same event or item. Such a setting is vulnerable to cloning attacks, where a potentially harmful expert imitates the advice of a genuine, informative one. While this may be modeled by treating all experts as potentially adversarial, this adversarial model overlooks the fact that attackers cannot depend on future honest ratings. Thus the adversarial model may be too conservative for this scenario.

Further, a prediction may need to be made before all of the experts have reported their advice. As noted earlier, partial availability of expert advice is handled in prior work by modeling sleeping experts, who may be inactive in certain rounds. However, these algorithms cannot distinguish between genuine forecasters and clones, even though the clones are forced to make forecasts later than the genuine forecasters they copy.

Algorithms based on prediction markets are attractive for the particular features of the domains we are interested in, because of the following reasons: First, traders' budgets allow us to control the total net impact of a single identity. By coupling

traders' payoffs to the effects of their actions, and limiting their effect so that their budget is never negative, we can provide worst-case bounds against adversarial forecasters. Second, in a setting with honest agents but stochastic outcomes, a budget-proportional betting scheme (the Kelly criterion (*Kelly*, 1956)) leads to exponential growth in traders' budgets (in expectation), and thus the small initial budgets are not crippling to honest agents in the long run. Prediction markets can thus be naturally applied to the sequential forecasting setting. Traders' profits are based on the extent to which they change forecasts, thus ensuring that merely cloning previous information is not profitable.

Our approach involves designing a learning algorithm by tracking a budget for each trader, and simulating a prediction market. For each input, the algorithm carries out a simulated trade on the forecasters' behalf, and then later updates the budgets by treating received feedback as the prediction market outcomes.

We begin in the next chapter by presenting results on the design of cost function based prediction markets using exponential family distributions.

CHAPTER III

Exponential Family Markets

3.1 Introduction

In this chapter, we present generalized log market scoring rules based on exponential family distributions. We derive a class of cost function based market mechanisms from these scoring rules. This chapter is based on joint work with Jacob Abernethy, Sébastien Lahaie and Rahul Sami (*Abernethy et al.*, 2014b).

Prediction markets are aggregation mechanisms that allow market prices to be interpreted as predictive probabilities on an event. Each trader in the market is assumed to have some private information that he uses to make a prediction on the outcome of the event. Traders are allowed to report their beliefs by buying and selling securities whose ultimate payoff depends on the future outcome. This will affect the state of the market, thus updating the predictive probabilities for the event. Further, since the trades are executed sequentially, the trader may observe all past trades in the market and update his private beliefs based on this information. In this sense the market prices, which are in effect the prices at which the marginal trader is willing to buy or sell the available securities, can be interpreted as an aggregate "consensus probability forecast" of the event in question.

One popular form of prediction markets is the market scoring rule (*Hanson*, 2003a). A market scoring rule considers all trades as a single chronological sequence.

Traders earn rewards proportional to the incremental reduction in prediction loss (measured by the negative log of the prediction probability) caused by their trades in comparison to the previous trade. In other words, their rewards depend on the change in market probabilities caused by their trade, as well as on the eventual outcome. Thus, each trader has an incentive to minimize the prediction loss. In this format, the *market maker* who runs the market can suffer an overall loss, but *Hanson* (2003a) showed that, for market scoring rules on finite outcome spaces, the loss of the market maker can be bounded.

Much of the work on prediction market design has focused heavily on structural properties of the mechanism: incentive compatibility, the market maker loss, the available liquidity, the fluctuations of the prices as a function of the trading volume, to name a few. Absent from much of the literature is a corresponding *semantics* of the market behavior or the observed prices. That is, how can we interpret the equilibrium market state when we have a number of traders with diverse beliefs on the state of the world? How is the market an aggregation mechanism? Do price changes relate to our usual Bayesian notion of information incorporation via posterior updating?

In this chapter we show that a number of classical statistical tools can be leveraged to design a prediction market framework in the mold of *exponential family distributions*; we show that this statistical framework leads to a number of attractive properties and interpretations. Common concepts in statistics—including *entropy maximization*, *log loss*, and *Bayesian inference*—relate to natural aspects of our class of mechanisms. In particular, the central objects in our market framework can be interpreted via concepts used to define exponential families:

- the market's *payoff function* corresponds to the *sufficient statistics* of the distribution;
- the vector of *outstanding shares* in the market corresponds to the *natural parameter* of the distribution;

- the market prices correspond to *mean parameters*;
- the market's cost function corresponds to the distribution's *log-partition* function.

We start in Section 3.2 by reviewing exponential family distributions and some of their relevant properties. We then provide an overview of scoring rules and cost function prediction markets. In Section 3.5 we discuss scoring rules based on exponential family distributions, and we show how the framework leads to a variety of scoring rules for continuous outcome spaces. We turn our attention to market design in Section 3.6 and give a full description of our proposed mechanisms. In addition to showing the syntactic relationship between exponential families and prediction markets, we explore a number of rich semantic implications as well. In particular, we show that our formulation allows us to analyze the evolution of the market under various trader models:

- In Section 3.11 we analyze the expected payoff of both linear utility and exponential utility traders in this market.
- Trader behavior varies depending on how they assimilate information; for example, should we consider our agents as Bayesians or frequentists. In Section 3.7 we consider traders that use a conjugate prior to update their beliefs, and we study how their trades would affect the market state.
- In Section 3.8 we consider *risk-averse* agents that optimize their bets according to exponential utility. In this case we can characterize precisely how a single trader interacts with the market, as well as the equilibrium reached given multiple traders; the latter result is achieved via a potential game argument as detailed in Section 3.10. The eventual market state is a weighted combination of traders' beliefs and the initial state; the weights are proportional to risk aversion parameters.

- Surprisingly we are able to characterize the correspondence between trader beliefs and financial transactions in this market. In particular, we are able to show that a trader with prior exposure in the market can be understood as having updated his private belief. This means that the cost function market exposes a deep connection between beliefs and financial transactions: an agent with some exposure in the market is in effect equivalent to an agent with a different risk attitude. We provide details in Section 3.9.

- In Section 3.12 we consider *budget-limited traders* who are constrained in how much they influence the market. We analyze the market under these circumstances; we are able to show that traders with good information can expect to profit and their influence over the market state increases over time whereas malicious traders have limited impact on the market.

A note about play-money markets: Even in prediction markets set up with play-money, risk aversion is plausible since it captures the fact that a trader high on the leaderboard may not want to risk her standing with large late trades. Further, in such markets especially, budget constraints are key since they help alleviate the problem that traders can easily manipulate prices with unreasonable trades. Our results are therefore particularly relevant in markets with play-money.

3.1.1 Related Work.

The notion of an exponential family distribution is fundamental to this work. For comprehensive introductions to these distributions, see (*Barndorff-Nielsen*, 1978; *Wainwright and Jordan*, 2008). Exponential families are intimately tied to the notions of log loss and entropy, but can be generalized to other types of convex losses and information as shown by *Grünwald and Dawid* (2004), who also make a connection to scoring rules.

Scoring rules are a measure of prediction accuracy, and we are concerned here with scoring rules for statistic expectations, typically over infinite outcome spaces. Such rules have been characterized by *Savage* (1971); see also (*Abernethy and Frongillo*, 2012; *Gneiting and Raftery*, 2007; *Lambert et al.*, 2008). Our rules are of course special cases of this characterization, but it appears the range of elegant scoring rules that arise from exponential families has not been appreciated. Indeed, *Gneiting and Raftery* (2007) observe that specific instances of scoring rules for continuous outcomes are lacking, and survey various possibilities. Closer to our work, *Lambert et al.* (2008) characterize the properties of probability distributions that are elicitable and provide a representation theorem for such properties.

In a seminal paper, *Hanson* (2003a) showed how to form a prediction market based on a sequentially-shared scoring rule, and specifically proposed the logarithmic market scoring rule (LMSR) based on log loss for finite outcome spaces (*Hanson*, 2007). The markets we introduce are direct generalizations of the LMSR to continuous outcomes, but take the form of cost-function based markets as introduced by *Chen and Pennock* (2007). *Gao et al.* (2009) and *Chen et al.* (2013) also consider extending various market makers to infinite outcome spaces.

Prediction markets are known to perform well in practice (*Pennock and Sami*, 2007; *Pennock et al.*, 2001). However, a sound theory for interpreting trader behavior and market prices is an ongoing area of study (*Wolfers and Zitzewitz*, 2006; *Manski*, 2004). At one extreme, agents are assumed myopic and risk-neutral, implying they move the market state to their belief (*Chen and Vaughan*, 2010). At the other extreme, agents are strategic and the market fully incorporates all information (*Ostrovsky*, 2012). Strategic behavior in prediction markets has been previously addressed (*Chen et al.*, 2010; *Dimitrov and Sami*, 2008). The aggregation properties of market mechanisms have also been explored from a machine learning perspective (*Storkey*, 2011). More closely related to our work, *Frongillo and Reid* (2013) also

touch upon the statistical interpretations of prediction market costs and payoffs from the viewpoint of exponential families.

One of the aims of this work is to understand the behavior of cost-function prediction markets with risk-averse agents, a subject which has received only limited attention; the only work we are aware of is (*Frongillo et al.*, 2012, Sec. 3.1). However, risk aversion is a fundamental component of mathematical finance and portfolio optimization, and there are close connections between the notion of a cost function and that of a convex risk measure (*Föllmer and Schied*, 2002; *Föllmer and Knispel*, 2011). Indeed, they arise from the same axioms as noted by *Othman and Sandholm* (2011). We see the potential to draw more on the mathematical finance literature to take into account risk aversion, as prediction markets can be viewed simply as single-period financial markets (*Föllmer and Schied*, 2004, Part I).

Another goal of this work is to characterize the market state at equilibrium and its relationship to trader beliefs. Market based belief aggregation is considered extensively by Pennock and Wellman (*Pennock*, 1999; *Pennock and Wellman*, 1997). His work analyzes equilibrium in a market with Arrow-Debreu securities priced via a Walrasian auction. The equilibrium prices in the market are shown to correspond to the arithmetic and geometric means of the individual trader beliefs depending on the risk aversion model of the trader when the securities are on mutually exclusive events.

3.2 Exponential Family Distributions

We let $p(x;\mu)$ be the maximum entropy distribution with expected statistic μ. Specifically, it is the solution to the following program:[1]

$$\min_{p\in\mathcal{P}} F(p) \quad \text{s.t.} \quad \mathbf{E}_p[\phi(x)] = \mu, \tag{3.1}$$

where the objective function is the negative entropy of the distribution, namely

$$F(p) = \int_{x\in\mathcal{X}} p(x)\log p(x)\, d\nu(x).$$

Note that the explicit set of constraints in (3.1) are linear, whereas the objective is convex. We let $G : \mathcal{M} \to \mathbf{R}$ be the optimal value function of (3.1), meaning $G(\mu)$ is the negative entropy of the maximum entropy distribution with expected statistics μ.

It is well-known that solutions to (3.1) are *exponential family* distributions; see, for instance *Wainwright and Jordan* (2008). These are distributions whose densities with respect to ν take the form

$$p(x;\theta) = \exp(\langle\theta,\phi(x)\rangle - T(\theta)). \tag{3.2}$$

The density is stated here in terms of its *natural* parametrization $\theta \in \mathbf{R}^d$, where θ arises as the Lagrange multiplier associated with the linear constraints in (3.1). The term $T(\theta)$ essentially arises as the multiplier for the normalization constraint (the

[1] We assume that the minimum is finite and achieved for all $\mu \in \mathcal{M}$. Some care is needed to ensure this holds for specific statistics and outcome spaces. For example, taking outcomes to be the real numbers, there is no maximum entropy distribution with a given mean μ (one can take densities tending towards the uniform distribution over the reals), but there is always a solution if we constrain both the first and second moments.

density must integrate to 1), and so ensures that (3.2) is normalized:

$$T(\theta) = \log \int_{\mathcal{X}} \exp\langle \theta, \phi(x) \rangle \, d\nu(x). \tag{3.3}$$

The function T is known as the *log-partition* or *cumulant* function corresponding to the exponential family. Its domain is $\Theta = \{\theta \in \mathbf{R}^d : T(\theta) < +\infty\}$, called the natural parameter space, and we assume throughout that it is nonempty.[2] The exponential family is *regular* if Θ is open—almost all exponential families of interest, and all those we consider in this work, are regular. The family is *minimal* if there is no $\alpha \in \Theta$ such that $\langle \alpha, \phi(x) \rangle$ is a constant over $\mathcal{X}$ (ν-almost everywhere); minimality is a property of the associated statistic ϕ, usually called the *sufficient statistic* in the literature.

What exactly is a *sufficient statistic*? A statistic is just a function of the data. If the data is drawn from some distribution parameterized by θ then a statistic is called *sufficient* if no other statistic that can be computed from the data gives you more information about θ. For instance the number of heads in a set of Bernoulli trials gives you everything you need in order to compute a joint distribution on the trial outcomes. In particular if there are n trials and k heads, it is not necessary to know exactly when the heads occurred in order to compute the probability of that sequence (which is always $\frac{1}{\binom{n}{k}}$ regardless of the success probability or the particular order of the sequence.).

Some commonly studied distributions that are in fact exponential families include the binomial, beta, Poisson, exponential, and normal distributions; the sufficient statistics and parametrizations for the normal will be covered in Section 3.5.2.

[2] This may impose additional conditions on the choice of base measure ν in certain special cases. For instance, if the density over $\mathbf{R}$ is known to have unit variance and statistic $\phi(x) = x$, then one uses the base measure $\nu(x) = e^{-x^2/2}$ leading to a normal distribution with fixed variance (*Barndorff-Nielsen*, 1978).

3.2.1 Some Properties of Exponential Families

We will now rederive, for completeness, some interesting results about exponential families. For a more complete treatment, see *Wainwright and Jordan* (2008).

Theorem 3.2.1. The log partition function

$$T(\theta) = \log \int_{\mathcal{X}} \exp\langle \theta, \phi(x) \rangle \, d\nu(x)$$

is convex

Proof. First we will show that $\mathrm{E}[\phi(\mathrm{x})] = \nabla \mathrm{T}(\theta)$ and $var[\phi(x)] = \nabla^2 T(\theta)$

$$\begin{aligned}
\nabla T(\theta) &= \nabla \log \int \exp[\phi(x)\theta] \, dx \\
&= \frac{\int \phi(x) \exp[\phi(x)\theta] \, dx}{\int \exp[\phi(x)\theta] \, dx} \\
&= \int \phi(x) \exp\left(\phi(x)\theta - \log \int \exp[\phi(x)\theta] \, dx] \right) dx \\
&= \mathrm{E}[\phi(\mathrm{x})]
\end{aligned}$$

$$
\begin{aligned}
\nabla^2 T(\theta) &= \nabla \frac{\int \phi(x) \exp[\phi(x)\theta]\, dx}{\exp[T(\theta)]} \\
&= \frac{\exp[T(\theta)] \nabla \left(\int \phi(x) \exp[\phi(x)\theta]\, dx \right)}{\left(\exp[T(\theta)]\right)^2} \\
&\quad - \frac{\int \phi(x) \exp[\phi(x)\theta]\, dx \nabla \left(\int \exp[\phi(x)\theta]\, dx \right)}{\left(\exp[T(\theta)]\right)^2} \\
&= \frac{\nabla \left(\int \phi(x) \exp[\phi(x)\theta]\, dx \right)}{\exp[T(\theta)]} - \frac{\int \phi(x) \exp[\phi(x)\theta]\, dx \nabla \left(\int \exp[\phi(x)\theta]\, dx \right)}{\left(\exp[T(\theta)]\right)^2} \\
&= \int \phi(x)\phi(x)^T \exp[\phi(x)\theta - T(\theta)]\, dx \\
&\quad - \frac{\int \phi(x) \exp[\phi(x)\theta]\, dx \left(\int \phi(x) \exp[\phi(x)\theta]\, dx \right)}{\left(\exp[T(\theta)]\right)^2} \\
&= \int \phi(x)\phi(x)^T \exp[\phi(x)\theta - T(\theta)]\, dx \\
&\quad - \int \phi(x) \exp[\phi(x)\theta - T(\theta)]\, dx \left(\int \phi(x) \exp[\phi(x)\theta - T(\theta)]\, dx \right) \\
&= \mathrm{E}_\theta[\phi(\mathrm{x})\phi(\mathrm{x})^{\mathrm{T}}] - (\mathrm{E}_\theta[\phi(\mathrm{x})]\mathrm{E}_\theta[\phi(\mathrm{x})]) \\
&= var[\phi(x)]
\end{aligned}
$$

Note that $var[\phi(x)] \geq 0$. Since the Hessian of $T(\theta)$ is always positive-semidefinite, it follows that it is convex. □

Consider the convex conjugate of the log partition function, $T^*(\mu)$ defined as

$$T^*(\mu) = \sup_\theta \theta \cdot \mu - C(\theta)$$

This supremum is obtained at the value of θ for which $\mu = \nabla T(\theta)$; that is the natural parameter θ for which $\mu = \mathrm{E}_{\mathrm{p}(\cdot|\theta)}[\phi(\mathrm{x})]$ is the mean parameter. Rewriting,

$$T^*(\mathrm{E}_{\mathrm{p}_\theta}[\phi(\mathrm{x})]) = \theta \cdot \mathrm{E}_{\mathrm{p}(\cdot|\theta)}[\phi(\mathrm{x})] - \mathrm{T}(\theta) \tag{3.4}$$

Thus, the mean parameters are the dual variables to the natural parameters.

Theorem 3.2.2. The value of the convex conjugate of the log partition function is the negative entropy of the exponential family distribution obtained from backward mapping the mean parameters.

Proof. To see this, we note that for $p(x) = \exp\{\theta \cdot \phi(x) - C(\theta)\}$

$$\begin{aligned} -H(p) &= \int_x p(x) \log p(x)\ dx \\ &= \int_x p(x)[\theta \cdot \phi(x) - T(\theta)]\ dx \\ &= \theta \cdot \int_x p(x)[\phi(x)]\ dx - \int_x p(x)T(\theta)\ dx \\ &= \theta \cdot \mathrm{E_p}[\phi(\mathrm{x})] - \mathrm{T}(\theta) \end{aligned}$$

As shown in equation 3.4, this is exactly the expression for the dual of the cost function of the exponential family market maker. □

Theorem 3.2.3. Negative differential entropy $-H(p) \stackrel{\text{def}}{=} \int_x p(x) \log p(x) dx$ is unbounded from above for an exponential family distribution.

Proof. Note that, for an exponential family distribution

$$\begin{aligned} H(p) &= -\int_x p(x) \log p(x) dx \\ &= -\int_x p(x)[\beta \cdot \phi(x) - T(\beta)] dx \\ &= -\beta \cdot \mathrm{E}[\phi(\mathrm{x})] + \mathrm{T}(\beta) \end{aligned}$$

If the range of $\phi(x)$ is unbounded, the negative differential entropy is unbounded as well. □

The following proposition collects the relevant results on regular exponential families; proofs may be found in *Wainwright and Jordan* (2008, Prop. 3.1–3.2, Thm. 3.3–3.4) and see also *Banerjee et al.* (2005a, Lem. 1, Thm. 2). A convex function T is of *Legendre type* if it is proper, closed, strictly convex and differentiable on the interior of its domain, and $\lim_{\theta \to \bar{\theta}} \|\nabla T(\theta)\| = +\infty$ when $\bar{\theta}$ lies on the boundary of the domain.

Proposition III.1. *Consider a regular exponential family with minimal sufficient statistic. Let T^* denote the convex conjugate of T, which here can be evaluated as $T^*(\mu) = \sup_{\theta \in \Theta} \langle \theta, \mu \rangle - T(\theta)$. Similarly, $G^*(\theta) = \sup_{\mu \in \mathcal{M}} \langle \theta, \mu \rangle - G(\mu)$. The following properties hold:*

1. *T and G are of Legendre type, and $T = G^*$ (equivalently $G = T^*$).*
2. *The gradient map ∇T is one-to-one and onto the interior of $\mathcal{M}$. Its inverse is ∇G which is one-to-one and onto the interior of Θ.*
3. *The exponential family distribution with natural parameter $\theta \in \Theta$ has expected statistic $\mu = \mathbf{E}_p[\phi(x)] = \nabla T(\theta)$.*
4. *The maximum entropy distribution with expected statistic μ is the exponential family distribution with natural parameter $\theta = \nabla G(\mu)$.*

3.2.2 Example: The Gaussian Distribution

Consider the normal distribution $\mathcal{N}(\mu, \sigma)$ where μ is the mean and σ^2 is the variance of the distribution as usual.

Log partition function and parametrizations

The natural parameters $\boldsymbol{\beta} = (\beta_1, \beta_2)$ can be written in terms of μ and σ as

$$\beta_1 = \frac{\mu}{\sigma^2}, \quad \beta_2 = \frac{-1}{2\sigma^2}$$

and the log partition function is

$$T(\boldsymbol{\beta}) = -\frac{\beta_1^2}{4\beta_2} - \frac{1}{2}\log(-2\beta_2)$$

Alternately, the log partition function can be written in terms of its variance and mean as $\frac{\mu^2}{2\sigma^2} + \log\sigma$. Also note that the mean parameters are μ and $\mu^2 + \sigma^2$.

Convex conjugate of the log partition function

We will now derive an expression for the dual of the log partition function for the Gaussian distribution. In this case, β is a 2-dimensional vector. Let $\beta = \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix}$ and $\mu = \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix}$. Rewriting the the expression for a normal distribution allows us to determine the natural parameters and the closed form expression for the log partition function. Since the gradient of the log partition function defines a one-to-one mapping to the mean parameters, we have

$$\begin{aligned} \boldsymbol{\mu} &= \nabla T(\boldsymbol{\beta}) \\ &= \nabla\left(-\frac{\beta_1^2}{4\beta_2} - \frac{1}{2}\log(-2\beta_2)\right) \\ &= \begin{pmatrix} -\frac{\beta_1}{2\beta_2} \\ \frac{\beta_1^2}{4\beta_2^2} - \frac{1}{2\beta_2} \end{pmatrix} \end{aligned}$$

Note that $\mu_2 = \mu_1^2 - \frac{1}{2\beta_2}$. Thus, $\boldsymbol{\beta}$ can be written in terms of $\boldsymbol{\mu}$ as follows: $\beta_1 = \frac{\mu_1}{\mu_2 - \mu_1^2}$ and $\beta_2 = \frac{1}{2(\mu_1^2 - \mu_2)}$. The dual of the log partition function $T^*(\boldsymbol{\mu}) = \sup_{\boldsymbol{\beta}} \boldsymbol{\beta}\cdot\boldsymbol{\mu} - T(\boldsymbol{\beta})$ may be expressed solely in terms of the mean parameters. To see this, observe that there is a closed form expression for $T(\boldsymbol{\beta})$ in terms of $\boldsymbol{\beta}$ which itself can be expressed in terms of $\boldsymbol{\mu}$. This leads to the following closed form expression for the dual of the

log partition function:

$$T^*(\mu) = -\frac{1}{2} - \frac{1}{2}\log(\mu_2 - \mu_1^2)$$

3.3 Scoring Rules and Market Scoring Rules

As far back as the 1950's researchers were interested in the question of incentivizing truthful reporting from agents (*Brier*, 1950) by assigning numerical scores to them based on their forecasts of future events. In fact it can be shown that the certain scoring rules like the quadratic and log scoring rules would require an agent to truthfully report his belief, if he is to maximize his expected score. Such scoring rules where the report that maximizes expected score is in fact the belief of the agent, are called *proper scoring rules*. It turns out that there are in fact a class of scoring rules that have this property. In this chapter we will study one of these in detail.

A key insight by *Hanson* (2003a) was that we could leverage this property of proper scoring rules to not only elicit information from one agent but also pool opinions from a crowd. He proposed a sequential mechanism where the score assigned to an agent is the difference between his score and the preceding agent's score. Trades are done through a central authority called a market maker.

3.4 Cost Function Prediction Market

It turns out that if you take an axiomatic approach to construct the market maker, you arrive at an alternate formulation of the market mechanism called the cost function-based prediction market. In this setup, the market maker decides to issue a finite number of securities each of which is guaranteed to pay off some amount dependent on the outcome of the event under consideration. We call this the payoff function and we represent it as $\phi(x)$ where x is the revealed outcome and the dimensionality of the range of ϕ matches the number of issued securities. Thus, when an

outcome x is revealed, one share of the security i pays off the amount given by the i^{th} dimension of $\phi(x)$. The market maker sets prices for the securities based on some potential function that takes as input the total number of shares of each of the securities collectively held by the trading population. This potential function is called the cost function $C(\cdot)$ of the prediction market and the cost to a trader of purchasing $\mathbf{q}$ shares when the current market state is $\mathbf{q}_0$ is given by $C(\mathbf{q}+\mathbf{q}_0)-C(\mathbf{q}_0)$. When the outcome is revealed the trader will thus make a net profit of $\mathbf{q} \cdot \phi(x) - (C(\mathbf{q}+\mathbf{q}_0) - C(\mathbf{q}_0))$

In a prediction market, an agent's expected belief μ is elicited indirectly through the purchase and sale of securities. Under this approach, each component i of the statistic ϕ is interpreted as the payoff function of a security; that is, a single share of security i pays off $\phi_i(x)$ when $x \in \mathcal{X}$ occurs. Thus if the vector of shares held by the agent (her *portfolio*) is $\delta \in \mathbf{R}^d$, where entry δ_i corresponds to the number of shares of security i, then the payoff to the agent when x occurs is the inner product $\langle \delta, \phi(x) \rangle$.

To be concrete, in the classic finite-outcome case the statistic has a component for each outcome x such that $\phi_x(x') = 1$ if $x' = x$ and 0 otherwise. Therefore the corresponding security pays 1 dollar if outcome x occurs. (These are known as Arrow-Debreu securities.)

The standard way to implement a prediction market in the literature, due to *Chen and Pennock* (2007), is via a centralized market maker. The market maker maintains a convex, differentiable cost function $C : \mathbf{R}^d \to (-\infty, +\infty]$, where $C(\theta)$ records the revenue collected when the vector of outstanding shares is θ. The cost to an agent of purchasing portfolio δ under a market state of θ is $C(\theta + \delta) - C(\theta)$, and therefore the instantaneous prices of the securities are given by the gradient $\nabla C(\theta)$.

A risk-neutral agent will choose to acquire shares up to the point where, for each share, expected payoff equals marginal price. Formally, if the agent acquires portfolio

δ, moving the market state vector to $\theta' = \theta + \delta$, then we must have

$$\mathbf{E}_p[\phi(x)] = \nabla C(\theta'). \tag{3.5}$$

In this way, by its choice of δ, the agent reveals that its expected belief is $\mu = \nabla C(\theta')$. We stress that this observation relies on the assumptions that 1) the agent is risk-neutral, 2) the agent does not incorporate the market's information into its own beliefs, and 3) the agent is not budget constrained. We will examine relaxations of each assumption in later sections.

3.5 Generalized Log Market Scoring Rule

Suppose that an agent holds a belief in the expected value of some function of the random variable x. The maximum entropy distribution that is consistent with these beliefs is an exponential family distribution.

We consider a measurable space consisting of a set of (mutually exclusive, exhaustive) outcomes $\mathcal{X}$ together with a σ-algebra $\mathcal{F}$. An agent or expert has a *belief* over potential outcomes taking the form of a probability measure absolutely continuous with respect to a base measure ν.[3] Throughout we represent the belief as the corresponding density p with respect to ν. Let $\mathcal{P}$ denote the set of all such probability densities.

We are interested in eliciting information about the agent's belief, in particular expectation information. Let $\phi : \mathcal{X} \to \mathbf{R}^d$ be a vector-valued random variable or *statistic*, where d is finite. The aim is to elicit $\mu = \mathrm{E_p}[\phi(\mathrm{x})]$ where x is the random

[3]Recall that a measure P is absolutely continuous with respect to ν if $P(A) = 0$ for every $A \in \mathcal{F}$ for which $\nu(A) = 0$. In essence the base measure ν restricts the support of P. In our examples ν will typically be a restriction of the Lebesgue measure for continuous outcomes or the counting measure for discrete outcomes.

outcome. A *scoring rule* is a device for this purpose. Let

$$\mathcal{M} = \left\{\mu \in \mathbf{R}^d : \mathbf{E}_p[\phi(x)] = \mu, \text{ for some } p \in \mathcal{P}\right\}$$

be the set of realizable statistic expectations. Unless otherwise mentioned, all integrals including expectations are taken with respect to base measure ν, which is therefore implicit in many of the formulas. A scoring rule $S : \mathcal{M} \times \mathcal{X} \to \mathbf{R} \cup \{-\infty\}$ pays the agent $S(\hat{\mu}, x)$ according to how well its report $\hat{\mu} \in \mathcal{M}$ agrees with the eventual outcome $x \in \mathcal{X}$. The following definition is due to *Lambert et al.* (2008).

Definition III.2. A scoring rule S is *proper* for statistic ϕ if for each $\mu \in \mathcal{M}$ and $p \in \mathcal{P}$ with expected statistic μ, we have for all $\hat{\mu} \neq \mu$

$$\mathbf{E}_p[S(\mu, x)] \geq \mathbf{E}_p[S(\hat{\mu}, x)]. \tag{3.6}$$

Given a proper scoring rule S, any affine transformation $\tilde{S}(\mu, x) = aS(\mu, x) + b(x)$ of the rule, with $a > 0$ and b an arbitrary real-valued function of the outcomes, again yields a proper scoring rule termed *equivalent* (*Dawid*, 1998; *Gneiting and Raftery*, 2007). Throughout we will implicitly apply such affine transformations to obtain the clearest version of the scoring rule. We will also focus on scoring rules where inequality (3.6) is strict to avoid trivial cases such as constant scoring rules.

Classically, scoring rules take in the entire density p rather than just some statistic, and incentive compatibility must hold over all of $\mathcal{P}$. When the outcome space is large or infinite, it is not feasible to directly communicate p, so the definition allows for summary information of the belief.

Note that Definition III.2 places only mild information requirements on the part of the agent to ensure truthful reporting. Because condition (3.6) holds for all p consistent with expectation μ, it is enough for the agent to simply know the latter and not the complete density to be properly incentivized. However, the agent must

also agree with the support of the density as implicitly defined by base measure ν.

3.5.1 Proper Scoring from Maximum Entropy

Our starting point for designing proper scoring rules is the classic logarithmic scoring rule for eliciting probabilities in the case of finite outcomes. This rule is simply $S(p, x) = \log p(x)$, namely we take the log likelihood of the reported density at the eventual outcome. To generalize the rule to expected statistics rather than full densities, we consider a subset of densities $\mathcal{D} \subseteq \mathcal{P}$. If $\mathcal{D}$ and $\mathcal{M}$ are bijective, then we say that $\mathcal{M}$ parametrizes $\mathcal{D}$ and write $p(\cdot\,; \mu)$ for the density mapping to μ. Given such a family parametrized by the relevant statistics, the generalized log scoring rule is then

$$S(\mu, x) = \log p(x; \mu). \tag{3.7}$$

Even though the log score is only applied to densities from $\mathcal{D}$, according to Definition III.2 it must work over all densities in $\mathcal{P}$. It turns out this is possible if $\mathcal{D}$ is chosen appropriately, drawing on a well-known duality between maximum likelihood and maximum entropy (*Grünwald and Dawid*, 2004).

Proper Log Scoring

We are now in a position to analyze the log scoring rule under exponential family distributions. From our discussion so far, we have that an exponential family density can be parametrized either by the natural parameter θ, or by the mean parameter μ, and that the two are related by the invertible gradient map $\mu = \nabla T(\theta)$. We will write $p(x; \theta)$ or $p(x; \mu)$ given the parametrization used.

The following observation is crucial. Let $\tilde{p} \in \mathcal{P}$ be any arbitrary density with expected statistic μ, let $p(\cdot\,; \mu)$ be the exponential family with the same expected

statistic, and let $\hat{\mu} \in \mathcal{M}$ be an alternative report. Then from (3.2) we have

$$\mathbf{E}_{\tilde{p}}[\log p(x;\hat{\mu})] = \mathbf{E}_{p(\cdot;\mu)}[\log p(x;\hat{\mu})] = \langle \hat{\theta}, \mu \rangle - T(\hat{\theta}), \tag{3.8}$$

where $\hat{\theta} = \nabla G(\hat{\mu})$ is the natural parameter for the exponential family with statistic $\hat{\mu}$. Note that the expected log score does not depend on the entire maximum entropy distribution but just its expected statistic μ. This is how we can achieve proper scoring according to Definition III.2.

Theorem III.3. *Consider the logarithmic scoring rule $S(\mu, x) = \log p(x;\mu)$ defined over a set of densities $\mathcal{D}$ parametrized by $\mathcal{M}$. The scoring rule is proper if and only if $\mathcal{D}$ is the exponential family with statistic ϕ, where $\mu = \mathrm{E}_{\mathrm{p(x;\mu)}}[\phi(\mathrm{x})]$.*

Proof. Let $\mu, \hat{\mu} \in \mathcal{M}$ be the agent's true belief and an alternative report, and let $p \in \mathcal{P}$ be a density consistent with μ. Let $\theta = \nabla G(\mu)$ and $\hat{\theta} = \nabla G(\hat{\mu})$, and note that $\mu = \nabla T(\theta)$. We have

$$\begin{aligned} \mathbf{E}_p[\log p(x;\mu)] - \mathbf{E}_p[\log p(x;\hat{\mu})] &= \langle \theta, \mu \rangle - T(\theta) - \langle \hat{\theta}, \mu \rangle + T(\hat{\theta}) \\ &= T(\hat{\theta}) - T(\theta) - \langle \hat{\theta} - \theta, \mu \rangle \\ &= T(\hat{\theta}) - T(\theta) - \langle \hat{\theta} - \theta, \nabla T(\theta) \rangle. \end{aligned} \tag{3.9}$$

The latter is positive by the strict convexity of T, which shows that the log score is proper. For the converse, assume the defined log score is proper. By the Savage characterization of proper scoring rules for expectations (see *Abernethy and Frongillo* (2012, Thm. 11)), we must have $S(\mu, x) = G(\mu) - \langle \nabla G(\mu), \mu - \phi(x) \rangle$ for some strictly convex function G. Let $T = G^*$, so that $\nabla G = \nabla T^{-1}$, and let $\theta = \nabla G(\mu)$. Then the

above can be written as

$$\begin{aligned}\log p(x;\mu) &= G(\mu) - \langle \nabla G(\mu), \mu - \phi(x) \rangle \\ &= \langle \theta, \mu \rangle - T(\theta) - \langle \theta, \mu - \phi(x) \rangle = \langle \theta, \phi(x) \rangle - T(\theta),\end{aligned}$$

which shows that $p(x;\mu)$ takes the form of an exponential family. □

It has been understood since (*McCarthy*, 1956; *Savage*, 1971) that scoring rules for densities and expectations can be characterized in terms of an underlying convex function. The generalized log scoring rule of Theorem III.3 obtains by applying the modern characterization of *Abernethy and Frongillo* (2012, Thm. 11) to the optimal value function G (negative maximum entropy). *Banerjee et al.* (2005b, Thm. 6) prove a similar result by showing a bijection between exponential families and Bregman divergences.

The notion of a Bregman divergence in fact provides further intuition for the result. Note that (3.9) is the definition of the Bregman divergence with respect to strictly convex function T, written D_T. Therefore we have

$$\mathbf{E}_p[\log p(x;\mu)] - \mathbf{E}_p[\log p(x;\hat{\mu})] = D_T(\hat{\theta}, \theta) = D_G(\mu, \hat{\mu}),$$

where the last equality is a well-known identity relating the Bregman divergences of T and $T^* = G$ as proved below.

Proposition III.4. *Let f be a convex function and f^* be its conjugate dual. Let x_1, x_2 and y_1, y_2 be the corresponding dual variables. Then*

$$D_f(x_1, x_2) = D_{f^*}(\nabla f(x_2), \nabla f(x_1))$$

where D is the Bregman Divergence.

Proof. First note that from definition

$$f^*(\nabla f(x)) = x \cdot \nabla f(x) - f(x)$$

$$\begin{aligned}
D_{f^*}(\nabla f(x_2), \nabla f(x_1)) &= f^*(\nabla f(x_2)) - f^*(\nabla f(x_1)) - \nabla f^*(\nabla f(x_1))(\nabla f(x_2) - \nabla f(x_1)) \\
&= x_2 \cdot \nabla f(x_2) - f(x_2) - x_1 \cdot \nabla f(x_1) + f(x_1) \\
&\quad -\nabla f(x_2)\nabla f^*(\nabla f(x_1)) + \nabla f(x_1)\nabla f^*(\nabla f(x_1)) \\
&= x_2 \cdot \nabla f(x_2) - f(x_2) - x_1 \cdot \nabla f(x_1) + f(x_1) - x_1\nabla f(x_2) + x_1\nabla f(x_1) \\
&= f(x_1) - f(x_2) - \nabla f(x_2)(x_1 - x_2)
\end{aligned}$$

□

The equation states that the agent's regret from misreporting its mean parameter does not depend on the full density p, only the mean μ.

3.5.2 Examples: Moments over the Real Line

Theorem III.3 leads to a straightforward procedure for constructing score rules for expectations. Define the relevant statistic, and consider the maximum entropy (equivalently, exponential family) distribution consistent with the agent's reported mean μ. The scoring rule compensates the agent according to the log likelihood of the eventual outcome according to this distribution. The interpretation is that the agent is only providing partial information about the underlying density, so the principal first infers a full density according to the principle of maximum entropy, and then scores the agent using the standard log score. We stress that the exponential families framework is a tool in the construction of scoring rules at this point; we are not actually modeling any agent's belief via an exponential family.

An advantage of this generalization of the log score is that, for many domains

(multi-dimensional included) and expectations of interest, it leads to novel closed-form scoring rules. By examining the log densities of various exponential families, we can for instance obtain scoring rules for several different combinations of the arithmetic, geometric, and harmonic means, as well as higher order moments. The following examples illustrate the construction. Here, we have used μ and σ for the true mean and variance and $\hat{\mu}$ and $\hat{\sigma}$ for the elicited mean and variance respectively (and $\hat{\Sigma}$ for the covariance matrix of the multivariate normal).

Example III.5. As a base measure we take the counting measure over the finite set $\{1, 2, \ldots, d\}$, and we consider the statistic $\phi(i) \in \{0, 1\}^d$ that maps outcome i to the unit vector with component i equal to 1. The expectation of $\phi(i)$ is simply the entire probability distribution p, which is a multinomial distribution (an instance of an exponential family). We recover the standard log scoring rule $S(\hat{p}, i) = \log \hat{p}(i)$.

Example III.6. As a base measure we take the Lebesgue over the real numbers $\mathbf{R}$. We are interested in eliciting the mean μ and variance σ^2, so as a statistic we take $\phi(x) = (x, x^2)$ for which $\mathbf{E}_p[\phi(x)] = (\mu, \mu^2 + \sigma^2)$. The max entropy distribution for a given mean and variance is the Gaussian, whose log density gives the scoring rule

$$S((\hat{\mu}, \hat{\sigma}^2), x) = -\frac{(x - \hat{\mu})^2}{\hat{\sigma}^2} - \log \hat{\sigma}^2. \tag{3.10}$$

Again, we stress that this scoring rule elicits the mean and variance of any density over $\mathbf{R}$, not just those of a normal distribution. The construction easily generalizes to a multi-dimensional outcome space by taking the log density of the multivariate normal:

$$S((\hat{\mu}, \hat{\Sigma}), x) = -(x - \hat{\mu})' \hat{\Sigma}^{-1} (x - \hat{\mu}) - \log |\hat{\Sigma}|. \tag{3.11}$$

Here the statistics being elicited are the mean vector μ and the covariance matrix Σ. These scoring rules have been studied by *Dawid and Sebastiani* (1999) as rules that only depend on the mean and variance of the reported density. They note that these

rules are weakly proper (because they do not distinguish between densities with the same first and second moments), but do not make the point that knowledge of the full density is not necessary on the part of the agent.

In the above, Example III.6 illustrates an important point about parametrizations of the elicited expectations. The variance σ^2 cannot be written as $\mathbf{E}[\phi(x)]$ for any ϕ.[4] Instead one must use the first two *uncentered* moments $\mathbf{E}[x]$ and $\mathbf{E}[x^2]$. These are in bijection with μ and σ^2, so the resulting scoring rule can be re-written in terms of the latter. Therefore, it is possible to elicit not just expectations but also bijective transformations of expectations.

3.6 Exponential Family Markets

In a single-agent setting, a scoring rule is used to *elicit* the agent's belief. In a multi-agent setting, a prediction market can be used to *aggregate* the beliefs of the agents. In his seminal paper *Hanson* (2003a) introduced the idea of a market scoring rule, which inherits the appealing elicitation and aggregation properties of both in order to perform well in thin or thick markets. In this section, we adapt the generalized log scoring rule to a market scoring rule which leads to markets with simple closed-form cost functions for many statistics of interest.

In the remainder of this chapter we focus on the following cost function, which arises from the generalized logarithmic market scoring rule (LMSR):

$$C(\theta) = \log \int_{x \in \mathcal{X}} \exp\langle \theta, \phi(x) \rangle \, d\nu(x). \tag{3.12}$$

This is exactly the log-partition function (3.3) for the exponential family with sufficient statistic ϕ, and we recover the classic LMSR using outcome indicator vec-

[4]This is an intuitive (but far from formal) explanation for the fact that the dimension of the message space, or *elicitation complexity*, for eliciting the variance is at least 2 (*Lambert et al.*, 2008).

tors as statistics. Because an agent would never select a portfolio with infinite cost, the effective domain (i.e., the possible vectors of outstanding shares) of C is $\Theta = \{\theta \in \mathbf{R}^d : C(\theta) < +\infty\}$, which gives an economic interpretation to the natural parameter space of an exponential family.

The correspondence between the cost function (3.12) and the log-partition function (3.3) suggests the following interpretation. The market maker maintains an exponential family distribution over the state space $\mathcal{X}$ parametrized by share vectors that lie in Θ. When an agent buys shares, it moves the distribution's natural parameter so that the market prices matches its beliefs, or in other words the market's mean parametrization matches the agent's expectation.

There is a well-known duality between scoring rules and cost-function based markets (*Abernethy et al.*, 2013; *Hanson*, 2003a). In our context, recall from (3.8) that

$$\mathbf{E}_{\tilde{p}}[\log p(x; \hat{\mu})] = \langle \hat{\theta}, \mu \rangle - T(\hat{\theta})$$

where $\tilde{p}$ is the agent's belief and $\hat{\mu}$ the agent's report. The expected log score from reporting $\hat{\mu}$ is exactly the same as the expected payoff from buying portfolio of shares $\hat{\theta} = \nabla C(\hat{\mu})$ (assuming an initial market state of 0), as $\langle \hat{\theta}, \mu \rangle$ is the expected revenue and $T(\hat{\theta})$ is the cost. As in Section 3.5 this reasoning relies on the assumption of risk-neutrality, not on any specific form for the agent's belief.

3.6.1 Example: Gaussian Market

For the normal distribution $\mathcal{N}(\mu, \sigma)$, the natural parameters $\boldsymbol{\beta} = (\beta_1, \beta_2)$ can be written in terms of μ and σ as

$$\beta_1 = \frac{\mu}{\sigma^2}, \quad \beta_2 = \frac{-1}{2\sigma^2}$$

and the log partition function is

$$T(\boldsymbol{\beta}) = -\frac{\beta_1^2}{4\beta_2} - \frac{1}{2}\log(-2\beta_2)$$

Alternately, the log partition function can be written in terms of its variance and mean as $\frac{\mu^2}{2\sigma^2} + \log\sigma$. Also note that the mean parameters of the Gaussian are μ and $\mu^2 + \sigma^2$; thus the price of the securities correspond to the mean and sum of the square of the mean and variance of the Gaussian.

Note that because of the peculiarity of the cost function of the Gaussian market maker, the second dimension of the share vector is always negative for a valid distribution. Thus, the security corresponding to this dimension always has more share sold than bought.

3.6.2 Loss of the market maker

The loss of the exponential family market maker can be written in terms of the conjugate dual of the cost function. First we derive an expression for the conjugate dual C^* in terms of the primal variables. Recall the definition of the conjugate dual:

$$C^*(\mu) = \sup_q q \cdot \mu - C(q)$$

The supremum is achieved at q' such that $\nabla C(q') = \mu$. So we may rewrite:

$$C^*(\nabla C(q')) = \sup_q q \cdot \nabla C(q') - C(q)$$

This supremum is achieved at q such that $\nabla C(q') = \nabla C(q)$. One such value of q is q'. So we have

$$C^*(\nabla C(q')) = q' \cdot \nabla C(q') - C(q')$$

Also, recall that $\nabla C^*(\nabla C(q)) = q$ for the exponential family market.

Let q_0 be the initial and q_f the final market state. Then if μ is the expected value of the outcome sufficient statistics (*i.e.*the mean parameter) under the true distribution, the loss of the exponential family market maker can be written as $\phi(x)(q_f - q_0) - C(q_f) + C(q_0)$ where $\phi(x)(q_f - q_0)$ is the net payoff to the traders, and $-C(q_f) + C(q_0)$ is the net cost charged to the traders. This can be rewritten as:

$$\begin{aligned}
\phi(x)(q_f - q_0) - C(q_f) + C(q_0) &= \phi(x)(q_f - q_0) - q_f \nabla C(q_f) \\
&\quad + C^*(\nabla C(q_f)) + q_0 \nabla C(q_0) - C^*(\nabla C(q_0)) \\
&= q_f(\phi(x) - \nabla C(q_f)) + C^*(\nabla C(q_f)) \\
&\quad - q_0(\phi(x) - \nabla C(q_0)) - C^*(\nabla C(q_0)) \\
&= -C^*(\nabla C(q_0)) + C^*(\phi(x)) - q_0(\phi(x) - \nabla C(q_0)) \\
&\quad + C^*(\nabla C(q_f)) - C^*(\phi(x)) + q_f(\phi(x) - \nabla C(q_f)) \\
&= C^*(\phi(x)) - C^*(\nabla C(q_0)) \\
&\quad - \nabla C^*(\nabla C(q_0))(\phi(x) - \nabla C(q_0)) \\
&\quad - [C^*(\phi(x)) - C^*(\nabla C(q_f)) \\
&\qquad - \nabla C^*(\nabla C(q_f))(\phi(x) - \nabla C(q_f))] \\
&= D_{C^*}[\phi(x), \nabla C(q_0))] - D_{C^*}[\phi(x), \nabla C(q_f))]
\end{aligned}$$

Remark. Recall that the LMSR is essentially a special case applied to a multinomial distribution. The LMSR is known to have bounded ($\log n$) market maker loss. Thus, while in general the exponential family LMSR does not guarantee bounded market maker loss, for some special cases it can.

Example: Loss of the Gaussian Market Maker Let's now work out the loss for the Gaussian market maker. Let μ_i denote the mean and σ_i the variance of the

Gaussian. First note that for a Gaussian market for mean parameters $\begin{pmatrix} \mu_1 \\ \mu_1^2 + \sigma_1^2 \end{pmatrix}$ and $\begin{pmatrix} \mu_2 \\ \mu_2^2 + \sigma_2^2 \end{pmatrix}$, we have

$$\begin{aligned}
D_{C^*}\left(\begin{pmatrix} \mu_1 \\ \mu_1^2 + \sigma_1^2 \end{pmatrix}, \begin{pmatrix} \mu_2 \\ \mu_2^2 + \sigma_2^2 \end{pmatrix}\right) &= C^*\left(\begin{pmatrix} \mu_1 \\ \mu_1^2 + \sigma_1^2 \end{pmatrix}\right) - C^*\left(\begin{pmatrix} \mu_1 \\ \mu_1^2 + \sigma_1^2 \end{pmatrix}\right) \\
&\quad -\nabla C^*\left(\begin{pmatrix} \mu_2 \\ \mu_2^2 + \sigma_2^2 \end{pmatrix}\right)\begin{pmatrix} \mu_1 - \mu_2 \\ \mu_1^2 + \sigma_1^2 - \mu_2^2 - \sigma_2^2 \end{pmatrix} \\
&= -\log\frac{\sigma_1}{\sigma_2} - \begin{pmatrix} \frac{\mu_2}{\sigma_2^2} \\ -\frac{1}{2\sigma_2^2} \end{pmatrix} \cdot \begin{pmatrix} \mu_1 - \mu_2 \\ \mu_1^2 + \sigma_1^2 - \mu_2^2 - \sigma_2^2 \end{pmatrix} \\
&= -\log\frac{\sigma_1}{\sigma_2} - \frac{\mu_2(\mu_1 - \mu_2) - \frac{1}{2}(\mu_1^2 - \mu_2^2 + \sigma_1^2 - \sigma_2^2)}{\sigma_2^2} \\
&= \log\frac{\sigma_2}{\sigma_1} + \frac{\sigma_2^2 - \sigma_1^2}{2\sigma_2^2} + \frac{(\mu_1 - \mu_2)^2}{2\sigma_2^2}
\end{aligned}$$

So the Gaussian market maker loss is

$$\begin{aligned}
D_{C^*}[\phi(x), \nabla C(q_0))] - D_{C^*}[\phi(x), \nabla C(q_f))] &= \log\frac{\sigma_0}{\sigma_x} + \frac{\sigma_0^2 - \sigma_x^2}{2\sigma_0^2} + \frac{(\mu_x - \mu_0)^2}{2\sigma_0^2} \\
&\quad - \left[\log\frac{\sigma_f}{\sigma_x} + \frac{\sigma_f^2 - \sigma_x^2}{2\sigma_f^2} + \frac{(\mu_x - \mu_f)^2}{2\sigma_f^2}\right] \\
&= \log\frac{\sigma_0}{\sigma_f} + \frac{(x - \mu_0)^2}{2\sigma_0^2} - \frac{(x - \mu_f)^2}{2\sigma_f^2}
\end{aligned}$$

Here we have used the fact that $\mu_x = x$ and $\sigma_x = 0$.

Remark. Thus, all other values being the same, a trader who decreases the predicted variance contributes to a loss for the market maker. Also, a trader who moves the predicted mean closer to the actual outcome increases the market maker loss. In

other words, the market maker pays for increased predicted accuracy and/or reduced predicted uncertainty.

3.7 Bayesian Traders with Linear Utility

In the standard model of cost-function based prediction markets, a sequence of myopic, risk-neutral agents arrive and trade in the market (*Chen and Pennock*, 2007; *Chen and Vaughan*, 2010). As we saw in Section 3.4, such a trader moves the prices to its own expectation μ. However, this means that the market does not perform meaningful aggregation of agents' beliefs, as the final prices are simply the final agent's expectation.

In this section we examine the aggregation behavior of the market when agents are Bayesian and take into account the current market state when forming their beliefs. This requires more structure to their beliefs. For this and the following sections, we will assume that agents have *exponential family beliefs*.

Recall that, we are interested in eliciting the sufficient statistics of the data. We assume that the outcome is drawn from an exponential family distribution; the prediction market is set up as before with the cost function corresponding to the log partition function and the payoff function corresponding to the sufficient statistics. Thus, the market state provides an estimate on the natural parameter of the distribution from which the outcome is drawn. Additionally, we assume that the market also makes public the total number of traders that have traded in the market.

The goal is to aggregate information from risk neutral agents who have a belief distribution over the natural parameters. This prior distribution is updated by the agents based on the current market state, They also each have to access to the empirical mean of sufficient statistics based on a fixed number m of data points. Assuming a conjugate prior, both the prior and posterior belief distributions on the natural

parameters are also an exponential family distributions.

The exponential families framework is well-suited to reasoning about Bayesian updates. As before let the data distribution be given by $p(x;\theta) = \exp(\langle\theta, \phi(x)\rangle - T(\theta))$ where T is the log partition function and ϕ are the sufficient statistics. Instead of direct beliefs about the data distribution, the agent maintains a conjugate prior over the parameters θ. Every exponential family admits a conjugate prior of the form

$$p(\theta; n\nu, n) = \exp(\langle n\nu, \theta\rangle + nT(\theta) - \psi(\nu, n)).$$

Note that this is also an exponential family with natural parameter $(n\nu, n)$ where $\nu \in \mathbf{R}^d$ and n is a positive integer. The sufficient statistic maps θ to $(\theta, T(\theta))$, and the log partition function ψ is defined as the normalizer as usual. For a complete treatment of exponential families conjugate priors, see for instance (*Barndorff-Nielsen*, 1978). Now *Diaconis and Ylvisaker* (1979, Thm. 2) and *Jewell* (1974) have shown that

$$\mathrm{E}_{\theta\sim(\mathrm{n}\nu,\mathrm{n})}\mathrm{E}_{\mathrm{x}\sim\theta}[\phi(\mathrm{x})] = \nu, \tag{3.13}$$

meaning that $\nu = n\nu/n$ is the posterior mean. Thus, it is helpful to think of the prior as being based on a phantom sample of size n and mean ν. Suppose now that the agent observes an empirical sample with mean $\hat{\mu}$ and size m. By a standard derivation (see *Diaconis and Ylvisaker*, 1979), the posterior conjugate prior parameters become $n\nu \leftarrow n\nu + m\hat{\mu}$ and $n \leftarrow n + m$, and the posterior expectation (3.13) evaluates to

$$\frac{n\nu + m\hat{\mu}}{n + m}. \tag{3.14}$$

Thus the posterior mean is a convex combination of the prior and empirical means, and their relative weights depend on the phantom and empirical sample sizes.

Consider Bayesian agents maintaining an exponential family conjugate prior over

the data model's natural parameters (equivalently, the expected security payoffs). Each agent has access to a private sample of the data of size m with mean statistic $\hat{\mu}$. If n agents have arrived before to trade, then the current market prices μ correspond to the phantom sample, and the phantom sample size is nm. After forming the posterior (3.14) with these substitutions, the (risk-neutral) agent purchases shares δ to move the current market share vector to $\nabla C(\theta + \delta) = \frac{n\nu + \hat{\mu}}{n+1}$. As a result, the final market prices under this behavior are a simple average of the agent's mean parameters and the initial market prices. We note that to facilitate such belief updating, the market should post the number of trades since initialization in which case updates would proceed as follows.

Suppose the current market state is θ and i traders have traded in the market when trader $i+1$ with prior belief distribution $p(\theta; b_0^i)$ enters the market. Here $b_0^i = (n\nu_i, n)$. This trader also has access to private information in the form of empirical sufficient statistics $\hat{\mu}_i$ from m data points. Recall from Proposition III.1 that natural parameter θ corresponds to expected statistics $\nabla T(\theta)$. Thus, he updates his belief as $p(\theta; b_i)$ where $b = (m\hat{\mu} + mi\nabla T(\theta) + n\nu_i, n + mi + m)$.

Suppose the trader wishes to maximize his expected payoff. Then the number of shares δ_i that he purchases when the current market state is θ is given by

$$\arg\max_{\delta_i} \mathrm{E}_{\theta\sim \mathrm{b_i}} \mathrm{E}_{\mathrm{x}\sim\theta} \left[\delta_{\mathrm{i}} \phi(\mathrm{x}) - \mathrm{T}(\delta_{\mathrm{i}} + \theta) + \mathrm{T}(\theta)\right]$$

But, from Equation 3.13 we have $\mathrm{E}_{\theta\sim \mathrm{b}} \mathrm{E}_{\mathrm{x}\sim\theta}[\phi(\mathrm{x})] = \frac{\mathrm{n}\nu + \mathrm{m}\hat{\mu} + \mathrm{mi}\nabla \mathrm{T}(\theta)}{\mathrm{n+m(i+1)}}$. To obtain the maximum, we set the gradient of the above expression with respect to δ_i to 0. Thus, we have for the optimal number of shares δ_i^*

$$\nabla T(\delta_i^* + \theta) = \frac{n\nu + m\hat{\mu} + mi\nabla T(\theta)}{n + m(i+1)}$$

Thus, from Proposition III.1 we have that for an exponential family prediction market,

the final market state is given by

$$\nabla G\left(\frac{n\nu + m\hat{\mu} + mi\nabla T(\theta)}{n + m(i+1)}\right)$$

where G is the convex conjugate of T. Thus, the final market state is a convex combination of prior, posterior and market means. Notice that this value of the natural parameter corresponds to its maximum a posteriori (MAP) estimate.

3.8 Risk-Averse Traders with Exponential Utility

In this section we relax the standard assumption that agents in the market are risk-neutral. We show that with sufficient extra structure to the agents' beliefs and utilities, the market performs a clean aggregation of the agents' beliefs via a simple weighted average. Assume that the agent has an exponential utility function for wealth w:

$$U_a(w) = -\frac{1}{a}\exp(-aw). \tag{3.15}$$

Here a controls the risk aversion: the agent's aversion grows as a increases, and as a tends to 0 we approach linear utility (risk-neutrality). Specifically, a is the Arrow-Pratt coefficient of absolute risk aversion, and exponential utilities of the form (3.15) are the unique utilities that exhibit constant absolute risk aversion (*Varian*, 1992, Chap. 11).

Theorem III.7. *Suppose an agent has exponential utility with coefficient a and exponential family beliefs with natural parameter $\hat{\theta}$. In the generalized LMSR market with current market state θ, the agent's optimal trade δ moves the state vector to*

$$\theta + \delta = \frac{1}{1+a}\hat{\theta} + \frac{a}{1+a}\theta. \tag{3.16}$$

Proof. Let δ be the vector of shares the agent trades. The payoff given eventual

outcome x is then $\delta\phi(x) - C(\delta+\theta) + C(\theta)$. The utility for this payoff is

$$U(\delta\phi(x) - C(\delta+\theta) + C(\theta)) = -\frac{1}{a}\exp(-a\delta\phi(x) + aC(\delta+\theta) - aC(\theta)).$$

Taking the expected utility, we obtain

$$\begin{aligned}
& \mathbf{E}\left[U(\delta\phi(x) - C(\delta+\theta) + C(\theta))\right] \\
= & \int_{\mathcal{X}} -\frac{1}{a}\exp(-a\delta\phi(x) + aC(\delta+\theta) - aC(\theta))\exp[\hat{\theta}\phi(x) - T(\hat{\theta})]\,dx \\
= & -\frac{1}{a}\int_{\mathcal{X}} \exp[(\hat{\theta}-a\delta)\phi(x) + aC(\delta+\theta) - aC(\theta)) - T(\hat{\theta})]\,dx \\
= & -\frac{1}{a}\exp[aC(\delta+\theta) - aC(\theta)) + T(\hat{\theta}-a\delta) - T(\hat{\theta})]\int_{\mathcal{X}} \exp[(\hat{\theta}-a\delta)\phi(x) - T(\hat{\theta}-a\delta)]\,dx \\
= & -\frac{1}{a}\exp[aC(\delta+\theta) - aC(\theta)) + T(\hat{\theta}-a\delta) - T(\hat{\theta})]\int_{\mathcal{X}} p(x;\hat{\theta}-a\delta)\,dx \\
= & -\frac{1}{a}\exp[aC(\delta+\theta) - aC(\theta)) + T(\hat{\theta}-a\delta) - T(\hat{\theta})] \\
= & U\left(-C(\delta+\theta) + C(\theta)) - \frac{1}{a}T(\hat{\theta}-a\delta) + \frac{1}{a}T(\hat{\theta})\right)
\end{aligned}$$

The second-last equality follows from the fact that $\int_{\mathcal{X}} p(x;\hat{\theta}-a\delta)\,dx = 1$. Since utility U is monotone increasing, it is maximized by maximizing its argument $-C(\delta+\theta) + C(\theta) - \frac{1}{a}T(\hat{\theta}-a\delta) + \frac{1}{a}T(\hat{\theta})$ which is a concave function of δ by convexity of C and T. The optimality condition for the argument is

$$\begin{aligned}
\nabla\left(-C(\delta^*+\theta) - \frac{1}{a}T(\hat{\theta}-a\delta^*)\right) &= 0 \\
\nabla C(\delta^*+\theta) &= -a\frac{1}{a}\nabla T(\hat{\theta}-a\delta^*) \\
\nabla C(\delta^*+\theta) &= \nabla T(\hat{\theta}-a\delta^*) \qquad (3.17)
\end{aligned}$$

Here the gradient is with respect to the share purchase δ. Now in the exponential family market, C is the log-partition function of the corresponding exponential family

and $C = T$. Then (3.17) can be solved by equating the arguments. This leads to $\delta^* = (\hat{\theta} - \theta)/(1 + a)$, which moves the share vector to $\theta + \delta^* = \frac{1}{1+a}\hat{\theta} + \frac{a}{1+a}\theta$. □

We stress that the aggregation in Theorem III.7 arises directly from the agents' choice of trades. The market maker does not need to know the risk aversion parameters. Note that as a tends to 0 we approach risk neutrality and the agent moves the share vector all the way to its private estimate $\hat{\theta}$. As a grows larger (the agent grows more risk averse) the agent makes smaller trades to reduce it exposure, and the final state stays closer to the current state θ. Update (3.16) implies that, under the conditions of the theorem, a market that receives a sequence of myopic traders aggregates their natural parameters in the form of an exponentially weighted moving average. The final market estimates (i.e., prices) are obtained by applying ∇T to this average.

3.9 Repeated Trading and the Effective Belief

In previous sections we analyzed trader behavior assuming it is his first entry into the market. We now pose the question: how will a trader reason about a possible future investment when the trader holds an existing portfolio? In the context of a trader possessing an exponential family belief together with exponential utility, we show that we can explicitly analyze how an agent incorporates an existing portfolio. The key conclusion is that a trader will reason about a future investment simply as though he had updated his belief and had no prior investment.

Suppose an exponential utility agent has exponential family belief parametrized by natural parameter $\hat{\theta}$. Based on this belief, let δ_1 be the vector of shares the agent has purchased on first entry in the market. On a subsequent entry into this market

with market state θ', his optimal purchase δ_2^* is given by the solution of

$$\arg\max_{\delta_2} \ \mathrm{E}_{\mathrm{x}\sim\mathrm{p}(\mathrm{x};\hat{\theta})}\mathrm{U}\left[\langle\delta_1+\delta_2,\phi(\mathrm{x})\rangle-\mathrm{C}(\delta_1+\theta)+\mathrm{C}(\theta)-\mathrm{C}(\delta_2+\theta')+\mathrm{C}(\theta')\right].$$

Then if $\theta''=\hat{\theta}-a\delta_1$ is the effective belief, the trader's optimal purchase is given by $\delta_2=(\theta''-\theta')/(1+a)$, moving the share vector to $\theta'+\delta_2=\frac{1}{1+a}\theta''+\frac{a}{1+a}\theta'$, which is a convex combination of the effective belief and the current market state.

Theorem III.8. *Suppose an exponential utility maximizing trader with utility parameter a who has belief $\hat{\theta}$ makes a purchase δ in a market. On subsequently re-entering the market, he will behave identically to an exponential utility maximizing trader with belief $\hat{\theta}-a\delta$ and no prior exposure in the market.*

Theorem III.8 implies that financial exposure can be equivalently understood as changing the privately held beliefs.

3.10 Equilibrium Market State for Exponential Utility Agents

We have shown that every exponential-utility maximizing trader picks the share vector δ so that the eventual market state can be represented as a convex combination of the current market state and the natural parameter of his (exponential family) belief distribution. In this section we will compute the equilibrium state in an exponential family market with multiple such traders.

We draw on a well-known result from game theory regarding the class of *potential games*. We say a function $f(\vec{x})$ is at a *local optimum* if changing any coordinate of $\vec{x}$ does not increase the value of f.

Theorem III.9 (*Monderer and Shapley* (1996))**.** *Let $U_i(\vec{\delta})$ be the utility function of the i^{th} trader given the strategy profile $\vec{\delta}=(\delta_1,\ldots,\delta_i,\ldots,\delta_n)$. Assume there exists a*

potential function $\Phi(\vec{\delta})$ *such that, for any* $\vec{\delta}$ *and* δ_i',

$$U_i(\vec{\delta}) - U_i(\vec{\delta}_{-i}, \delta_i') = \Phi(\vec{\delta}) - \Phi(\vec{\delta}_{-i}, \delta_i').$$

Then $\vec{\delta}$ *is a pure-strategy Nash equilibrium if and only if* $\vec{\delta}$ *is a local optimum for* $\Phi(\cdot)$.

Proof sketch: If $\vec{\delta}$ is a local optimum of $\Phi(\cdot)$, then for any $\vec{\delta}'$, $\Phi(\vec{\delta}) - \Phi(\vec{\delta}') \geq 0$ and hence $U_i(\vec{\delta}) \geq U_i(\vec{\delta}_{-i}, \delta_i')$ or $\vec{\delta}$ is a Nash equilibrium. The other direction can be similarly argued.

In the exponential family market, the cost function C is identical to the log partition function T defined in (3.3). Let $\vec{\delta}$ be the matrix of share vectors purchased by every trader in the market at equilibrium. Let θ be the initial market state, $\hat{\theta}_i$ the natural parameter of trader i's belief distribution, and a_i his risk aversion parameter.

Define a potential function as $\Phi(\vec{\delta}) = T\left(\theta + \sum_i \delta_i\right) + \sum_i \frac{1}{a_i} T(\hat{\theta}_i - a_i\delta_i)$. Rather than working directly with the utilities of every trader, we will work with the log of their utility values since the potential function analysis still applies for any monotonically increasing transformation of the traders' utility functions. Now the log-utility of trader i is

$$U_i(\vec{\delta}) = -T(\theta + \textstyle\sum_j \delta_j) + T(\theta + \sum_{j \neq i} \delta_j) - \frac{1}{a_i} T(\hat{\theta}_i - a_i\delta_i) + \frac{1}{a_i} T(\hat{\theta}_i).$$

We can now apply Theorem III.9, hence the equilibrium state is obtained by jointly maximizing $\Phi(\vec{\delta})$ for each δ_i:

$$\nabla_{\delta_i} \Phi(\vec{\delta}) = \nabla T\left(\theta + \textstyle\sum_{j=1}^n \delta_j\right) - \nabla T(\hat{\theta}_i - a_i\delta_i) = 0.$$

This leads to the following expression for the final market state.

$$\theta + \sum_{j=1}^{n} \delta_j = \frac{\theta + \sum_{i=1}^{n} \left(\frac{\hat{\theta}_i}{a_i} \right)}{1 + \sum_{i=1}^{n} \frac{1}{a_i}}$$

We see that the equilibrium state is a convex combination of the initial market state and all agent beliefs, with the latter weighted according to risk tolerance.

3.11 Expected Payoff in the Exponential Family Market

Linear Utility Traders The agent's expected profit from moving the share vector from θ to θ' is

$$\begin{aligned} & \langle \theta' - \theta, \mu \rangle - C(\theta') + C(\theta) \\ = \; & C(\theta) - C(\theta') - \langle \theta - \theta', \nabla C(\theta) \rangle \\ = \; & D_C(\theta, \theta') = D_{C^*}(\mu', \mu), \end{aligned}$$

recalling that $D_C(\cdot, \cdot)$ is the Bregman divergence based on the cost function $C(\cdot)$ (3.9). Now *Banerjee et al.* (2005b) have observed (among others) that the Kullback-Leibler divergence between two exponential family distributions is the Bregman divergence, with respect to the log-partition function, between their natural parameters.

Theorem 3.11.1.

$$KL(P_{\beta_1}, P_{\beta_2}) = D_T(\beta_2, \beta_1)$$

where P_{β_1} and P_{β_2} are exponential family distributions with natural parameters β_1 and β_2 respectively and $T(\cdot)$ is the log partition function.

Proof.

$$\begin{aligned}
KL(P_{\beta_1}, P_{\beta_2}) &= \int_{-\infty}^{\infty} P_{\beta_1}(x) \ln \frac{P_{\beta_1}(x)}{P_{\beta_2}(x)}\, dx \\
&= \int_{-\infty}^{\infty} P_{\beta_1}(x)(\ln P_{\beta_1}(x) - \ln P_{\beta_2}(x))\, dx \\
&= (\beta_1 - \beta_2) \int_{-\infty}^{\infty} P_{\beta_1}(x)\phi(x)\, dx \\
&\quad +(T(\beta_2) - T(\beta_1)) \int_{-\infty}^{\infty} P_{\beta_1}(x)\, dx \\
&= (\beta_1 - \beta_2)\nabla T(\beta_1) + T(\beta_2) - T(\beta_1) \\
&= D_T(\beta_2, \beta_1)
\end{aligned}$$

□

The agent's expected profit is therefore the KL divergence between the market's implied expectation and the exponential family corresponding to the agent's expectation.

Exponential Utility Traders Let θ be the current market state. We have shown that an exponential utility trader with belief distribution parametrized by β will move the market state to $\theta' = \frac{1}{1+a}\beta + \frac{a}{1+a}\theta$. Therefore, the trader's expected net payoff is

given by

$$\begin{aligned}
& \mathrm{E}_{\mathrm{x}\sim\mathrm{P}_\beta}[\mathrm{C}(\theta) - \mathrm{C}(\theta') - (\theta - \theta')\phi(\mathrm{x})] \\
= \; & T(\theta) - \theta \mathrm{E}_{\mathrm{x}\sim\mathrm{P}_\beta}[\phi(\mathrm{x})] - (\mathrm{T}(\theta') - \theta' \mathrm{E}_{\mathrm{x}\sim\mathrm{P}_\beta}[\phi(\mathrm{x})]) \\
= \; & T(\theta) - \theta \nabla T(\beta) - (T(\theta') - \theta' \nabla T(\beta)) \\
= \; & T(\theta) - T(\beta) - \nabla T(\beta)(\theta - \beta) - (T(\theta') - T(\beta) - \nabla T(\beta)(\theta' - \beta)) \\
= \; & D_T(\theta, \beta) - D_T(\theta', \beta) \\
\geq \; & \frac{1}{a} D_T(\theta', \beta) \geq 0
\end{aligned}$$

The second to last inequality holds since $D_T(\theta', \beta)$ is convex in θ' and we have:

$$\begin{aligned}
D_T(\theta', \beta) &= D_T\left(\frac{1}{1+a}\beta + \frac{a}{1+a}\theta, \beta\right) \\
&\leq \frac{1}{1+a} D_T(\beta, \beta) + \frac{a}{1+a} D_T(\theta, \beta) \\
&= \frac{a}{1+a} D_T(\theta, \beta)
\end{aligned}$$

Thus, a trader who moves the market state can expect his profit to be positive and at least $\frac{1}{a} D_T(\theta', \beta)$.

3.12 Budget-limited Aggregation

In this section, we consider the evolution of the market state when traders are budget-limited. We assume that the traders trade in multiple instances of the market. That is, after the initial setup and trades, the outcome is revealed and the traders are paid off. Then, the market runs again with the same set of traders and the outcome drawn from a (possibly different) exponential family distribution. The goal of this section is to analyze how the budgets of traders evolve under these circumstances. As before, the market price is interpreted as a probability density over the outcome space

and the share vector as the natural parameter of an exponential family distribution. Consistent with the connections drawn in Section 3.5 and throughout, we measure the error in prediction using the standard log loss.

We show that traders with faulty information can only impose a limited amount of additional loss to the market's prediction. Further, since informative traders experience an expected increase in budget, they will eventually be unconstrained and allowed to carry out unrestricted trades. Taken together, this means that while the market suffers limited damage from ill-informed traders, it is also able to make use of all the information from informative traders in the long run.

Budget-limited trades Let α be the budget of a trader in the market. Suppose that with infinite budget, the trader would have moved the market state from θ to $\hat{\theta}$, where $\hat{\theta}$ represents his true belief. Now suppose further that $\alpha < C(\hat{\theta}) - C(\theta)$; that is, the trader's budget disallows purchasing enough shares to move the market state to his belief. In this case, we want to budget-limit the trader's influence on the market state.

Let the current market state be given by θ and let the final market state be $\theta' = \lambda\hat{\theta} + (1-\lambda)\theta$ where $\lambda = \min\left(1, \frac{\alpha}{C(\hat{\theta})-C(\theta)}\right)$. The cost to the trader to move the market state from θ to θ' is at most his budget α and is called his *budget-limited trade*. We note here that it is not clear that this is the trader's optimal budget limited trade. In fact, under some circumstances it is known that moving along the straight line is not optimal (*Fortnow and Sami*, 2012).

Note that while an uninformative trader is unconstrained in his belief, the informative trader's belief corresponds to the parameter of the true distribution.

Limited Damage We will now quantify the error in prediction that the market maker might have to endure as a result of ill-informed entities entering the market. We assume that these entities trade in multiple instances of the market; thus the

exposure of the market maker is over several rounds. The log loss function for θ shares held is defined as $L(\theta, x) = -\log p(x;\theta) = C(\theta) - \langle \theta, \phi(x) \rangle$.

Lemma III.10. *The loss induced on the market by an uninformative trader is bounded by his initial budget.*

Proof. First consider the change in budget of a trader i over multiple rounds of the prediction market. Let his budget at rounds t and $t-1$ be α_i^t and α_i^{t-1} respectively. The change in budget for trader i moving the market state from θ to θ' with outcome x^t is

$$\alpha_i^t - \alpha_i^{t-1} \quad = \quad C(\theta) - C(\theta') - (\theta - \theta')^T \phi(x^t) = L(\theta, x^t) - L(\theta', x^t) = \Delta_i^t$$

Here Δ_i^t is called the myopic impact of a trader i in round t. Thus, the myopic impact captures incremental gain in prediction due to the trader in a round and is equal to the change in his budget in that round.

Since the market evolves so that the budget of any trader never falls below zero, the total myopic impact in T rounds caused due to trader i is

$$\Delta_i := \sum_{t=1}^{T} \Delta_i^t = \sum_{t=1}^{T} (\alpha_i^t - \alpha_i^{t-1}) = \alpha_i^T - \alpha_i^0 \geq -\alpha_i^0$$

□

An interesting aspect of Lemma III.10 is that the log loss can be quantified in the same units as the traders' budgets.

Budget of Informative Traders We now characterize the expected change in budget for an informative trader.

Lemma III.11. *Let θ be the current market state. Suppose that an informative trader with belief distribution parametrized by $\hat{\theta}$ moves the market state to the budget-limited*

state $\theta' = \lambda\hat{\theta} + (1-\lambda)\theta$*. Then, the expectation (over the trader's belief) of the trader's profit is strictly positive whenever his budget is positive and his belief differs from the previous market position* θ*.*

Proof. Let C be the log partition function T of the belief distribution. The payoff is given by the sufficient statistics $\phi(x)$. Then the trader's expected net payoff is given by

$$\begin{aligned} \mathrm{E}_{\mathrm{x}\sim\mathrm{P}_{\hat{\theta}}}[\mathrm{C}(\theta) - \mathrm{C}(\theta') - (\theta - \theta')\phi(\mathrm{x})] &= T(\theta) - \theta\nabla T(\hat{\theta}) - (T(\theta') - \theta'\nabla T(\hat{\theta})) \\ &= D_T(\theta, \hat{\theta}) - D_T(\theta', \hat{\theta}) \geq \lambda D_T(\theta, \hat{\theta}) \geq 0 \end{aligned}$$

where $D_T(\cdot, \cdot)$ is the Bregman divergence based on T. The second to last inequality holds since $D_T(\theta', \hat{\theta})$ is convex in θ' and we have:

$$D_T(\theta', \hat{\theta}) = D_T\left(\lambda\hat{\theta} + (1-\lambda)\theta, \hat{\theta}\right) \leq \lambda D_T(\hat{\theta}, \hat{\theta}) + (1-\lambda)D_T(\theta, \hat{\theta}) = (1-\lambda)D_T(\theta, \hat{\theta})$$

A trader who adjusts the market state may expect profit of at least $\lambda D_T(\theta, \hat{\theta})$. □

We note one important aspect of Lemma III.11: the expectation is taken with respect to each trader's belief at the time of trade, rather than with respect to the true distribution. This is needed because we have made no assumptions about the optimality of the traders' belief updating procedure. If we assume that the traders' belief formation is optimal, then this growth result will extend to the true distribution as well.

Given a continuous density the probability a trader will form exactly the same beliefs as the current market position is 0, and thus, each trader will have positive expected profit on almost all sequences of observed samples and beliefs. This result suggests that, eventually, every informative trader will have the ability to influence the market state in accordance with his beliefs, without being budget limited.

Notice that Lemma III.11 only required that the market state to which the trader moves be representable as a convex combination of the current market state and his belief. This means that the result holds for exponential utility traders aiming to maximize their utility by Theorem III.7. In this case, the trader who moves the market state can expect his profit to be positive and at least $\frac{1}{a}D_T(\theta, \hat{\theta})$ where a is the exponential utility parameter. When the cost function is adjusted to C_λ with an inverse liquidity parameter λ (Section 3.8), the trader receives expected payoff of at least $\frac{1}{a}D_T(\lambda\theta, \hat{\theta})$.

3.13 Discussion and Conclusion

The log partition function of the exponential family distribution can be used to define a generalized LMSR cost function. If you further define securities whose payoffs correspond to the sufficient statistics then the outstanding share vector corresponds exactly to the natural parameters of the exponential family. This means that the market state now defines an exponential family distribution over the outcome space. It turns out that the dual variables of the natural parameters are the expected values of the sufficient statistics. In terms of the market semantics, these may be interpreted as the instantaneous prices of the securities. For instance, for a Gaussian market, these values would correspond to the first and second moments of the outcome variable.

The market evolution when traders have exponential utility is particularly striking. The market would essentially correspond to the average of the agent beliefs weighted by their risk aversion parameters at equilibrium. There is also a surprising equivalence between beliefs and trades in this market. An exponential utility trader engaging in a trade in this market can be thought of as essentially updating his belief.

We have shown that the equilibrium market state in our prediction market mechanism is a risk-tolerance-weighted average of the natural parameters of the traders and the market maker, with the more risk tolerant traders contributing more to the

market state. This result is quite natural, but appears to crucially depend on the synergy between exponential families and exponential utility. Based on recent promising results (*Hu and Storkey*, 2014; *Othman and Sandholm*, 2011), Jacob Abernethy, Rafael Frongillo and I advocate using *risk measures*, previously used predominantly in financial mathematics, as a way to analyze trading decisions made by agents in prediction markets (*Abernethy et al.*, 2014a). For instance, Frongillo and Reid (*Frongillo and Reid*, 2014) show that the equilibrium result we attained in exponential family markets extends to risk-tolerance families of arbitrary risk measures: if the market maker is risk-constant and traders seek to minimize their own risk measure, then the equilibrium state is again the weighted average of trader beliefs. Thus, using risk measures to characterize trader behavior appears to be a promising avenue for further exploration.

CHAPTER IV

Prediction Markets for Multiple Events

4.1 Introduction

In the previous chapter, we explored a deep connection between the seemingly disparate concepts of exponential family distributions and cost function prediction markets. In this chapter, we exploit this connection to develop prediction markets for multiple events using graphical models. A graphical model (GM) provides a way to efficiently encode interdependencies among jointly distributed variables especially when conditional (in)dependencies exist. It is helpful to think of a graphical model in terms of syntax and semantics. The graph itself is the *syntax* and the *semantics* are the values you assign to the individual pdfs and the corresponding joint distributions.

We are interested in studying the interaction between prediction markets and graphical models.

1. First, we consider a simple case of two prediction markets set up on the same outcome space. In this case, the market makers may have different market states based on the population of traders in each market. We ask, how should such market makers communicate with each other to resolve any potential discrepancies.

2. Now suppose we set up a single market on multiple outcomes. How should a

trader reason about trading only on outcomes relevant to him?

3. We then generalize our first question as follows. Suppose we have separate markets on related events. Is there some formally characterizable communication between the market makers that recognizes this relationship and reflects it in their market states?

4.1.1 Related Work

Using graphical models for representing aggregate beliefs have been considered by Pennock and Wellman (*Pennock and Wellman*, 2005). Their results focus on characterizing the structure of the aggregate belief for a particular structure of agent beliefs. Amos Storkey has shown that the equilibrium price can be modeled as a probabilistic graphical model when individual agents are knowledgeable about some subset of variables (*Storkey*, 2011). Recently, Frongillo and Reid have modeled agent behavior using risk measures (*Frongillo and Reid*, 2014). They outline future work based on modeling networks of agents graphically and characterizing their equilibrium state. Prediction Market models based on graphical models have also been considered by *Sun et al.* (2012, 2013). They use graphical models to efficiently compute the assets held by a trader in combinatorial prediction markets.

4.2 Multiple Markets on a Single Event

To illustrate the need for understanding the relationship between related market makers, we first examine the case with two market makers who have (currently) disjoint sets of traders. A potential arbitrager may then exploit the discrepancy between the market states, making a guaranteed profit from the resulting surplus. We would like to formally characterize the behavior of an arbitrager who purchases shares to maximize profit. This surplus can then potentially be split fairly amongst

the market makers thus eliminating the arbitrage opportunity.

An arbitrager purchasing δ shares in one market with current share vector m_1 and selling it in the other market with current share vector m_2 would make a profit of

$$-[C(m_1 + \delta) - C(m_1) + C(m_2 - \delta) - C(m_2)]$$

To maximize his profit the arbitrager sets $\delta = \frac{m_1+m_2}{2}$ which would give a net profit to the arbitrager. Note that the arbitrager has zero exposure in either market. In general, if $m_2 > m_1$, any price in the interval $(C(\frac{m_1+m_2}{2}) - C(m_1), C(m_2) - C(\frac{m_1+m_2}{2}))$ paid from the second market maker to the first would leave both market makers in at least as good a position as if an arbitrager made his optimal trade.

4.3 Partially Informed Traders

For this and the following sections, we are interested in developing market makers for multiple, possibly correlated events. In this section, we consider a joint market over multiple variables.

Typically, one assumes that traders in a prediction market have a belief on the entire event space (or some statistic of the outcome, which is a function of the event space). We can imagine scenarios where this is not necessarily the case. In this section, we aim to characterize the interaction of traders with the Exponential Family Market when they have access to some part of the data. For this we first recall the Expectation Maximization Algorithm on exponential family distributions.

4.3.1 The Expectation Maximization Algorithm

The EM algorithm applies when you have some observed and some unobserved variables. Let X be the set of unobserved and $Y = y$ the set of observed variables

that are jointly distributed as an exponential family

$$p(X, Y) = \exp\{\theta^T \phi(X, Y) - \psi(\theta)\}$$

Thus, taken together, these variables represent the actual outcome and $p(X, Y)$ defines the joint distribution on the outcome space. To compute the incomplete log likelihood, notice $p(X, y) = \exp\{\theta^T \phi(X, y) - \psi(\theta)\}$, so that the **conditional distribution**,

$$p(X|Y = y) \propto p(X, y) \propto \exp\{\theta^T \phi(X, y)\}$$

Normalizing we'd have $p(X|Y = y) = \exp\{-\psi_y(\theta)\} \exp\{\theta^T \phi(X, y)\}$ where $\exp\{-\psi_y(\theta)\} = \frac{1}{\int_X p(X,y)}$ or

$$\psi_y(\theta) = \log \int_X \exp\{\theta^T \phi(X, y)\}\ dx$$

So we can write $p(X|Y = y) = \exp\{\theta^T \phi(X, y) - \psi_y(\theta)\}$ where θ are the natural parameters, $\psi_y(\theta)\}$ is the log partition function and $\phi(X, y)$ are the sufficient statistics.

Now to maximize the **incomplete log likelihood**. The idea is to marginalize out the unobserved variables. So

$$\begin{aligned} l(\theta; y): &= \log \int_X \exp\{\theta^T \phi(X, y) - \psi(\theta)\}\ dx \\ &= \log \left(\exp\{-\psi(\theta)\} \int_X \exp\{\theta^T \phi(X, y)\} \right)\ dx \\ &= -\psi(\theta) + \log \int_X \exp\{\theta^T \phi(X, y)\}\ dx \\ l(\theta; y) &= \psi_y(\theta) - \psi(\theta) \end{aligned}$$

Now we can rewrite the incomplete log likelihood using convex analysis. Since

$\psi_y(\theta) = \sup_{\mu_y} \theta \cdot \mu_y - \psi_y^*(\mu_y)$ we can write

$$\begin{aligned} l(\theta; y) &= \psi_y(\theta) - \psi(\theta) \\ &= \sup_{\mu_y} \theta \cdot \mu_y - \psi_y^*(\mu_y) - \psi(\theta) \\ &\leq \theta \cdot \mu_y - \psi_y^*(\mu_y) - \psi(\theta) := L(\mu_y, \theta) \end{aligned}$$

The EM algorithm can then be seen as *coordinate ascent* on $L(\mu_y, \theta)$. Note that this isn't the same as the incomplete log likelihood.

E Step $\mu_y^{t+1} = \arg\max_{\mu_y} L(\mu_y, \theta^t)$

M Step $\theta^{t+1} = \arg\max_{\theta} L(\mu_y^{t+1}, \theta)$

Note that

$$\begin{aligned} \mu_y^{t+1} &= \arg\max_{\mu_y} L(\mu_y, \theta^t) \\ &= \arg\max_{\mu_y} \theta^t \cdot \mu_y - \psi_y^*(\mu_y) - \psi(\theta^t) \\ &= \arg\max_{\mu_y} \theta^t \cdot \mu_y - \psi_y^*(\mu_y) \end{aligned}$$

which means $\mu_y^{t+1} = \mathrm{E}_{\theta^t}[(\phi(\mathrm{X}, \mathrm{y}))]$ hence this is the **E**xpectation step.

Note also that in the second equation above, the argmax makes this equivalent to directly working on the incomplete log likelihood so this step increases the incomplete log likelihood as well (since there's no slack).

Thus, if you look at the EM algorithm in the context of exponential families, you can look at the expectation step as maximizing the mean parameter for a likelihood function, and the maximization step as maximizing the natural parameter for that mean parameter.

4.3.2 Market Semantics of the Expectation Maximization Algorithm

Let us formalize the problem of a partially informed trader that was introduced at the start of this section.

Suppose the prediction market is set up with a cost function of $C(\theta)$ where as before $C(\cdot)$ is the log partition function of an exponential family distribution parameterized by θ. Let the payoff be given by $\phi(x, y)$. Suppose now that a trader in this market has access to the actual values of $y = Y$. In this case, the optimal trade of this trader will be given by $(\theta' - \theta)$ where θ is the current market state and θ' is the solution to

$$\arg\max_{\theta'} \{(\theta' - \theta) \cdot \mathrm{E}[\phi(\mathrm{x}, \mathrm{y})] - (\mathrm{C}(\theta') - \mathrm{C}(\theta))\}$$

Since the trader is indifferent to the variables x and he has a certain belief that $y = Y$, the expectation of $\phi(x, y)$ would be given by $\mathrm{E}[\phi(\mathrm{x}, \mathrm{Y})] = \int_{\mathcal{X}} \Pr(\mathrm{x}, \mathrm{Y}|\theta)\phi(\mathrm{x}, \mathrm{Y})$. That is, the trader forms his belief about the expected payoff of the contracts based on the revealed variables y and the current market state θ.

This leads to the following interesting observation.

Remark IV.1. Consider an exponential family market on variables $X \cup Y$. Suppose a trader, who has access to the realized values of $Y = y$, forms his beliefs on the payoff of securities based on the current market state and values y. Then the trader's optimal trade effectively performs an iteration of the Expectation Maximization algorithm in this market.

4.4 Multiple Markets on Multiple Events

In this section, we set up a separate market for each of the correlated variables where the dependencies between the variables is encoded using a graphical model.

We consider a case where the relationship between these variables can be characterized by a chain.

We can thus factorize the joint density as follows.

$$\begin{aligned} p(\mathbf{x}) &= \exp\left\{\langle\theta, \mathbf{x}\rangle + \frac{1}{2}\langle\langle\Theta, \mathbf{x}\mathbf{x}^T\rangle\rangle - \psi(\theta, \Theta)\right\} \\ &\propto \exp\left\{\sum_i \theta_i x_i + \frac{1}{2}\sum_i\sum_j \Theta_{ij} x_i x_j\right\} \end{aligned}$$

Here $\theta = \Lambda\mu$ where Λ is the precision matrix and $\Theta = -\Lambda$ with the additional constraint that $\Theta_{ij} = 0$ whenever $(v_i, v_j) \notin E$ and θ. This constraint follows from the Hammersley-Clifford theorem. This is the parametrization of the Gaussian in exponential family form. Note that for this to be a valid distribution we require that $\Theta \prec 0$ i.e., Θ is a negative definite matrix or its eigenvalues are less than 0. For the chain, every row of Θ will only contain at most 3 non-zero elements.

Example 4.4.1. For instance for a 5 node graph, this would be

$$p(\mathbf{x}) \propto \exp\left\{\sum_{i=1}^{5} \theta_i x_i + \frac{1}{2}\sum_{i=1}^{5} \Theta_{ii} x_i^2 + \sum_{i=1}^{4} \Theta_{i,i+1} x_i x_{i+1}\right\}$$

Given this relationship between dependent variables, can we quantify the effect that a trade in one market has on the predictive probabilities of events in a dependent market? More formally, how does a shift in securities of x_1 affect the marginal distribution of x_3. Let's use the fact that the marginal distribution is actually parametrized simply by μ_3 and Σ_{33}. We also use the fact that we have an expression for the natural parameters in terms of the mean and precision matrix to compute the marginal distribution as follows. First note that $\Theta = -\frac{1}{2}\Sigma^{-1}$ and $\theta = \Sigma^{-1}\mu$. Note that $\mu_3 \propto (\Theta^{-1} \cdot \theta)_3$. Let's represent buying δ shares in the first dimension as $e_1 \cdot \delta$ where e_i is the vector

with zeroes in all but the i^{th} dimensions.

The new value of the x_3's mean is now $\mu_3' \propto (\Theta^{-1} \cdot (\theta + e_1 \cdot \delta))_3 = (\Sigma \cdot (\theta + e_1 \cdot \delta))_3 = \mu_3 + \sigma_{31}\delta$. The Sherman-Morrison formula (*Sherman and Morrison*, 1950) gives a way to compute the new covariance matrix when there is change an element of the precision matrix. In the following let $u = v = (10 \ldots 0)$

$$\begin{aligned}
(\Lambda + uv^T)^{-1} &= \Sigma - \frac{\Sigma u v^T \Sigma}{1 + v^T \Sigma u} \\
&= \Sigma - \frac{(\Sigma u)(\Sigma u)^T}{1 + \sigma_{11}} \\
&= \Sigma - \frac{(\sigma_{11} \ldots \sigma_{n1})(\sigma_{11} \ldots \sigma_{n1})^T}{1 + \sigma_{11}} \\
&= \Sigma - \frac{M}{1 + \sigma_{11}}
\end{aligned}$$

. where the matrix M is given by $M_{ij} = \sigma_{1i}\sigma_{1j}$. This means that the the new covariance matrix for a purchase of δ shares is given by

$$\Sigma'_{ij} = \Sigma_{ij} - \frac{\delta \sigma_{1i} \sigma_{1j}}{1 + \delta \sigma_{11}}$$

Thus we are able to exactly characterize the shift in the marginal distribution of a variable due to trades in a market of *a separate (possibly indirectly) dependent variable*!

4.5 Single Market on Multiple Events

In this section, we consider a joint market over multiple variables and develop a model, based on Gaussian Mean Random Fields, to characterize trading over some subset of variables.

4.5.1 A GMRF Market Maker

A graphical model (GM) is a representation of a joint probability distribution over a collection of random variables usually represented as nodes on a graph and encoding the dependencies using edges between these nodes. A particular type of GM is the *Gaussian Mean Random Field* (GMRF) where each of the nodes is a Gaussian random variable. The joint distribution turns out to be a Gaussian also. This joint distribution needs to satisfy the Markov properties of the graph which in essence encodes conditional independence relationships. Our goal is to construct and analyze a market on dependent variables based on a GMRF.

Imagine we are given an undirected graph $G = (V, E)$ and that each vertex $v_i \in V$ corresponds to some random variable x_i. Let the corresponding multivariate variable $x = (x_1, \ldots, x_m)^T$ be distributed as a multivariate normal (MVN). We abuse notation slightly and refer to both the vertices and the corresponding variables as x_i.

For this to be a valid GMRF, x will also have to respect the following *equivalent* **Markov properties** of G:

Pairwise independence : $x_i \perp x_j \mid x_{-ij}$ if $\{i, j\} \notin E$ and $i \neq j$

Local independence : $x_i \perp x_{-i,ne(i)} \mid x_{ne(i)} \forall i \in V$

Global independence : $x_A \perp x_B \mid x_C$ for all disjoint sets A, B, C where C separates A and B, $A, B \neq \emptyset$.

The Automated Market Maker We now define a *joint* market maker for multiple correlated variables, where the (in)dependence relationships are encoded by a Gaussian Markov Random Field. The *sufficient statistics* for the corresponding MVN are given by the vector

$$(x_i, x_i^2, \forall v_i \in V; x_i x_j, \forall (v_i, v_j) \in E)$$

First we set up the securities whose payoffs correspond to the sufficient statistics of the model. This turns out to be

$$(\mathbf{x}, \mathbf{x}\mathbf{x}^\top)$$

Then we define the cost of purchasing securities based on a potential function as

$$C(\mathbf{q}_1, \mathbf{Q}_2) = -\frac{1}{4}\mathbf{q}_1^\top \mathbf{Q}_2^{-1}\mathbf{q}_1 - \frac{1}{2}\log|-2\mathbf{Q}_2|$$

Recall that the share vector $(\mathbf{q}_1, \mathbf{Q}_2)$ corresponds to the number of outstanding shares of securities that pay off $\mathbf{x}$ and $\mathbf{x}\mathbf{x}^\top$ respectively. This corresponds to the natural parameters of the MVN and can also be written in terms of the mean vector and covariance matrix as $\mathbf{q}_1 = \Sigma^{-1}\mu$ and $\mathbf{Q}_2 = -\frac{1}{2}\Sigma^{-1}$. This means that the marginal distribution of any variable in this market can be directly obtained by a simple matrix inversion and matrix vector product since the marginal distribution of the i^{th} component is simply the Gaussian parametrized by the mean $\mu^{(i)}$ and variance Σ_{ii}.

Now we analyze the behavior of a trader in this market who may be aware of only some of the variables in this market. Such a trader should be able to represent his belief in this market by purchasing only those securities whose payoff depends only on the variables relevant to him.

For instance, the optimal trade of a trader who is only interested in x_1 is obtained as a solution to the following equations:

$$\begin{aligned}
\nabla_{\mathbf{q}_1^{(1)}} C(\mathbf{q}_1, \mathbf{Q}_2) &= m \\
\nabla_{\mathbf{Q}_2^{(1)}} C(\mathbf{q}_1, \mathbf{Q}_2) &= m^2 + v^2
\end{aligned}$$

where m and $m^2 + v^2$ are his expected values of x_1 and x_1^2. This is equivalent to

solving the minimization problem,

$$\min_{\mathbf{q}_1^{(1)},\mathbf{Q}_2^{(1)}} \left\{ C(\mathbf{q}_1, \mathbf{Q}_2) - m\mathbf{q}_1^{(1)} - (m^2+v^2)\mathbf{Q}_2^{(1)} \right\}$$

For a 2×2 covariance matrix and 2-D mean vector we can explicitly compute these values as follows.

$$\begin{aligned}
C(q_1,q_2,q_3,q_4,q_5) &= -\frac{1}{4}(q_1\ q_2)\begin{bmatrix} q_3 & q_4 \\ q_4 & q_5 \end{bmatrix}^{-1}\begin{pmatrix} q_1 \\ q_2 \end{pmatrix} - \frac{1}{2}\log\begin{vmatrix} -2q_3 & -2q_4 \\ -2q_4 & -2q_5 \end{vmatrix} \\
&= -\frac{1}{4}(q_1\ q_2)\begin{bmatrix} q_3 & q_4 \\ q_4 & q_5 \end{bmatrix}^{-1}\begin{pmatrix} q_1 \\ q_2 \end{pmatrix} - \frac{1}{2}\log(4q_3q_5 - 4q_4^2) \\
\text{Now, } (q_1\ q_2)\begin{bmatrix} q_3 & q_4 \\ q_4 & q_5 \end{bmatrix}^{-1}\begin{pmatrix} q_1 \\ q_2 \end{pmatrix} &= (q_1\ q_2)\frac{1}{q_3q_5 - q_4^2}\begin{bmatrix} q_5 & -q_4 \\ -q_4 & q_3 \end{bmatrix}\begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \\
&= \frac{1}{q_3q_5 - q_4^2}(q_5q_1^2 - 2q_1q_2q_4 + q_3q_2^2) \\
\text{So, } \nabla_{q_1}C(q_1,q_2,q_3,q_4,q_5) &= \frac{q_2q_4 - q_5q_1}{2(q_3q_5 - q_4^2)} = m \\
q_1 &= \frac{q_2q_4 + 2m(q_3q_5 - q_4^2)}{q_5} \\
\nabla_{q_3}C(q_1,q_2,q_3,q_4,q_5) &= m^2 + v^2
\end{aligned}$$

If a probability distribution satisfies the Markov properties of a given graph, then it can shown that its density factorizes in terms of functions of the variables in the cliques of the graph. That is

$$p(\mathbf{x}) = \frac{1}{Z}\prod_C \psi_C(\mathbf{x}_C)$$

where Z is the normalization constant, ψ_C are potential functions dependent on C the maximal cliques of the graph.

4.6 Conclusion

In this chapter, we have analyzed interactions between concurrently run prediction markets. We have identified the surplus that arises due to discrepancies in identical markets run in different venues. We have also been able to precisely characterize the effects of trades in a market on dependent markets. We have analyzed the behavior of partially informed traders and shown a surprising correspondence to learning algorithms.

While we have explored market interactions for a particular structure of dependencies between variables, it remains to be seen whether these results are generalizable to arbitrary relationships. We are also interested in characterizing the market semantics of other learning algorithms (especially message passing algorithms) in these graphs.

CHAPTER V

Myopic Regret Sequential Learning with Partial Feedback

5.1 Introduction

Many online ranking, recommendation, and personalization systems rely on input from multiple forecasters or experts. Combining multiple forecasters' inputs appropriately is the central goal of a rich machine learning literature, but these internet domains present a unique set of challenges to effective aggregation. In this chapter, we introduce a new learning model that captures some of the characteristic features of this forecast setting, and we present a technique to construct efficient learning algorithms for this class of problems. Parts of this chapter were accepted for presentation as *Kutty and Sami* (2010).

Internet-based Recommender Systems Expert forecasts and recommendations in internet settings present the following challenges: First, the forecasters may be a mix of best-effort forecasters and attackers with vested interests. We use a hybrid stochastic-adversarial model to capture this peculiarity. Second, as a consequence of forecast inputs arriving haphazardly over time, the algorithm not only has to be able to provide prediction based on partial availability of expert forecasts, but also detect

and mitigate the effect of cloning attacks.

In this chapter, we describe a technique to develop machine learning algorithms for forecast aggregation systems based on the metaphor of a *prediction market*. Prediction markets are markets that allow traders to bet on securities whose value depends on a future event. One form of prediction markets, is a market scoring rule where traders earn rewards proportional to the reduction in "loss" (measured using a proper scoring rule) caused by their trades. Our approach involves designing a learning algorithm by tracking a budget for each trader, and simulating a prediction market.

Prediction Market based Learning Algorithms based on prediction markets are attractive for the particular features of the domains we are interested in, because of the following reasons: First, traders' budgets allow us to control the total net impact of a single identity. By coupling traders' payoffs to the effects of their actions, and limiting their effect so that their budget is never negative, we can provide worst-case bounds against adversarial forecasters. Second, in a setting with honest agents but stochastic outcomes, a budget-proportional betting scheme (the Kelly criterion (*Kelly*, 1956)) leads to exponential growth in traders' budgets (in expectation), and thus the small initial budgets are not crippling to honest agents in the long run. Third, betting protocols have been used before in machine learning algorithms, for the reasons above (see, *e.g.*, *Shafer and Vovk* (2001)). Prediction markets are a natural extension of betting protocols to the sequential forecasting setting. Traders' profits are based on the extent to which they change forecasts, thus ensuring that merely cloning previous information is not profitable.

In this chapter, we develop an algorithm that provides a weak performance guarantee that we call *myopic regret*. This notion of regret captures loss due to damage from dishonest experts and loss of information from honest experts. However, this regret does not capture loss due to a dishonest expert's predictions affecting later

honest experts' inputs. This algorithm is based on work by *Resnick and Sami* (2007) that introduced the notion of manipulation resistance in recommendation systems.

5.2 Problem Statement

The goal of a recommendation system is to provide item recommendations for a target user from a set of items. To facilitate this recommendation, the algorithm has access to the item ratings of other users (called raters) in the system. Thus, the problem can be defined as that of predicting a label for every item based on input from other users in the system. Note that in this case the target user is fixed and irrelevant to a particular instance of the algorithm. The labels are assumed to be binary $\in \{0, 1\}$ and the input from the raters is in the interval $[0, 1]$ and is interpreted as the probability of an outcome of 1. Since all the ratings on a particular item are not available simultaneously, the recommender system takes sequentially arriving ratings as input produces a prediction as output. At some point the target user rates the item. The algorithm uses this as feedback on the quality of predictions provided by both itself and the raters.

In this scenario, the recommender system can be manipulated by malicious raters that imitate helpful raters and thus artificially boost their perceived reliability. The manipulation resistance layer defined by Resnick and Sami *Resnick and Sami* (2007) is a way of weighting the sequence of predictions on a single item produced by the recommender system due to each additional rating. Over a finite number of items in the system, this layer renders the recommender system provably manipulation resistant – in the sense that the loss incurred due to malicious raters is limited as is the information lost from honest ones.

We extend this work as follows. First, we cast the problem in a generalized online learning context. We provide a justification for using a prediction market approach for machine learning algorithms. Additionally, we study a setting where the true label

or outcome is not always known. Thus, we define a model and related analysis for this limited feedback setting.

Related Work The idea of making it prohibitive for attackers to enter the system is related to results on cloning-proof voting schemes that work when there is a small cost to creating an account *Wagman and Conitzer* (2008). In other prior work *Yu et al.* (2009) specifically consider a system to thwart cloning attacks in recommender systems. They do not consider a sequential ordering on the experts; further, unlike our model, their model assumes a strong similarity between the actual outcomes and the forecasts of at least one expert. In *Awerbuch and Kleinberg* (2008), a generalized multi-armed bandit model of recommendation is studied where there are multiple users selecting an arm in each round. The users form coalitions allowing them to exchange information; however, some of these users are dishonest. The actions describe the choice of a source of recommendations, and the quality of the actions is allowed to change over time. The goal of the algorithm is to minimize the total cost incurred by honest agents. They achieve a regret of $O(T^{3/4}n \log^4 n)$. However, none of these models explicitly capture the sequential nature of information or offer a hybrid stochastic-adversarial analysis of the experts. Further, our work benchmarks our algorithms against the optimal *combination* of experts. We call the previous algorithms where all experts provide predictions on every round *insomniac* algorithms following the nomenclature in *Freund et al.* (1997). In this section we will focus on a model that extends the insomniac model to allow so-called *specialists* or *sleeping experts*. This is a model of online learning with expert advice, where the experts are allowed to abstain from giving their predictions. The motivation for this model comes from various real-world scenarios where the goal is to combine the predictions of learning algorithms that are trained for particular kinds of input instances, e.g., in document classification or rating agencies. These algorithms may choose not to provide pre-

dictions on instances that are not their specialty. Additionally, some of the experts may be adversarial agents, who may provide their input strategically. One of the key questions to address in this case is what a reasonable benchmark would be. Directly applying that the usual best expert/combination does not work per se – what, for instance, would 'best' really mean in this case? Current literature deals with this in the following ways.

Kleinberg et al. (2008) deal with a best expert-type scenario. They set up the problem so that there is no exogenous outcome being predicted. Instead, the experts are viewed as actions and the goal is to pick the best action in each round. Each expert incurs a loss in each round. At the end of each round, the algorithm either observes the entire loss vector (full feedback) or only the loss of the expert they choose (partial feedback). They benchmark their algorithm against the best ordering of experts; the prediction in each round is compared against the best awake expert in that round. They analyze their algorithm in two scenarios: one where the loss on the experts are generated stochastically and the other where it is generated adversarially. In the stochastic case with full feedback, their regret is dependent on the inverse of the difference in expert loss means. In the partial feedback setting there is an additional multiplicative factor of $\log T$. Both of these algorithms are variants on the respective insomniac versions. In the fully adversarial case, the bounds they achieve are $O(\sqrt{Tn \log n})$ and $O(\sqrt{Tn^2 \log n})$.

The goal in *Freund et al.* (1997) is to compare against a best linear combination of awake experts. They provide a general reduction from an insomniac algorithm to a sleeping version. However their bound weights the regret in each round by the total weight of awake experts in that round. Thus, in a case where a majority of high-weight experts are asleep, the actual regret of the algorithm is allowed to be high even though the accounted regret falls within the given bounds. This type of bound may be relevant in scenarios where the total weight of the awake experts affects the

significance of a round.

Partial availability of expert advice is one way in which the algorithm is forced to work with incomplete or missing information. In this section, we consider another setting where the algorithm receives limited information. In this variant, the algorithm receives feedback on its performance only in certain situations. Partial availability of feedback has been modeled in one of two ways. In the first case, the outcome is itself only revealed to the algorithm under certain conditions. In the other, the algorithm's goal is to choose between actions in each round, and its feedback is restricted to the action that is chosen in that round. The challenge in both these cases is to make good predictions with strong guarantees while dealing with this lack of information.

In prior work partial feedback has been studied as the Apple Tasting problem *Helmbold et al.* (1992). The problem is set up as the task of inspecting and either accepting or rejecting apples from a basket. Maximal loss is incurred when either a bad apple is accepted or a good apple is rejected. To model partial feedback, their model specifies that 'accept' always receives feedback, but a 'reject' never does. The goal is to minimize loss in this setting. Their solution relies on an underlying insomniac learning algorithm with a known mistake bound. Their loss is bounded with respect to this algorithm's bounds.

In this chapter, we consider the effect of partial feedback on a model where the goal is to do almost as well as the optimal combination of expert advice rather than the more restrictive mistake bound model. Partial feedback in our model is defined so that the outcome is revealed every time the prediction exceeds a predefined threshold and is not guaranteed to be revealed otherwise. In other words, if the prediction exceeds the threshold, the outcome is revealed with probability 1, and if not, the outcome is revealed with some probability < 1. We show that our algorithm achieves a regret bound of $O(n\sqrt{T}\log T)$.

5.3 Model

We provide the highlights of this model below. First some notation. Let N be the total number of experts. Let M be the total number of rounds. Let $L(\cdot, \cdot)$ be the loss function that takes as input the true label $\in \{0, 1\}$ (or equivalently {LO, HI}) and a prediction $\in [0, 1]$. The loss function is convex and has range $\in [0, 1]$. Here we focus on the quadratic loss function.

We define $\sigma(N)$ as a permutation of the set $\{1, \ldots, N\}$. Let the sequence $E = \langle e_1, \ldots, e_n \rangle \subseteq \sigma(N)$. Thus, the length of E is $|E| = n \leq N$. For $a, b \in E$,

- we say $a \preceq b$ if a precedes or is equal to b in the sequence E
- we say $a = b \backsim 1$ if a immediately precedes b in the sequence E

Model

For a round $i \in \{1, \ldots, M\}$:

1. Nature selects the i^{th} label $\in$ {LO, HI} according to some known prior p_0. Here p_0 is interpreted as the probability of HI.
2. $E \subseteq \sigma(N)$ is stochastically picked from some unknown distribution. This defines the sequence of participating experts.
3. For every participating expert $j \in \langle e_1, \ldots, e_n \rangle$
   (a) j provides a prediction r_j to some aggregation process
   (b) The aggregation outputs q_j which is a function of all q_e where $e \preceq j$
   (c) PFIL-Pred takes q_j as input and produces $\tilde{q}_j$ as output
4. If $\tilde{q}_{e_n} \geq q_{cutoff}$, the label l^i is revealed to PFIL-Rep

5.4 Algorithm

The Partial Feedback Influence Limiter has two modules. The first PFIL-PRED makes updated influence limited predictions based on the sequential output of the aggregation process. This module is called at n times in *each* round. PFIL-REP updates the reputation of the experts based on their incremental informativeness once feedback int he form of the true label has been received. This module is called only once at the end of each round.

We will now describe the modules for The Partial Feedback Influence Limiter:

Partial Feedback Influence Limiter

Parameters:

λ: for all experts $e \in \{1, \ldots, N\}$, initialize reputations at round 1, $R_e \leftarrow e^{-\lambda}$

p_0: known prior, $\tilde{q_0} \leftarrow p_0$

PFIL-Pred (q_j):

For a round $i \in \{1, \ldots, M\}$:

Parameter:	ϵ: parameter for the biased coin
Internal state:	$\tilde{q}_{j \backsim 1}$: output from previous call

1. Compute influence limited prediction

   (a) $\beta_j^i \leftarrow \min(1, \epsilon R_j)$

   (b) $\tilde{q_j} \leftarrow (1 - \beta_j^i)\tilde{q}_{j \backsim 1} + \beta_j^i q_j$

2. toss a biased coin with $\Pr(heads) = \epsilon$

   if ($\tilde{q_j} < q_{cutoff}$ and $heads$) output q_{cutoff}

   else output $\tilde{q_j}$

PFIL-Rep (q_j, l^i)**:**

For a round $i \in \{1, \ldots, M\}$:

Internal state:	*heads*: outcome of biased coin from PFIL-PRED
	R_j: current reputation of expert j
	ϵ: parameter for the biased coin from PFIL-PRED

1. if $\tilde{q}_j \geq q_{cutoff}$

   update reputation $R_j \leftarrow R_j + \beta_j^i[L(l^i, \tilde{q}_{j\backsim 1}) - L(l^i, q_j)]$

2. if $\tilde{q}_j < q_{cutoff}$ and *heads*

   update reputation $R_j \leftarrow R_j + \frac{\beta_j^i[L(l^i, \tilde{q}_{j\backsim 1}) - L(l^i, q_j)]}{\epsilon}$

5.5 Myopic Regret

In this section we will compute the total myopic regret of the algorithm as a function of the loss induced by dishonest experts and the loss of information from honest experts due to influence-limiting. This regret does not account for loss due to imperfect aggregation.

5.5.1 Limited Damage

The limited damage theorem says that the algorithm is secure against cloning attacks when the number of clones is finite and bounded. Note that since an attacker has no control over ϵ, that part of the algorithm cannot be used in an attack.

Proposition V.1. *For any iteration of the algorithm R_j is always non-negative. That is, $R_j \geq 0$. Similary for β_j^i.*

Proof. For $R_j \geq 1/\epsilon \geq 1$, $\beta_j^i = 1$ and $R_j \geq 0$. For $R_j < 1/\epsilon$, $\beta_j^i = \epsilon R_j$ and either $R_j \geq R_j(1-\epsilon) \geq 0$ or $R_j \geq 0$. □

Let Δ_j^i denote expert j's myopic impact on round i i.e., the *reduction* in prediction loss.

Proposition V.2. *The reduction of incremental prediction loss (i.e., impact of player j on round i's prediction) is at least the expected change in his reputation on i's prediction, i.e.,*

$$\Delta_j^i \geq \mathrm{E}[\Delta \mathrm{R}_\mathrm{j}^\mathrm{i}]$$

for a fixed value of β_j^i.

Note that impact of a expert is defined as the incremental gain that the expert causes. Thus, it is the improvement in prediction due to the expert.

Proof.

$$\begin{aligned}
\Delta_j^i &\stackrel{def}{=} L(l^i, \tilde{q}_{j\backsim 1}) - L(l^i, \tilde{q}_j) \\
&= L(l^i, \tilde{q}_{j\backsim 1}) - L(l^i, (1-\beta_j^i)\tilde{q}_{j\backsim 1} + \beta_j^i \tilde{q}_j) \\
&\geq L(l^i, \tilde{q}_{j\backsim 1}) - (1-\beta_j^i) L(l^i, \tilde{q}_{j\backsim 1}) - \beta_j^i L(l^i, \tilde{q}_j) \\
&= \beta_j^i [L(l^i, \tilde{q}_{j\backsim 1}) - L(l^i, \tilde{q}_j)] = \mathrm{E_c}[\Delta \mathrm{R}_\mathrm{j}^\mathrm{i}]
\end{aligned}$$

where $\mathrm{E_c}[\Delta \mathrm{R}_\mathrm{j}^\mathrm{i}]$ is the expected value of the change in reputation over the random coin tosses. □

Let B_j be a distribution over the sequence $(\beta_j^1, \ldots, \beta_j^m)$ as generated during m iterations for expert j and the outcome of the random coin tosses have distribution c.

Proposition V.3. *Expected net decrease in incremental prediction error due to j over all rounds,*

$$\mathrm{E}[\Delta_\mathrm{j}] \geq -\mathrm{e}^{-\lambda}$$

Proof. Since $R_j \geq 0$ and the initial value of $R_j = e^{-\lambda}$, R_j can reduce by at most this much over all rounds and the expectation of change in R_j can never be less than this.

$$\begin{aligned}
\mathrm{E_{B_j}}[\Delta_\mathrm{j}] &= \mathrm{E_{B_j}}[\sum_\mathrm{i} \Delta_\mathrm{j}^\mathrm{i}] \\
&\geq \mathrm{E_{B_j}}[\sum_\mathrm{i} \mathrm{E_c}[\Delta \mathrm{R_j^i}]] \\
&= \mathrm{E_{B_j}}[\mathrm{E_c}[\sum_\mathrm{i} \Delta \mathrm{R_j^i}]] = \mathrm{E_{B_j}}[\mathrm{E_c}[\Delta \mathrm{R_j}]] \\
&\geq \mathrm{E_{B_j}}[-\mathrm{e}^{-\lambda}] \\
&= -e^{-\lambda}
\end{aligned}$$

where $\mathrm{E_{B_j}}[\Delta_\mathrm{j}]$ is the expected value of reduction in prediction loss over m rounds over the distribution B_j on $(\beta_j^1, \ldots, \beta_j^m)$. □

Using the fact that budget changes are tied to the actual increase or decrease in loss due to an expert, we immediately get the following result:

Theorem V.4. *(Limited Expected Damage) If an attacker controls η experts, the total expected increase in prediction loss is at most $\eta e^{-\lambda}$ over all rounds where the expectation is over the random coin tosses of the algorithm. This result is with respect to an adversarial model of experts whose forecasts may be arbitrarily chosen.*

5.5.2 Limited Expected Information Loss

In this model, each expert j is assumed to have some private information that tells him something about the the world. Specifically, the expert sees the world as divided into disjoint and complete subsets where any two elements in a particular subset are indistinguishable to him. The reported predictions of all experts and a realization of the features of a round will define a particular state of the world. Obviously the world actually exists in a particular state. A stochastic assumption on these states says that each round is drawn iid from a distribution on these states. This will allow

us to define informativeness of a user with respect to the refinement of partitions that she induces. Note that a smaller subset does not always mean a more accurate prediction i.e., the probability that the target will like the round does not necessarily always grow towards the actual label. Since we are assuming that each round is either liked (HI) or disliked (LO), and the identification of the partition is correct, we can accurately predict the probability that an round that lies in this component is liked. This is ideal; we would like to say that the algorithm does not differ too much from this ideal – i.e., not too much information is lost due to discounting some of the experts' recommendations.

First define informativeness as:

$$\begin{aligned} I(\hat{\pi}_j|\hat{\pi}_{j\backsim 1}) &\stackrel{\text{def}}{=} \sum_{\omega\in\Omega} p_\omega[L(l(\omega), q_{j\backsim 1}(\omega)) - L(l(\omega), q_j(\omega))] \\ &= \sum_{s\in\hat{\pi}_j} p_s[q_j(s)\{L(HI, q_{j\backsim 1}(s)) - L(HI, q_j(s))\} \\ &\qquad +(1-q_j(s))\{L(LO, q_{j\backsim 1}(s)) - L(LO, q_j(s))\}] \\ &= \sum_{s\in\hat{\pi}_j} p_s D(q_j(s)||q_{j\backsim 1}(s)) \end{aligned}$$

where $D(q||r) = q[L(HI,r) - L(HI,q)] + (1-q)[L(LO,r) - L(LO,q)]$. Here $q_j(s)$ is the probability that the target outcome will be HI in state s as identified by the information received from experts 1, 2, ..., j i.e., s is a component of $\hat{\pi}_j$ and $q_j(s)$ is the fraction of rounds in s that are labelled HI. Note that at this stage, it is not known exactly which component of $\hat{\pi}_j$ the true state of the world lies in. This is reflected in the informativeness by summing over all possible states. This, of course, means that where you are in the sequence could change an expert's informativeness. Thus, we would need to assume that an expert cannot conspire to change the sequence. In other words, this bound assumes that the attackers are *passive* in this sense. Note that the damage bound does not require this. We do not need to assume the same sequence over all rounds, since the stochastic assumption can include in the state of

the world all possible sequences of predictions as well. If the expert could pick where he occurs in the sequence he could use the probability distribution on the states of the world to compute the optimal placement in the sequence so as to maximize his informativeness in each round.

Now consider the growth of R_j, in each iteration. R_j is updated as:

$$R_j^i \leftarrow R_j^{i-1} + \beta_j^i[L(l^i, \tilde{q}_{j\backsim 1}) - L(l^i, q_j)]$$

where $\tilde{q}_{j\backsim 1}$ is the prediction based on previous experts and q_j is j's prediction. Thus, j's reputation grows differently when the expert is influence limited than when he is not.

Consider a fixed round i and β_j.

Case 1 $R_j \geq 1/\epsilon$

In this case, $\beta_j = min(1, \epsilon R_j) = 1$. Thus, if expert j causes the prediction of a component to change from u to q, the reputation is updated with probability q as

$$R_j^i \leftarrow R_j^{i-1} + [L(HI, u) - L(HI, q)]$$

and with probability $1 - q$ as

$$R_j^i \leftarrow R_j^{i-1} + [L(LO, u) - L(LO, q)]$$

Thus, j can expect the change in his reputation to be:

$$\begin{aligned} E[R_j^i - R_j^{i-1}] &= q[L(HI, u) - L(HI, q)] + (1 - q)[L(LO, u) - L(LO, q)] \\ &= D(q||u) \end{aligned}$$

Case 2 $R_j < 1/\epsilon$

In this case, $\beta_j = min(1, \epsilon R_j) = \epsilon R_j$ and the expert is influence limited. The reputation is updated with probability q as

$$R_j^i \leftarrow R_j^{i-1}(1 + \epsilon[L(HI, u) - L(HI, q)])$$

and with probability $1 - q$ as

$$R_j^i \leftarrow R_j^{i-1}(1 + \epsilon[L(LO, u) - L(LO, q)])$$

Note that if $\tilde{q}_{iter} < q_{cutoff}$, with probability $1 - \epsilon$, R_j remains unchanged and the following equations still hold. Thus,

$$\begin{aligned} E[\log R_j^i] &= \log R_j^{i-1} + q \log(1 + \epsilon[L(HI, u) - L(HI, q)]) \\ &\quad + (1 - q) \log(1 + \epsilon[L(LO, u) - L(LO, q)]) \\ &= \log R_j^{i-1} + \mathrm{GF}_\epsilon(q||u) \end{aligned}$$

where

$$\begin{aligned} \mathrm{GF}_\epsilon(q||u) &\stackrel{\text{def}}{=} q \log(1 + \epsilon[L(HI, u) - L(HI, q)]) \\ &\quad + (1 - q) \log(1 + \epsilon[L(LO, u) - L(LO, q)]) \end{aligned}$$

and the expectation is over the random coin tosses and q. This is the change expected once the component is fixed. Averaging over all components, we have

$$\mathrm{EGF}_\epsilon(\hat{\pi}_j||\hat{\pi}_{j\backsim 1}) \stackrel{\text{def}}{=} \sum_{s \in \hat{\pi}_j} p_s \mathrm{GF}_\epsilon(q_j(s)||q_{j\backsim 1}(s))$$

Note that for MSE loss, and with $u = q + y$ and $\overline{q} = 1 - q$

$$\begin{aligned}
\mathrm{GF}_\epsilon(q||u) &= q\log(1+\epsilon[(1-(q+y))^2-(1-q)^2]) \\
&\quad +(1-q)\log(1+\epsilon[(q+y)^2-q^2]) \\
&= q\log(1+\epsilon[(\overline{q}-y))^2-\overline{q}^2])+\overline{q}\log(1+\epsilon[2qy+y^2]) \\
&= q\log(1+\epsilon[y^2-2\overline{q}y])+\overline{q}\log(1+\epsilon[y^2+2qy])
\end{aligned}$$

Lemma V.5. *For the quadratic scoring rule (MSE) loss, for all $q, u \in [0,1]$, $GF_\epsilon(q||u) \geq \frac{\epsilon D(q||u)}{2}$.*

Proof. Key observation: $GF_\epsilon(q||u) = GF(q||u)$ for $\epsilon = 1$ and

$GF_\epsilon()$ is a concave function[1].

First consider the function $\log(1+\epsilon c)$ for constant (wrt ϵ) c. Observe that the second derivative is

$$\begin{aligned}
\frac{\delta^2}{\delta\epsilon^2}\log(1+\epsilon c) &= \frac{\delta}{\delta\epsilon}\left(\frac{c}{1+\epsilon c}\right) \\
&= \frac{-c^2}{(1+\epsilon c)^2}
\end{aligned}$$

which is negative for any real value of c.

Thus, the second derivative (wrt ϵ) of $GF_\epsilon(q||u)$:

$$\begin{aligned}
\frac{\delta^2}{\delta\epsilon^2}\mathrm{GF}_\epsilon(q||u) &= \frac{\delta^2}{\delta\epsilon^2}\left(q\log(1+\epsilon[y^2-2\overline{q}y])+\overline{q}\log(1+\epsilon[y^2+2qy])\right) \\
&\leq 0 \quad \texttt{(for any q and u)}
\end{aligned}$$

[1] A function f is concave iff for x, y in the domain of f and $0 \leq t \leq 1$ $f(tx+(1-t)y) \geq tf(x)+(1-t)f(y)$

In other words, $GF_\epsilon(q||u)$ is a concave function of $0 \leq \epsilon \leq 1$ and thus,

$$\begin{aligned} GF_\epsilon(q||u) &\geq \epsilon GF_1(q||u) + (1-\epsilon)GF_0(q||u) \\ &= \epsilon GF(q||u) + (q+\overline{q})\log 1 \\ &= \epsilon GF(q||u) + 0 \\ &\geq \epsilon D/2 \end{aligned}$$

□

The last inequality was proved in *Resnick and Sami* (2007). We will also need the following lemma for Theorem V.8.

Lemma V.6. *For the quadratic loss function, for all $q, u \in [0,1]$, and for any $t \geq 1$, $GF_t(q||u) \geq 0$ where*

$$\begin{aligned} GF_t(q||u) \stackrel{\text{def}}{=} & [q\log(t + L(HI,u) - L(HI,q)) + \\ & (1-q)\log(t + L(LO,u) - L(LO,q))] - \log t \end{aligned}$$

This was proved in *Resnick and Sami* (2007). We will reproduce the proof here for completeness. It is easy to see that $GF_t'(y) \geq 0$, which is sufficient to show that $GF_t(q||u)$ is nonnegative, because $GF_t(q,q) = 0$.

Lemma V.7. *Suppose $\hat{\pi}_j$ and $\hat{\pi}_{j\backsim 1}$ are two partitions such that $\hat{\pi}_j$ is a refinement of $\hat{\pi}_{j\backsim 1}$. For each state ω, let $\mathbf{q}_j(\omega) \stackrel{\text{def}}{=} E(l(\omega)|\hat{\pi}_j)$ be the optimal prediction function given partition $\hat{\pi}_j$. Let $\mathbf{u}(\omega)$ be any function that is constant on each component of $\hat{\pi}_{j\backsim 1}$. Then,*

$$EGF_\epsilon(\mathbf{q}_j||\mathbf{u}) \geq \frac{\epsilon}{2}\, I(\hat{\pi}_j||\hat{\pi}_{j\backsim 1})$$

in the quadratic loss model.

Proof. For simplicity, we prove the result assuming for a single component $s_{j\frown 1}$ of $\hat{\pi}_{j\frown 1}$; the stated result follows easily by averaging over all such components.

Suppose component $s_{j\frown 1} \in \hat{\pi}_{j\frown 1}$ has been identified. Corresponding to $s_{j\frown 1}$, there is some set S of components of $\hat{\pi}_j$, such that $\cup_{s\in S}\, s = s_{j\frown 1}$. Now since $\mathbf{u}$ is constant on each component of $\hat{\pi}_{j\frown 1}$, we can define $u = \mathbf{u}(\omega)$ for $\omega \in s_{j\frown 1}$.

Let $q_{j\frown 1} \stackrel{\text{def}}{=} E(l(\omega)|\hat{\pi}_{j\frown 1})$ be the optimal prediction for $\omega \in s_{j\frown 1}$ (recall that this is constant over $s_{j\frown 1}$) and $q_j(s) \stackrel{\text{def}}{=} \mathbf{q}_j(s)$, $s \in S$, *i.e.* $q_j(s)$ is the optimal prediction for a state in s.

Recall that we have assumed that $s_{j\frown 1}$ (and hence S) has been identified. Thus we may define p_s as the probability of component s, so that $\sum_{s\in S} p_s = 1$. These probabilities are assumed to be common knowledge (stochastic assumption).

Now,

$$\begin{aligned}
EGF_\epsilon(\hat{\pi}||u) &= \sum_{s\in S} p_s \mathrm{GF}_\epsilon(q_j(s)||u) \quad \text{(by definition)} \\
&\geq (\epsilon/2) \sum_{s\in S} p_s D(q_j(s)||u) \quad \text{(from Lemma 5)} \\
&\geq (\epsilon/2) \sum_{s\in S} p_s D(q_j(s)||q_{j\frown 1}) \quad \text{(see note below)} \\
&= (\epsilon/2) I(\hat{\pi}_j||\hat{\pi}_{j\frown 1}) \quad \text{(by definition)}
\end{aligned}$$

Note: This inequality follows from the fact that $q_{j\frown 1}$ is the optimal prediction given information $\hat{\pi}_{j\frown 1}$, *i.e.*, it minimizes expected loss among all functions $\mathbf{u}$ that are constant on components of $\hat{\pi}_{j\frown 1}$, where the expectation is over the probabilities p_s.If u is not optimal, $D(q_j(s)||u)$ can only go up in expectation (over components s). □

We can use the fact that trades are proportional to current budgets to prove a result on the expected growth of reputation among honest experts, thereby bounding the information lost from these experts:

Theorem V.8. *(Limited Expected Information Loss) Suppose expert j has made predictions for m rounds. Let h_j denote the expected reduction in prediction loss due to j's prediction. Then, for all sufficiently large m, expert j's expected reputation (with MSE loss) is bounded below by*

$$E(R_j) \geq mh_j - (2\lambda/\epsilon) + (2/\epsilon)\log\epsilon - (2/\epsilon)\log[mh_j\epsilon - 2\lambda + 2\log\epsilon]$$

Here the expectation is with respect to a stationary distribution on the forecasts of honest experts.

Proof. As discussed above, the reputation of an informative expert j grows in two phases. Here we show that while ϵR_j is below 1, it tends to grow exponentially. Once the reputation hits $1/\epsilon$, ϵR_j grows linearly. To this end, we define a function $G : \Re^+ \to \Re$:

$$G(x) = x + 2\log x$$

We observe that $G(x)$ is increasing, invertible, and concave. Also, note that for the initial value of the reputation,

$$\begin{aligned} G(\epsilon R_j) &= G(\epsilon e^{-\lambda}) \\ &= \epsilon e^{-\lambda} + 2\log(\epsilon e^{-\lambda}) \\ &= \epsilon e^{-\lambda} + 2\log\epsilon + 2\log(e^{-\lambda}) \\ &> -2\lambda + 2\log\epsilon \end{aligned}$$

Now, let $\overline{G}^{(i)}$ denote the expected value of $G(\epsilon R_j)$ after rounds $1, 2, \cdots, i$. $\overline{G}^{(0)} = G(\epsilon e^{-\lambda})$.

Claim: $\overline{G}^{(i+1)} \geq \overline{G}^{(i)} + \epsilon h$

Consider the distribution of $G(\epsilon R_j)$ after i rounds. Let g be any possible value in this distribution. We show that, conditioning on $G(\epsilon R_j) = g$ after round i, the

expected value of G after round $i+1$ is at least $g+\epsilon h$. Note that $E(G(\epsilon R_j)) = E(\epsilon R_j) + 2E(\log \epsilon R_j)$. When $\epsilon R_j > 1$, we will show that ϵR_j increases by ϵh in expectation. When $\epsilon R_j \leq 1$, we will show that $2\log \epsilon R_j$ increases by ϵh in expectation. In either case, the other term does not decrease in expectation.

Case (i) : $g < 1$. In this case, $\epsilon R_j + 2\log \epsilon R_j < 1$, and so $\epsilon R_j < 1$ and j is influence limited. Consider the logarithmic term $2\log x$ in $G(x)$. The experts before j have combined information represented by the partition $\hat{\pi}_{j\frown 1}$; thus, none of them could have distinguished between two states in the same component of $\hat{\pi}_{j\frown 1}$. Thus, the predictions on round i just before j's prediction is a function that is constant on components of $\hat{\pi}_{j\frown 1}$. The influence-limited prediction $\tilde{q}_{j\frown 1}$ is therefore also a function that is constant on $\hat{\pi}_{j\frown 1}$. Thus, by Lemma V.7, the expected increase in the $\log \epsilon R_j$ term from the ith to the $i+1$st round is at least $\epsilon h/2$. Since log is a monotonically increasing function, the linear term also increases in expectation. Thus, the expectation of G after $i+1$ rounds must be at least $g+\epsilon h$.

Case (ii) : $g \geq 1$ In this case, $\epsilon R_j \geq 1$ and j has full credibility with $\beta_j = 1$. By the same argument as in case (i), the previous predictions $\tilde{q}_{j\frown 1}$ is a function that is constant on $\hat{\pi}_{j\frown 1}$. Thus, as shown, R_j increases in expectation by $D(\hat{\pi}_j||\hat{\pi}_{j\frown 1})$. By definition of informativeness $I(\hat{\pi}_j||\hat{\pi}_{j\frown 1})$, the expected value of ϵR_j increases by at least ϵh. By lemma V.6, with $t = \epsilon R_j \geq 1$, the expected value of the logarithmic term does not reduce. Thus, in this case too, the expected value of G after $i+1$ rounds must be at least $g+\epsilon h$.

As this is true conditioned on any value of g, it must be true in expectation. Thus, $\overline{G}^{(i+1)} \geq \overline{G}^{(i)} + \epsilon h$, and hence, $\overline{G}^{(m)} \geq \overline{G}^{(0)} + m\epsilon h > m\epsilon h - 2\lambda + 2\log \epsilon$.

For

$$m \geq \frac{1 + 2\lambda - 2\log \epsilon}{\epsilon h}$$

we have $m\epsilon h - 2\lambda + 2\log \epsilon \geq 1$ and thus, $\log[\epsilon m h - 2\lambda + 2\log \epsilon] \geq 0$.

Setting $r = \epsilon mh - 2\lambda + 2\log\epsilon - 2\log[\epsilon mh - 2\lambda + 2\log\epsilon]$, we see that

$$\begin{aligned} G(r) &= r + 2\log r \\ &= r + 2\log[\epsilon mh - 2\lambda + 2\log\epsilon - 2\log(\epsilon mh - 2\lambda + 2\log\epsilon)] \\ &\leq r + 2\log[\epsilon mh - 2\lambda + 2\log\epsilon] \quad \texttt{(since } \log(\epsilon mh - 2\lambda + 2\log\epsilon) \geq 0\texttt{)} \\ &= mh\epsilon - 2\lambda + 2\log\epsilon < \overline{G}^{(m)} = G(E(\epsilon R_j)) \end{aligned}$$

As G is an increasing function, it follows that $E(\epsilon R_j) \geq r = mh\epsilon - 2\lambda - 2\log(mh\epsilon - 2\lambda)$ and

$$E(R_j) \geq mh - (2\lambda/\epsilon) - (2/\epsilon)\log[mh\epsilon - 2\lambda]$$

□

Tying this result to that of Proposition V.2, we have that the expected reduction in prediction loss due to expert j over m rounds is at least $mh - (2\lambda/\epsilon) - (2/\epsilon)\log[mh\epsilon - 2\lambda]$, where the expectation is over the distribution on j's influence limit (i.e., β_j), the random coin tosses and the stochastic assumption on the rounds. Note that if the expert were not influence limited (had β_j always been 1), the expected impact would have been mh. Thus, at most $(2\lambda/\epsilon) + (2/\epsilon)\log[mh\epsilon - 2\lambda]$ units of information have been lost to accommodate influence limiting from a expert j.

5.5.3 Bounded Myopic Regret

In addition to the loss of information due to influence limiting, we also incur a loss of at most 1 for those rounds i for which expert predictions are ignored and a boosted probability of q_{cutoff} is reported. Thus, if we assume ψ to be the probability of the event that $\tilde{q}_j < q_{cutoff}$ then the probability that boosted probability is output by the algorithm is $\psi\epsilon$. Then, the gain in prediction over all rounds and all experts

in an execution of the algorithm is at least

$$(1 - \psi\epsilon) \sum_{j=1}^{n} [mh_j - (2\lambda/\epsilon) - (2/\epsilon) \log[mh\epsilon - 2\lambda]] - \psi\epsilon$$

Picking $\epsilon = 1/\sqrt{m}$ gives us a myopic bound of $O(m^{1/2} \log m)$ per round. Intuitively, this choice of ϵ allows us to minimize regret while maximizing information gained.

As noted earlier, this notion of regret is myopic in that it fails to capture the effect that dishonest predictions have on later honest experts' predictions. In other words, we do not capture the loss due to aggregating dishonest predictions in making predictions attributed to honest experts.

Combining these two results we obtain the following regret bound:

Corollary V.9. *The Partial Feedback Influence Limiter achieves an asymptotic regret bound of*
$O(n\sqrt{m} \log m)$ *for an appropriate choice of algorithm parameters* ϵ *and* λ *where regret is measured with respect to the expected reduction in prediction loss due to* n *experts across* m *rounds.*

5.6 Discussion and Extensions

5.6.1 Alternative Feedback Models

In this chapter, we considered a model in which feedback is not always available when the predicted probability of a '1' label is below a threshold. This is natural in a setting where '1' is interpreted as the high-value prediction. However, there may be other natural models of partial feedback under different circumstances. For example, feedback may be expected whenever the probability placed on any single label is high; alternatively, it may be expected only when the probability is not concentrated on

any one label. Our technique can be extended directly to these alternative models of feedback.

5.6.2 Betting Protocols and Prediction Markets

The use of a betting analogy is a powerful tool in online learning algorithms: the state of the algorithm is represented as a *capital process*, such that the transition between states (i.e., changes in capital) can be represented as bets *Shafer and Vovk* (2001), *Vovk et al.* (2005). In models that require a hybrid of worst-case and expected-case analysis, such as the one we have presented and analyzed here, betting models are particularly attractive as a way to combine both objectives:

1. The allocation of initial budgets, together with a non-negative capital constraint, provide a framework to prove worst-case bounds across all possible evolutions of the system, as long as we can tie the variable to be bounded to the outcome of a bet with variable stakes.

2. We can use wealth-proportional betting strategies, scaled according to the Kelly criterion *Kelly* (1956), to prove results in expected growth of capital under stochastic informativeness assumptions, while respecting the non-negative capital constraint.

Prediction markets are markets that allow traders to bet on securities whose value depends on a future event; for example, on the Iowa Electronic Market, the outcome of a presidential election. One of the key motivations of using prediction markets as a forecasting tool is that the provide an incentive to acquire additional information and improve the current market forecast. One form of prediction markets, which is rapidly gaining in popularity, is the *market scoring rule Hanson (2003b).* In a market scoring rule, traders earn rewards proportional to the reduction in "loss" (measured using a proper scoring rule) caused by their trades; in other words, the difference in

the loss of forecasting based on market price after their trade as compared to the market price after the previous trade. The reputation update rule in Algorithm 2 roughly implements a market scoring rule: An expert wagers a fraction of her current reputation in a market to forecast the label of the current round. This technique translates the advantages of a betting/capital process model of online learning to a setting with sequential forecasts.

5.6.3 Limitations of the Technique

In the discussion above, we have higlighted the advantages of using the sequence information if available, through a weight-update algorithm based on sequential betting. Here, we remark that there are some situations in which it may be better to move away from a sequential structure, or ignore the sequence information even when available. One danger of using the sequence information is that, as the first contributor of a piece of information is disproportionately rewarded, it could create incentives to race if information is public and freely accessible. Hence, if the genuine experts are more passive than the attackers, they may command a smaller share of the total weight over time. If information is public but costly, this may still occur, but there is a countervailing advantage that the genuine expert community has been spared the cost of acquring information.

5.7 Conclusion

In this chapter, we presented a model and an algorithm that uses a sequence of expert advice to make predictions on the class label of a data point under partial monitoring conditions. Our main technique involves a reputation system based on incremental information received from the experts. We showed that for particular choices of algorithm parameters, we are able to achieve $O(n\sqrt{m}\log m)$ regret. We also considered separate information loss and damage bounds, and argued for the

utility of such a dual analysis. Different choices of the algorithm parameter allow us to shrink one bound at the expense of the other. This can be exploited with specific domain knowledge to thwart attacks from malicious entities. We also considered other solutions to this problem using existing techniques and identified cases where our algorithm performs better.

In our model for analyzing information loss, we have assumed that every additional advice received is aggregated perfectly with advice received before. In the next chapter we relax this assumption and prove a nonmyopic regret bound.

CHAPTER VI

Bounded Regret Sequential Learning of Exponential Families

6.1 Introduction

In Chapter V, we presented an algorithm based on a prediction market metaphor that gave a myopic regret bound of $O(n\sqrt{m}\log m)$ for a partial feedback setting; this regret bound does not account for loss due to imperfect aggregation of information. In this chapter we develop a new algorithm that satisfies a stricter definition of regret; in particular the algorithm we study here learns exponential family distributions in a hybrid stochastic-adversarial setting with sequentially arriving data. Parts of this chapter were accepted for presentation as *Kutty and Sami* (2011).

Similar to other learning algorithms, the advice of an expert is combined in accordance with his past performance when making a prediction. The difference here is that we use the notion of budgets (mapped to 'influence' here) and budget-proportional betting. This allows us to port the advantages of prediction markets to a learning environment. Our focus is the following hybrid model: a stochastic process generates data sequentially and a Byzantine adversary is allowed to inject noise at any point during this process. A prediction market-based model provide a natural way to capture this scenario and hence provide better bounds. It also allows for *composability*.

By this we mean that although the reliability of the experts needs to be the same across all rounds, the distribution being learned can vary. We also require that the distribution be a member of an exponential family. This approach also allows for partial aggregation and thus not all experts are required to make predictions in every round. The ability to deal with experts abstaining from giving advice in every round has been studied previously as 'sleeping experts' or 'specialists'. The particular advantage with our approach is that we are able to provide partial aggregations as we receive more information.

We develop a modular framework for the construction of algorithms based on prediction markets. The first module, the Influence Limiting and Scoring module, is domain independent; it performs a budget update and determines the influence of an expert based on his current budget. The second, domain-specific module, called the Weighted Trade Market module, will map updates of the learned forecast to trades in a prediction market.

We demonstrate the applicability of this framework by using it to construct an algorithm for a general problem: learning proceeds in sequence of rounds. In each round, a sequence of datapoints is received from multiple experts. The experts comprise adversarial attackers as well as honest experts with stochastic samples of data. The stochastic process is assumed to be modeled by an exponential family with a different parameter in each round whose value is revealed at the end of every round. The goal of the algorithm is to predict the stochastic distribution generating the data samples by evaluating the reliability of the sources; ideally the algorithm learns to discount the noisy samples provided by the adversarial experts while completely incorporating the legitimate samples provided by the honest ones in its prediction. Existing methods that do not explicitly handle sleeping experts yield trivial bounds when experts sleep strategically. Our algorithm achieves a regret bound of $O(a\log(1+e^{-r})+b\log(1+e^{r}))$ where r is an algorithm parameter and a is the number of honest experts and b is

the number of dishonest experts. We compare this algorithm to existing methods for handling sleeping experts in Section 6.8.

Related Work The connection between machine learning and prediction markets is an active area of research. *Chen and Vaughan* (2010) and *Abernethy et al.* (2011) have previously explored the connection to learning algorithms to inform the design and understanding of prediction markets. In particular, *Chen and Vaughan* (2010) consider the correspondence between prediction markets with market scoring rules and the Follow the Regularized Leader algorithm proposed by *Kalai and Vempala* (2005) and thus provide insight into the aggregation mechanism of a prediction market. *Abernethy et al.* (2011) use convex optimization techniques to design efficient markets. *Storkey* (2011) has considered machine learning algorithms, particularly aggregation methods, and has shown how to interpret these algorithms as prediction markets using appropriately defined utility functions. *Lay and Barbu* (2010) set up and simulate a prediction market to aggregate multiple classifiers and provide an interpretation for the resultant prices. They measure the performance of their algorithm experimentally. To the best of our knowledge, the use of prediction markets to construct bounded regret algorithms in sequential advice settings has not been previously explored.

For problems where the number of dishonest experts dominate the number of honest ones, our bound is comparable to *Littlestone et al.* (1991); in others it is slightly worse. However, our algorithm allows for the experts to sleep strategically which makes the resulting problem more challenging. The only other prior work that has a similar model is *Freund et al.* (1997); unlike our bound, however, their regret bound is weighted so that all rounds do not have the same significance in computing regret. *Azoury and Warmuth* (2001) consider learning exponential family distributions in a traditional online model (without experts) and provide worst case

loss bounds relative to using an offline algorithm. *Dekel et al.* (2008) are concerned with eliciting truthful advice from self-interested agents who each believe in different true distributions. Thus, rather than comparing against a particular true distribution, they use the average of all agent's beliefs as a benchmark.

6.2 Definitions and Notation

Exponential Families and Conjugate Priors Recall that a member of an exponential family $\mathcal{F}$, $P_{\boldsymbol{\beta}} \in \mathcal{F}$ assigns a probability density (with respect to some base measure) over x defined over a space $\mathcal{X}$ as follows:

$$P_{\boldsymbol{\beta}}(x) = e^{\boldsymbol{\beta}.\boldsymbol{\phi}(x) - \psi(\boldsymbol{\beta})}$$

Note that $\mathcal{X}$ could be a multi-dimensional space.

Here, the set of parameters $\boldsymbol{\beta}$ is drawn from some space $\mathcal{B}$. $\psi(\boldsymbol{\beta})$ is the log partition function and $\boldsymbol{\phi}(x)$ is the vector of sufficient statistics.

We will consider the problem of determining the value of the natural parameter $\boldsymbol{\beta}$ in a Bayesian setting. In this setting, a prior distribution on all possible values of $\boldsymbol{\beta} \in \mathcal{B}$ is known. Sequentially arriving data $x \in \mathcal{X}$ drawn according to $P_{\boldsymbol{\beta}}(x)$ is provided to the algorithm based on which it updates the distribution on $\mathcal{B}$. This posterior distribution on $\mathcal{B}$ is the prediction output by the algorithm.

In Bayesian probability theory, if the posterior distribution is of the same form as the prior probability distribution, the prior is called a *conjugate prior*. This is desirable for analytic convenience. It is known *Diaconis and Ylvisaker* (1979) that the corresponding member of the conjugate prior exponential family $\mathcal{F}^*$ defined on $\boldsymbol{\beta} \in \mathcal{B}$ has the form

$$P^*_{\mathbf{b}}(\boldsymbol{\beta}) = e^{\mathbf{b}\cdot\boldsymbol{\beta}^* - \psi^*(\mathbf{b})}$$

where ψ^* is the log-partition function, $\mathbf{b}$ is the natural parameter and the sufficient

statistics are $\boldsymbol{\beta}^* = (\boldsymbol{\beta}, -\psi(\boldsymbol{\beta}))$.

Expert identities We assume that the datapoints arrive sequentially from sources called experts. These experts have identities in $\{1, \ldots, N\}$. We assume throughout that these identities are non-forgeable. The set of expert identities is partitioned into the set of honest experts $\mathcal{H}$ and the adversarial experts $\overline{\mathcal{H}}$.

Partial permutation of participating experts Learning in our model occurs in rounds. In each round, the set of experts that participate and the order in which they provide their datapoints may vary. To formalize this, we define a partial permutation E_k that identifies the experts who participate in a round k. E_k also fixes the order in which they participate. E_k is picked adversarially.

Define $\sigma(N)$ as a permutation of the set $\{1, \ldots, N\}$. Let the sequence $E_k = \langle e_1, \ldots, e_{N_k} \rangle \subseteq \sigma(N)$. Thus, the length of E_k is $|E_k| = N_k \leq N$.

- For $a, b \in E_k$, we say $a \preceq b$ if a precedes or is equal to b in the sequence E_k
- For $a, b \in E_k$, we say $a = b \backsim 1$ if a immediately precedes b in the sequence E_k
- For $E_k = \langle e_1, \ldots, e_{N_k} \rangle \subseteq \sigma(N)$, we call $\langle e_1, \ldots, e_n \rangle$ with $n \leq N_k$ a *prefix* of E_k, $\langle e_{a_1}, \ldots, e_{a_n} \rangle$ a *subsequence* of E_k if the indices a_i are in strictly increasing order and $\langle e_{a_{n'}}, \ldots, e_{a_n} \rangle$ a *substring* of E_k if the indices a_i are consecutive natural numbers.

Structure of a round In each round k, an adversarially picked sequence E_k of length $N_k \leq N$ is given. Based on E_k the algorithm is given a sequence of possibly noisy datapoints $\tilde{\mathbf{x}}_k = (\tilde{x}_k^{(e_1)}, \ldots, \tilde{x}_k^{(e_{N_k})}) \in \mathcal{X}^{N_k}$. These samples $\tilde{x}_k^{(e_i)}$ are drawn adversarially if the identity $e_i \in \overline{\mathcal{H}}$. If $e_i \in \mathcal{H}$ the sample is drawn from $P_{\boldsymbol{\beta}_k}$ for some $\boldsymbol{\beta}_k \in \mathcal{B}$. $\boldsymbol{\beta}_k$ is itself drawn according to a known prior distribution $P_0^* \in \mathcal{F}^*$. $\boldsymbol{\beta}_k$ is

revealed to the algorithm at the end of every round. The goal of the algorithm is to predict a distribution Q_k over $\mathcal{B}$ so as to minimize the loss $\log[Q_k(\boldsymbol{\beta}_k)]$.

Attack strategies for adversarial samples In this model, we restrict the power of attackers by prescribing an attack model that captures the fact that while attackers can modify the honest data by adversarially injecting new data into the sequence, the data injected can only depend on honest data that is revealed earlier.

Let $\mathcal{A}_k^{(e_i)}$ be the attack strategy for a round k with parameter $e_i \in \overline{\mathcal{H}}$. Then $\mathcal{A}_k^{(e_i)}$ is a function that depends on the datapoints $(\tilde{x}_k^{e_1}, \ldots, \tilde{x}_k^{(e_{i\frown 1})})$. The parameter (e_i) specifies both the identity and position of the attacker in the sequence. $\mathcal{A}_k^{(e_i)}$ has access to all historical data from rounds $(1, 2, \ldots, k-1)$, including realized data $(\boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \ldots, \boldsymbol{\beta}_{k-1})$, the reputations of all the experts at the start of the kth round, etc. The only relevant constraint is that $\mathcal{A}_k^{(e_i)}$ must be independent of future data. We denote by $\mathcal{A}_k$ the collective attack strategies for all attack identities for round k.

Apart from being independent of future data, the attack datapoints are completely arbitrary, and the attacker is free to choose the timing of her data as well as their content. This is captured by the fact that the partial permutation of participating experts is adversarially determined. Thus, this notion of an attack strategy admits non-myopic attacks as well: the attacker may inject a datapoint before anticipated honest data, not because of the immediate effect of the spurious data, but because of the eventual damage it will cause after further honest data us added. Indeed, the data may be injected to improve an identity's reputation on future rounds, whence it can cause greater damage.

We will also include the adversarial choice of the sequence of participating experts in an attack strategy for a particular round.

Notation For a round k and sequence of participating experts E_k:

- For every $e_i \in \mathcal{H}$, let $x_k^{(e_i)}$ be their reported datapoints. We define $\mathbf{x}_k = (x_k^{(e_i)})$.

Thus, $\mathbf{x}_k$ is the sequence of datapoints $(x_k^{(e_i)})$ received for round k from the honest experts alone. We call this the *honest sequence*.

- We will use $\mathbf{x}_k \sim T_k$ as shorthand to indicate that the true parameter $\boldsymbol{\beta}_k$ is drawn according to the hyperdistribution P_0^* and each $(x_k^{(e_i)})$ is drawn from $P_{\boldsymbol{\beta}_k}$. Note that this sequence of $(x_k^{(e_i)})$ defines a posterior distribution conditioned on only the honest datapoints. We will denote by $\mathbf{x}_k^i \sim T_k$ the posterior distribution defined by only the honest datapoints up to and including $x_k^{(e_i)}$.

- The honest sequence $\mathbf{x}_k$ is distinct from what we call the *extended data sequence* $\tilde{\mathbf{x}}_k = (\tilde{\mathbf{x}}_k^{(e_i)})$ for $e_i \in E_k$. This is because $\tilde{\mathbf{x}}_k$ contains both honest datapoints as well as the attack datapoints provided to the algorithm in round k. Particularly, the number of datapoints included in the sequence $\mathbf{x}_k$ may be less than the number N_k of participating experts in round k.

- Let Z be the algorithm that receives the noisy sequence $\tilde{\mathbf{x}}_k$ as input in round k. The probability distribution as predicted by Z

$$Q_k \leftarrow Z[\tilde{\mathbf{x}}_k]$$

- Let $\mathbf{Z}$ be an omniscient version of Z that knows the identities of the honest experts. $\mathbf{Z}$ produces a prediction based solely and entirely on the datapoints submitted by those experts. Specifically, $\mathbf{Z}$ performs a Bayesian update based on the prior and the datapoints received from the honest experts alone.

- Let $\mathbf{Q}_k$ be the distribution predicted by $\mathbf{Z}$. Thus, this is the optimal prediction given the data.

$$\mathbf{Q}_k \leftarrow \mathbf{Z}[\tilde{\mathbf{x}}_k]$$

- To refer to the prediction made by $\mathbf{Z}$ based on a prefix of length $i \leq N_k$, we use

$$\mathbf{Q}_{k,i} \leftarrow \mathbf{Z}[\tilde{x}_1, \ldots, \tilde{x}_i]$$

  Thus, $\mathbf{Q}_{k,i}$ is the predicted probability distribution by $\mathbf{Z}$ on the k^{th} round after datapoints from the first i experts in the extended data sequence $\tilde{\mathbf{x}}_k$ have been received.

- We use G_{ik} to refer to the *incremental gain*. This is just the difference in gain between the predictions that the i^{th} and the $(i-1)^{st}$ datapoint in the extended sequence $\tilde{\mathbf{x}}_k$ induced. Here $\boldsymbol{\beta}_k$ is the true value of the parameter as revealed eventually.

$$G_{ik} = \log[Q_{k,i}(\boldsymbol{\beta}_k)] - \log[Q_{k,(i-1)}(\boldsymbol{\beta}_k)]$$

  Note that since the algorithm does not know a priori the number of participating experts, it stands to reason that it should be able to produce a prediction based on an input sequence of any size from 1 to N.

6.3 Model

We provide a high-level summary of the model below.

For an round $k \in \{1, \ldots, M\}$ the round proceeds as follows:

1. Nature selects $\boldsymbol{\beta}_k \sim P_0^* \in \mathcal{F}^*$. This prior distribution P_0^* may be different for each round.

2. An adversary selects $E_k \subseteq \sigma(N)$. This defines the sequence of participating experts. Let the participating experts be $e_i \in \langle e_1, \ldots, e_{N_k} \rangle$. Note that the number of experts that provide a prediction in round k, $|\langle e_1, \ldots, e_{N_k} \rangle| \leq N$. Each e_i is such that either $e_i \in \mathcal{H}$ or $e_i \in \overline{\mathcal{H}}$.

3. An adversary picks an attack strategy $\mathcal{A}_k$.

4. For every $e_i \in \mathcal{H}$,

$$\tilde{x}_k^{(e_i)} \sim P_{\boldsymbol{\beta}_k} \in \mathcal{F}$$

5. For every $e_i \in \overline{\mathcal{H}}$,

$$\tilde{x}_k^{(e_i)} \leftarrow \mathcal{A}_k^{(e_i)}(\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_{k-1}, \boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_{k-1}, x_k^{e_1}, \ldots, x_k^{(e_{i \backsim 1})})$$

6. Let $\tilde{\mathbf{x}}_k = (\tilde{x}_k^{(e_i)})$ for $e_i \in \langle e_1, \ldots, e_{N_k} \rangle$. Thus, this sequence includes the datapoints from *every* participating expert.

7. The algorithm Z takes $\tilde{\mathbf{x}}_k$ as input and predicts a distribution over $\mathcal{B}$ as $Q_k \in \mathcal{F}^*$.

8. The true parameter value $\boldsymbol{\beta}_k$ is revealed and the algorithm's loss is $\log\left[Q_k(\boldsymbol{\beta}_k)\right]$

Regret Rather than simply minimizing the worst case loss $\log\left[Q_k(\boldsymbol{\beta}_k)\right]$ in each round (any reasonable algorithm will perform poorly if given honest but unlikely samples), the goal of the algorithm is to minimize a hybrid stochastic-adversarial notion of *regret*, defined below.

Definition VI.1. The **regret** of algorithm Z is defined as the maximum, over all possible honest sets $\mathcal{H}$, all possible attacks $\mathcal{A}$, and all prior distributions $\in \mathcal{F}^*$ and the corresponding $\mathbf{x}_i \sim T_i$, of the reduction in total log score over all rounds relative to the omniscient algorithm $\mathbf{Z}$ that knows $\mathcal{H}$.

$$\mathrm{Reg}(Z) = \max_{\mathcal{H}, \{T_i\}, \mathcal{A}} \left\{ \sum_{k=1}^{M} E_{(\mathbf{x}_1, \mathbf{x}_2, \ldots \mathbf{x}_k) \sim (T_1, T_2, \ldots T_k)} \left[\log \mathbf{Q}_k(\boldsymbol{\beta}_k) - \log Q_k(\boldsymbol{\beta}_k) \right] \right\}$$

Note that, in the regret definition, the expectation was taken over all possible values of

$(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k)$, and not just over $\mathbf{x}_k$. The reason for this is that the state of the algorithm during round k (including, for example, budget, reputation, or influence values) may depend on the outcomes of earlier rounds. For a particular round k, we may refer to regret of the algorithm Z under attack $\mathcal{A}$ as

$$\mathrm{Reg}_k(\mathcal{A}) = \mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_\mathrm{k})\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_\mathrm{k})}\left[\log \mathbf{Q}_\mathrm{k}(\boldsymbol{\beta}_\mathrm{k}) - \log \mathrm{Q}_\mathrm{k}(\boldsymbol{\beta}_\mathrm{k})\right]$$

6.4 Algorithm

For every round k, the algorithm's goal is to make a prediction on the distribution over $\boldsymbol{\beta}_k$ given (possibly noisy) samples $\tilde{\mathbf{x}}_k = (x_k^{(e_i)})$ for $e_i \in E_k$ with $x_k^{(e_i)} \in \mathcal{X}$.

The algorithm we propose is composed of two modules: the Weighted Trade Market module and the Influence Limits and Scoring module. We provide the operational highlights of the two modules for a round $k \in \{1, \ldots, M\}$ and expert $i \in E_k$.

Note that for the first round influence y_{i1} is computed as $y_{i1} = \frac{e^{r_{i1}}}{1+e^{r_{i1}}}$ where r_{i1} is an algorithm parameter. Recall that the known prior distribution $P_0^*(\boldsymbol{\beta}) \in \mathcal{F}^*$ defined on $\boldsymbol{\beta} \in \mathcal{B}$ has the form

$$P_0^*(\boldsymbol{\beta}) = e^{\mathbf{b}_0 \cdot \boldsymbol{\beta}^* - \psi^*(\mathbf{b}_0)}$$

where ψ^* is the log-partition function, $\mathbf{b}_0$ is the value of the natural parameter of the prior distribution and the sufficient statistics are $\boldsymbol{\beta}^* = (\boldsymbol{\beta}, -\psi(\boldsymbol{\beta}))$.

6.4.1 Weighted Trade Market (WTM) module

The Weighted Trade Market (WTM) module is called every time an expert provides a prediction. This module updates its predictions sequentially and hence is called multiple times in each round. It is also called once at the end of every round when the value of the true parameter $\boldsymbol{\beta}_k$ is revealed. It then updates the gain due to each of the participating experts.

Highlights: WTM module

Given:	i's datapoint $x_k^{(i)}$ and influence $y_{ik} \in [0, 1]$
Find:	*output to environment:* updated forecast Q_k *output to ILS module:* incremental gain G_{ik}
Parameter:	D

Algorithm:

1. To compute the updated forecast Q_k:

   - First the hyperparameter is updated as

   $$\mathbf{b}_i = \mathbf{b}_{i \backsim 1} + y_{ik}(\boldsymbol{\phi}(x_k^{(i)}), 1)$$

   - This corresponds to the following distribution over $\boldsymbol{\beta}_k$

   $$Q_k(\boldsymbol{\beta}_k) = P^*_{\mathbf{b}_i}(\boldsymbol{\beta}_k)$$

2. For every expert i, incremental gain G_{ik} is computed once the true parameter $\boldsymbol{\beta}_k$ is revealed:

   $$G_{ik} = \frac{\log(P^*_{\mathbf{b}_i}(\boldsymbol{\beta}_k)) - \log(P^*_{\mathbf{b}_{i \backsim 1}}(\boldsymbol{\beta}_k))}{D}$$

   Here D is a scaling constant that depends on the range of $\boldsymbol{\beta}_k^* = (\boldsymbol{\beta}_k, -\psi(\boldsymbol{\beta}_k))$. We will now detail how the parameter D is picked. Suppose that we are given an exponential family $\mathcal{F}$ such that $|\boldsymbol{\phi}(x)|$ lies within $(0, 1)$. Let $D' > 0$ denote a sufficiently large range such that for $\boldsymbol{\beta}_k \sim P_0^*$, $|\boldsymbol{\beta}_k^*| < D'$. This implies that

for any $\boldsymbol{\beta}^*, \hat{\boldsymbol{\beta}}^*$ satisfying this property, and any x,

$$|(\boldsymbol{\phi}(x), 1)\boldsymbol{\beta}^* - \hat{\boldsymbol{\beta}}^*| \leq |\sqrt{2}\boldsymbol{\beta}^* - \hat{\boldsymbol{\beta}}^*| \leq (\sqrt{2}+1)D' \stackrel{\text{def}}{=} D \tag{6.1}$$

This D is the scaling parameter we use in the WTM.

6.4.2 Influence Limiting and Scoring (ILS) module

The Influence Limiting and Scoring (ILS) module is called at the end of every round when the value of the true parameter $\boldsymbol{\beta}_k$ is revealed. It then computes the updated influence value of each of the participating experts.

This module has a parameter, α, that is determined based on the smallest constant c for which the WTM bounded variance property (defined in Section 6.6) is satisfied; setting $\alpha = \min \frac{1}{8}, \frac{1}{4c}$ is adequate.

Highlights: ILS module

Given:	incremental gain G_{ik} and influence y_{ik} from current round internal state r_{ik}
Find:	*updated internal state:* $r_{i(k+1)}$ *output to WTM module:* influence for the next round $y_{i(k+1)} \in [0, 1]$
Parameter:	α

Algorithm:

1. Compute the variance-normalized gain based on the output incremental gain

G_{ik} for expert i of the WTM for the current round k

$$g_{ik} = \frac{1}{y_{ik}} \alpha G_{ik}$$

2. The current internal state of the module is r_{ik}. This is updated as:

$$r_{i(k+1)} = r_{ik} + S(g_{ik})$$

where the scoring function $S(g)$ is defined as:

$$S(g) \stackrel{\text{def}}{=} g - \frac{3}{4} g^2$$

3. Compute influence $y_{i(k+1)} = \frac{e^{r_{i(k+1)}}}{1+e^{r_{i(k+1)}}}$.

Figure 6.1 captures the dependencies of the various variables defined in this module. These variables perform the following functions in the analysis:

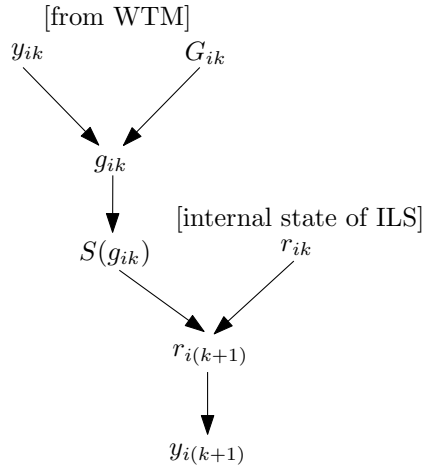


Figure 6.1: ILS variable dependencies

- $y_{ik} = \frac{e^{r_{ik}}}{1+e^{r_{ik}}}$ is simply the sigmoid or logistic function. This along with the bounded gain property allows us to limit the movement due to any one expert.

- $S(g) \stackrel{\text{def}}{=} g - \frac{3}{4}g^2$ allows us to keep the growth in reputation as strictly concave
- Defining reputation as $r_{i(k+1)} = r_{ik} + S(g_{ik})$ allows us to keep the updates additive.

6.5 An Example

Here is a specific example to illustrate our model and algorithm. Suppose that we are forecasting popularity for a sequence of movies. Each movie's has a true quality β within a bounded range $[0, 1]$ with high probability. Honest agents see previews, and perceive a sample from a normal distribution with mean β and known constant variance say 1. This family of distributions is an exponential family with $\boldsymbol{\phi}(x) = x$ and parameter β with a suitable base measure; *Wainwright and Jordan* (2008). The conjugate family is the set of all normal distributions over β. A specific conjugate distribution is indexed by a pair $\mathbf{b} = (nz, n)$; this distribution has mean z and variance $\frac{1}{n}$. For any new movie, we begin with a prior distribution P that has some hyperparameters $\mathbf{b}_0$; we denote its mean by z_0 and its precision by n_0.

Suppose we receive a report x_1 from agent 1. Bayesian update (without influence limits) would lead us to update the hyperparameters to $\mathbf{b}' = \mathbf{b} + (x_1, 1)$; these hyperparameters correspond to the Bayesian posterior. Eventually, we observe the true parameter β. Subsequently, we would compute the gain of agent 1 as $\log P_{\mathbf{b}'}(\beta) - \log P_{\mathbf{b}}(\beta)$. For an honest agent, the expected gain is the KL-divergence between the two distributions, which is equal to

$$0.5 \left[\log \frac{n_0 + 1}{n} - \frac{1}{n_0 + 1} + \frac{(x_1 - z_0)^2 n_0}{(n_0 + 1)^2} \right]$$

We can take expectations over x_1; $E(x_1 - z_0)^2 = \frac{1}{n_0} + 1$, as x_1 is the sum of the mean β (which has prior variance $1/n_0$) and an independent deviation with variance 1. With this, the expected gain is seen to be $\log(1 + \frac{1}{n_0})$. Likewise, we can also

calculate the variance of gain in terms of n_0, and verify that the variance is less than twice the expected gain ($c \leq 2$). As n_0 and z_0 were arbitrary, this holds for all honest agents. These are the conditions under which our regret bound holds, as we will see in Section 6.7.

In this setting, movie boosters may try to create fake accounts to push their favorite movies. Our algorithm would guard against this by changing the update to $\mathbf{b}' = \mathbf{b} + y_1(x_1, 1)$, where y_1 is the influence of agent 1. The influence values would change over time. Our regret bound would hold, in expectation over honest agents' signals, for any attack strategy. Importantly, this does not require any assumptions about the fraction of honest agents, their frequency of reporting, the distribution of agents on different items, etc.

6.6 Properties of the WTM

The WTM defined in Section 6.4.1 satisfies the following properties which will be used in the proofs of our main theorems. Here $\hat{G}_{ik}$ is the incremental gain due to expert i on round k when her influence $y_{ik} = 1$. We call this her gain of unlimited-influence.

6.6.1 Bounded Gain

Property 1 – bounded gain: $|G_{ik}| \leq y_{ik}$

This property shows that the influence value effectively limits the range of feasible gains. This also implies that for $y_{ik} \leq 1$, $|G_{ik}| \leq 1$ and for influence $y_{ik} = 0$, $G_{ik} = 0$.

The proof follows from the definition of the scaling factor D.

Proof.

$$
\begin{aligned}
G_{ik} &= \frac{\log(P^*_{\mathbf{b}_i}(\boldsymbol{\beta}_k)) - \log(P^*_{\mathbf{b}_{i\backsim 1}}(\boldsymbol{\beta}_k))}{D} \\
&= \frac{\mathbf{b}_i \cdot \boldsymbol{\beta}^* - \psi^*(\mathbf{b}_i) - (\mathbf{b}_{i\backsim 1} \cdot \boldsymbol{\beta}^* - \psi^*(\mathbf{b}_{i\backsim 1}))}{D} \\
&= \frac{(\mathbf{b}_i - \mathbf{b}_{i\backsim 1}) \cdot \boldsymbol{\beta}^* - (\psi^*(\mathbf{b}_i) - \psi^*(\mathbf{b}_{i\backsim 1}))}{D} \\
\text{We know,} \quad & \mathbf{b}_i = \mathbf{b}_{i\backsim 1} + y_{ik}(\boldsymbol{\phi}(x_k^{(i)}), 1) \\
\text{So, } G_{ik} &= \frac{y_{ik}(\boldsymbol{\phi}(x_k^{(i)}), 1) \cdot \boldsymbol{\beta}^* - (\psi^*(\mathbf{b}_i) - \psi^*(\mathbf{b}_{i\backsim 1}))}{D} \\
\text{Rewriting, with} \quad & \mathbf{b}_y = \mathbf{b}_{i\backsim 1} + y(\boldsymbol{\phi}(x_i), 1) \text{ we have} \\
G_{ik} &= \int_{y=0}^{y_{ik}} \frac{(\boldsymbol{\phi}(x_k^{(i)}), 1) \cdot \boldsymbol{\beta}^* - \nabla\psi^*(\mathbf{b}_y)}{D} dy \\
&= \int_{y=0}^{y_{ik}} \frac{(\boldsymbol{\phi}(x_k^{(i)}), 1) \cdot \boldsymbol{\beta}^* - \mathrm{E}_{\mathrm{P}^*_{\mathbf{b}_y}}[\boldsymbol{\beta}^*]}{D} dy
\end{aligned}
$$

The last equality follows from (*Wainwright and Jordan*, 2008, Prop.3.1) which states that the gradient of the log partition function at a point is equal to the expected value of the sufficient statistics with expectation taken with respect to the probability distribution at that point.

Now from choice of D as defined in Equation 6.1 we have that

$$|(\boldsymbol{\phi}(x_k^{(i)}), 1) \cdot \boldsymbol{\beta}^* - \mathrm{E}_{\mathrm{P}^*_{\mathbf{b}_y}}[\boldsymbol{\beta}^*]| \leq \mathrm{D}$$

Thus,

$$|G_{ik}| \leq \int_{y=0}^{y_{ik}} dy = y_{ik}$$

□

6.6.2 Concave Gain

Property 2 – concave gain: $G_{ik} \geq y_{ik}\hat{G}_{ik}$

Proof. First note that for a concave function $f(\cdot)$, we have

$$f(tx + (1-t)y) \geq tf(x) + (1-t)f(y)$$

We can rewrite the gain as a function of the influence y_{ik} as $G(y_{ik})$. Then concavity of $G(\cdot)$ in y_{ik} would imply

$$G(1 \cdot y_{ik} + 0) \geq y_{ik}G(1) + 0 \implies G_{ik} \geq y_{ik}\hat{G}_{ik}$$

To show concavity of G_{ik}, we will consider the terms constituting the gain separately. Then if each term is concave, then G_{ik} is the sum of two concave functions and is itself concave. Recall that

$$G_{ik} = G(y_{ik}) = \frac{y_{ik}(\boldsymbol{\phi}(x_k^{(i)}), 1) \cdot \boldsymbol{\beta}^* - (\psi^*(\mathbf{b}_i) - \psi^*(\mathbf{b}_{i\backsim 1}))}{D}$$

The first term $\frac{y_{ik}(\boldsymbol{\phi}(x_k^{(i)}),1)\cdot\boldsymbol{\beta}^*}{D}$ is linear in y_{ik}. The second term $\frac{(\psi^*(\mathbf{b}_i)-\psi^*(\mathbf{b}_{i\backsim 1}))}{D}$. Notice that $\psi^*(\mathbf{b}_{i\backsim 1})$ is constant with respect to y_{ik}. Now $\psi^*(\mathbf{b}_i)$ is convex in $\mathbf{b}_i$ because it is the log partition function. Since $\mathbf{b}_i = \mathbf{b}_{i\backsim 1} + y_{ik}(\boldsymbol{\phi}(x_i), 1)$ and $\mathbf{b}_{i\backsim 1}$ is constant with respect to y_{ik}, $\psi^*(\mathbf{b}_i)$ is also convex in y_{ik}. Thus, $-\psi^*(\mathbf{b}_i)$ is concave in y_{ik}. Hence, the net gain is concave in y_{ik}. □

6.6.3 Bounded Variance

Property 3 – bounded variance: $\text{Var}[\hat{G}_{ik}] \leq cE[\hat{G}_{ik}]$

That is, there exists a universal positive constant c that bounds the variance of a honest expert i's gain as a multiple of her expected unlimited-influence gain. While we have a complete proof of this property for the Gaussian family of distributions, we do not yet have a general proof. As such we treat this property as a requirement

on the particular exponential family being considered.

Bounded variance for a univariate Gaussian By definition

$$\mathcal{N}_{m,v^2}(x) = \frac{1}{\sqrt{2\pi v^2}} \exp\left\{-\frac{(x-m)^2}{2v^2}\right\}$$

For known variance v^2 and unknown mean m, the conjugate prior of a normal distribution is itself normal. For simplicity of exposition we use $v^2 = 1$. Let μ_0 and σ_0^2 be the mean and variance of the prior distribution on m. Thus m is itself distributed as $\mathcal{N}_{\mu_0,\sigma_0^2}(m)$. Given a single input $x^{(i)}$, the posterior distribution on m is given by $\mathcal{N}_{\mu_i,\sigma_i^2}(m)$ where

$$\mu_i = \frac{1}{\sigma_0^2+1}\mu_0 + \frac{\sigma_0^2}{\sigma_0^2+1}x^{(i)}$$

and

$$\frac{1}{\sigma_i^2} = \frac{1}{\sigma_0^2} + 1$$

Proof of Bounded Variance. Want: $Var[\hat{G}_{ik}] \leq c\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}]$ or equivalently

$$\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}^2] - (\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}])^2 \leq \mathrm{cE}[\hat{\mathrm{G}}_{\mathrm{ik}}]$$

Let us now consider each of these terms. In the equalities below, we have used the following facts.

$$\begin{aligned} \mathrm{E}[(\mathrm{m}-\mu_{\mathrm{i}})^2] &= \sigma_i^2 \\ \mathrm{E}[\mathrm{m}] &= \mu_i \end{aligned}$$

$$\begin{aligned}
\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}] &= \mathrm{E}\left[-\frac{(\mathrm{m}-\mu_{\mathrm{i}})^2}{2\sigma_{\mathrm{i}}^2} - \log\sqrt{2\pi\sigma_{\mathrm{i}}^2} + \frac{(\mathrm{m}-\mu_0)^2}{2\sigma_0^2} + \log\sqrt{2\pi\sigma_0^2}\right] \\
&= \frac{\sigma_i^2 + (\mu_i-\mu_0)^2}{2\sigma_0^2} + \frac{1}{2}\log(1+\sigma_0^2) - \frac{1}{2}
\end{aligned}$$

$$\begin{aligned}
\hat{G}_{ik}^2 &= \left\{-\frac{(m-\mu_i)^2}{2\sigma_i^2} + \frac{(m-\mu_0)^2}{2\sigma_0^2} + \frac{1}{2}\log(1+\sigma_0^2)\right\}^2 \\
&= \frac{(m-\mu_i)^4}{4\sigma_i^4} + \frac{(m-\mu_0)^4}{4\sigma_0^4} + \frac{1}{4}[\log(1+\sigma_0^2)]^2 \\
&\quad + \frac{1}{2}\left[\frac{(m-\mu_0)^2}{\sigma_0^2}\log(1+\sigma_0^2) - \frac{(m-\mu_i)^2}{\sigma_i^2}\log(1+\sigma_0^2) - \frac{(m-\mu_0)^2(m-\mu_i)^2}{\sigma_0^2\sigma_i^2}\right]
\end{aligned}$$

Let us now consider each of these terms separately. In the equalities below, we have used the following known facts about the moments of the normal distribution.

$$\begin{aligned}
\mathrm{E}[(\mathrm{m}-\mu_{\mathrm{i}})^4] &= 3\sigma_i^4 \\
\mathrm{E}[\mathrm{m}-\mu_{\mathrm{i}}] &= \mathrm{E}[(\mathrm{m}-\mu_{\mathrm{i}})^3] = 0 \\
\mathrm{E}[\mathrm{m}^4] &= \mu_i^4 + 6\mu_i^2\sigma_i^2 + 3\sigma_i^4 \\
\mathrm{E}[\mathrm{m}^3] &= \mu_i^3 + 3\mu_i\sigma_i^2 \\
\mathrm{E}[\mathrm{m}^2] &= \mu_i^2 + \sigma_i^2
\end{aligned}$$

$$\mathrm{E}[\frac{(\mathrm{m}-\mu_{\mathrm{i}})^4}{4\sigma_{\mathrm{i}}^4}] = \frac{3\sigma_{\mathrm{i}}^4}{4\sigma_{\mathrm{i}}^4} = \frac{3}{4}$$

$$\begin{aligned}
\mathrm{E}[\frac{(\mathrm{m}-\mu_0)^4}{4\sigma_0^4}] &= \mathrm{E}[\frac{((\mathrm{m}-\mu_\mathrm{i})+(\mu_\mathrm{i}-\mu_0))^4}{4\sigma_0^4}] \\
&= \frac{3\sigma_i^4+(\mu_i-\mu_0)^4+6(\mu_i-\mu_0)^2\sigma_i^2}{4\sigma_0^4}
\end{aligned}$$

$$\mathrm{E}[(\mathrm{m}-\mu_0)^2] = \sigma_\mathrm{i}^2 + (\mu_\mathrm{i}-\mu_0)^2$$

$$\mathrm{E}[(\mathrm{m}-\mu_\mathrm{i})^2] = \sigma_\mathrm{i}^2$$

$$\begin{aligned}
\mathrm{E}[(\mathrm{m}-\mu_0)^2(\mathrm{m}-\mu_\mathrm{i})^2] &= \mathrm{E}[(\mathrm{m}^2+\mu_0^2-2\mathrm{m}\mu_0)(\mathrm{m}^2+\mu_\mathrm{i}^2-2\mathrm{m}\mu_\mathrm{i})] \\
&= \frac{(\mu_i-\mu_0)^2+3\sigma_i^2}{\sigma_0^2}
\end{aligned}$$

Putting it together, we have,

$$\begin{aligned}
\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}^2] &= \mathrm{E}[\frac{(\mathrm{m}-\mu_\mathrm{i})^4}{4\sigma_\mathrm{i}^4}] + \mathrm{E}[\frac{(\mathrm{m}-\mu_0)^4}{4\sigma_0^4}] + \frac{1}{4}[\log(1+\sigma_0^2)]^2 \\
&\quad + \frac{1}{2}\frac{\log(1+\sigma_0^2)}{\sigma_0^2}\mathrm{E}[(\mathrm{m}-\mu_0)^2] - \frac{\log(1+\sigma_0^2)}{2}\mathrm{E}[\frac{(\mathrm{m}-\mu_\mathrm{i})^2}{\sigma_\mathrm{i}^2}] - \mathrm{E}[\frac{(\mathrm{m}-\mu_0)^2(\mathrm{m}-\mu_\mathrm{i})^2}{2\sigma_0^2\sigma_\mathrm{i}^2}] \\
&= \frac{3}{4} + \frac{3\sigma_i^4+(\mu_i-\mu_0)^4+6(\mu_i-\mu_0)^2\sigma_i^2}{4\sigma_0^4} + \frac{1}{4}[\log(1+\sigma_0^2)]^2 \\
&\quad + \frac{(\sigma_i^2+(\mu_i-\mu_0)^2)}{\sigma_0^2}\frac{\log(1+\sigma_0^2)}{2} - \frac{\log(1+\sigma_0^2)}{2} - \frac{(\mu_i-\mu_0)^2+3\sigma_i^2}{2\sigma_0^2}
\end{aligned}$$

Now from the expression for $\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}]$ derived earlier, we have

$$\begin{aligned}(\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}])^2 &= \left(\frac{\sigma_i^2+(\mu_i-\mu_0)^2}{2\sigma_0^2}+\frac{1}{2}\log(1+\sigma_0^2)-\frac{1}{2}\right)^2 \\ &= \frac{\sigma_i^4+(\mu_i-\mu_0)^4+2\sigma_i^2(\mu_i-\mu_0)^2}{4\sigma_0^4}+\frac{1}{4}(\log(1+\sigma_0^2))^2+\frac{1}{4} \\ &\quad -\frac{1}{2}\log(1+\sigma_0^2)+\frac{(\sigma_i^2+(\mu_i-\mu_0)^2)\log(1+\sigma_0^2)}{2\sigma_0^2}-\frac{\sigma_i^2+(\mu_i-\mu_0)^2}{2\sigma_0^2}\end{aligned}$$

Getting back to the bounded variance property, we see that

$$\begin{aligned}\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}^2]-(\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}])^2 &= \frac{2\sigma_i^4+4\sigma_i^2(\mu_i-\mu_0)^2}{4\sigma_0^4}+\frac{1}{2}-\frac{\sigma_i^2}{\sigma_0^2} \\ &= \frac{1}{2(1+\sigma_0^2)^2}+\frac{(\mu_i-\mu_0)^2}{\sigma_0^2(1+\sigma_0^2)}+\frac{1}{2}-\frac{1}{1+\sigma_0^2}\end{aligned}$$

and

$$\begin{aligned}\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}] &= \frac{\sigma_i^2+(\mu_i-\mu_0)^2}{2\sigma_0^2}+\frac{1}{2}\log(1+\sigma_0^2)-\frac{1}{2} \\ &= \frac{1}{2(1+\sigma_0^2)}+\frac{(\mu_i-\mu_0)^2}{2\sigma_0^2}+\frac{1}{2}\log(1+\sigma_0^2)-\frac{1}{2}\end{aligned}$$

For readability we use $M=(\mu_i-\mu_0)^2$ and $a=\sigma_0^2$. Note that $M, a \geq 0$. Thus,

$$\begin{aligned}\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}^2]-(\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}])^2-\mathrm{cE}[\hat{\mathrm{G}}_{\mathrm{ik}}] &= \\ &\frac{1}{2(1+a)^2}+\frac{M}{a(1+a)}+\frac{1}{2}-\frac{1}{1+a} \\ &-c\left(\frac{1}{2(1+a)}+\frac{M}{2a}+\frac{1}{2}\log(1+a)-\frac{1}{2}\right) \quad (6.2)\end{aligned}$$

Let us now consider the group of terms in Equation (6.2) that include M. We see

that:

$$\begin{aligned}\frac{M}{a(1+a)} - c\frac{M}{2a} &= M\left(\frac{1}{a(1+a)} - \frac{c}{2a}\right) \\ &= M\left(\frac{1-(c/2)-(ac/2)}{a(1+a)}\right) \leq 0 \quad (\text{for } c \geq 2)\end{aligned}$$

Let us define the remaining terms of Equation (6.2) as

$$f(a) = \frac{1}{2(1+a)^2} + \frac{1}{2} - \frac{1}{1+a} - c\left(\frac{1}{2(1+a)} + \frac{1}{2}\log(1+a) - \frac{1}{2}\right)$$

Note that

$$\begin{aligned}f(0) &= \frac{1}{2} + \frac{1}{2} - 1 - c\left(\frac{1}{2} + \frac{1}{2}\log(1) - \frac{1}{2}\right) \\ &= 0\end{aligned}$$

and

$$\begin{aligned}f'(a) &= -\frac{1}{(1+a)^3} + \frac{1}{(1+a)^2} + \frac{c}{2(1+a)^2} - \frac{c}{2(1+a)} \\ &= \frac{1}{(1+a)^3}\left(a - \frac{ac}{2} - \frac{a^2c}{2}\right) \\ &\leq 0 \quad (\text{for } c \geq 2)\end{aligned}$$

Thus, so long as $c \geq 2$, $f(a)$ is a decreasing function of a for $a \geq 0$. Since $f(0)$ is negative for $c \geq 2$, $f(a) \leq 0$ for all $a \geq 0$.

Thus $\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}^2] - (\mathrm{E}[\hat{\mathrm{G}}_{\mathrm{ik}}])^2 - \mathrm{cE}[\hat{\mathrm{G}}_{\mathrm{ik}}] \leq 0$ for a choice of $c \geq 2$. □

6.6.4 Damage Reduction

Property 4 – damage reduction: The additional loss induced by an attack is lower (in expectation) after additional honest datapoints have been received. We formalize this in Theorem VI.7 in Section 6.7.3.

6.7 A Non-Myopic Regret Bound

Based on the properties of the WTM, we prove a regret bound for our algorithm in this section. We construct the bound in three parts. We first consider a simplified setting in which attackers only inject datapoints *after* honest experts. In this setting, we can bound the worst-case total *damage* that the attack data causes, relative to the forecasts without attack. We can also bound the expected *information loss* from honest experts, relative to the omniscient algorithm that gives them full influence. The third component of our proof is a regret bound for the general case that equals the sum of the damage and information loss bounds. The key ingredient in moving to the general case is in using the damage-reduction property to show that the worst case is in fact when attack data arrive last.

6.7.1 Limited Damage

First, consider a setting with all attack data arriving after honest data. Thus, we can think of each attack datapoint as causing some damage (negative incremental gain) to the prediction made so far. We will bound the total incremental gain of a single attacker below. However, because the definition of gain is based on the change in loss, the theorem directly extends to the case of any number of successive reports by attackers.

Theorem VI.2. *Consider any sequence of rounds and sequences of reported datapoints on those rounds. For any expert i, the net incremental gain due to that expert is bounded below in terms of i's initial reputation r_{i1}:*

$$\sum_{k=1}^{M} G_{ik} \geq -\frac{1}{\alpha} \log(1 + e^{r_{i1}})$$

Proof sketch Recall that the reputation of an expert is updated additively as some function of the incremental gain in each round. The crux of the proof involves

showing that a function of reputation (that we call budget) is concave in the variance-normalized gain. This is then related to the incremental gain of an expert.

Proof of Limited Damage. To prove this formally, we recall some definitions. For a round k and expert i, whose reputation at the beginning of the round is r_{ik}, we have:

- $G_{ik} = \frac{\log(P^*_{\mathbf{b}_i}(\boldsymbol{\beta}_k)) - \log(P^*_{\mathbf{b}_{i-1}}(\boldsymbol{\beta}_k))}{D}$
- $y_{ik} = \frac{e^{r_{ik}}}{1+e^{r_{ik}}}$
- α is the parameter of the ILS module; $\alpha = \min \frac{1}{8}, \frac{1}{4c}$
- $g_{ik} = \frac{1}{y_{ik}} \alpha G_{ik}$
- $S(g) \stackrel{\text{def}}{=} g - \frac{3}{4}g^2$ where g is the value of the variance normalized gain
- $r_{i(k+1)} = r_{ik} + S(g_{ik})$

For ease of analysis, we define a budget function as $B(r) \stackrel{\text{def}}{=} \log(1 + e^r)$ where r is a reputation value. Note that by definition $B(r) \geq 0$. Restated in terms of the budget function, we want to show

$$\sum_{k=1}^{M} G_{ik} \geq -\frac{1}{\alpha} B(r_{i1})$$

The budget function $B(r_{i(k+1)}) = B(r_{ik} + S(g_{ik}))$ can be seen as a function of g_{ik}. We will now show that $B(r_{i(k+1)})$ is concave in g_{ik}. This follows from the fact that $\frac{d^2 B(r_{i(k+1)})}{dg^2} \leq 0$ as shown below. Here g is the variance-normalized gain variable that has value g_{ik} in this round.

- Let $y(r)$ be the influence value for reputation r. Taking derivatives, we observe that $B'(r) = y(r)$, and $y'(r) = y(r)/(1 + e^r)$.

- We evaluate the second derivative of $B(r)$ at $r = r_{i(k+1)}$

$$\begin{aligned}\frac{dB(r_{i(k+1)})}{dg} &= y(r_{i(k+1)})\frac{dr_{i(k+1)}}{dg} = y(r_{i(k+1)})\frac{dS(g_{ik})}{dg} \quad \text{(since } r_{ik} \text{ is constant wrt } g\text{)} \\ &= y(r_{i(k+1)})[1 - 1.5g_{ik}]\end{aligned}$$

$$\begin{aligned}\frac{d^2B(r_{i(k+1)})}{dg^2} &= \left[(1 - 1.5g_{ik})\frac{y(r_{i(k+1)})}{1 + e^{r_{i(k+1)}}}(1 - 1.5g_{ik}) - 1.5y(r_{i(k+1)})\right] \\ &\leq y(r_{i(k+1)})\left[(1 - 1.5g_{ik})^2 - 1.5\right]\end{aligned}$$

- The **bounded gain property** of the WTM requires that $|G_{ik}| \leq y_{ik}$. By choice of parameter we have $\alpha \leq \frac{1}{8}$. Thus, we have $|g_{ik}| = |\frac{1}{y_{ik}}\alpha G_{ik}| \leq \frac{1}{8}$.
- Thus, $\frac{d^2B(r_{i(k+1)})}{dg^2} \leq 0$, and hence $B(r)$ is a concave function of g.

Since the reputation changes as g, we observe that $B(r)$ is a function of g and at $r = r_{ik}$, $g = 0$. Thus, it follows from concavity in g that:

$$B(r_{i(k+1)}) \leq B(r_{ik}) + g_{ik}\frac{dB}{dg}|_{g=0} \Rightarrow B(r_{i(k+1)}) - B(r_{ik}) \leq g_{ik}y_{ik} \tag{6.3}$$

Now,

$$\begin{aligned}\alpha\sum_{k=1}^{M} G_{ik} &= \sum_{k=1}^{M} g_{ik}y_{ik} \quad (\text{ by definition of } g_{ik}) \\ &\geq \sum_{k=1}^{M}[B(r_{i(k+1)}) - B(r_{ik})] \quad \text{(by eqn. 6.3)} \\ &= [B(r_{iM}) - B(r_{i1})] \geq -B(r_{i1}) \quad \text{(by non-negativity of budget)}\end{aligned}$$

Thus, we have

$$\sum_{k=1}^{M} G_{ik} \geq -\frac{1}{\alpha}B(r_{i1})$$

as required. □

Note that the proof would go through even without the parameter α (i.e., based solely on the concavity of the budget function in terms of G_{ik}/y_{ik}). This parameter becomes relevant only in the information loss bound.

6.7.2 Information Loss Bound

In this section, we consider a setting with all attack data arriving after honest data. We will now analyze the loss due to influence limiting honest datapoints. To this end, we use a concept of informativeness defined below.

Definition VI.3. The **informativeness** h_{ik} of expert i on round k is defined as:

$$h_{ik} = E_{\mathbf{x}_k \sim T_k} \left[\log[\mathbf{Q}_{k,i}(\boldsymbol{\beta}_k)] - \log[\mathbf{Q}_{k,(i-1)}(\boldsymbol{\beta}_k)] \right]$$

Thus, the informativeness of an expert i in round k, h_{ik} is the incremental gain attributed to i by the omniscient algorithm $\mathbf{Z}$. The informativeness provides us with a benchmark for the incremental gain obtained from an expert i; if the sum of expected incremental gains under an algorithm is equal to the sum of informativeness h_{ik} over all honest i, then the algorithm would be optimally using the received data.

We define expected information lost from expert i as

$$\mathrm{IL}_i = \sum_{k=1}^{M} \left(h_{ik} - \mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_k^i) \sim (\mathrm{T}_1, \mathrm{T}_2, ... \mathrm{T}_k)} [\mathrm{G}_{\mathrm{ik}}] \right)$$

The **concave gain property** of the WTM states that the incremental gain $G_{ik} \geq y_{ik}\hat{G}_{ik}$ where $\hat{G}_{ik}$ is the incremental gain due to expert i on round k when her influence $y_{ik} = 1$. By the **damage reduction property**, we can show that any influence-limiting on earlier experts only increases the incremental gain of an expert; this is shown in Lemma VI.10. Thus

$$\mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_k) \sim (\mathrm{T}_1, \mathrm{T}_2, ... \mathrm{T}_k)} [\hat{\mathrm{G}}_{\mathrm{ik}}] \geq \mathrm{h}_{\mathrm{ik}}$$

Note that since r_{ik} is independent of the datapoints in this round, y_{ik} and $\hat{G}_{ik}$ are independent random variables.

From this, we obtain an alternate expression that is an upper bound on the information loss:

$$\begin{aligned}
\mathrm{IL}_i &= \sum_{k=1}^{M} \left(h_{ik} - \mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_k^i) \sim (\mathrm{T}_1, \mathrm{T}_2, ... \mathrm{T}_k)} [\mathrm{G_{ik}}] \right) \\
&\leq \sum_{k=1}^{M} \left(h_{ik} - \mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_k^i) \sim (\mathrm{T}_1, \mathrm{T}_2, ... \mathrm{T}_k)} [\mathrm{y_{ik}} \hat{\mathrm{G}}_{\mathrm{ik}}] \right) \\
&\leq \sum_{k=1}^{M} \left(h_{ik} - \left(\mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_k^i) \sim (\mathrm{T}_1, \mathrm{T}_2, ... \mathrm{T}_k)} [\mathrm{y_{ik}}] \mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_k^i) \sim (\mathrm{T}_1, \mathrm{T}_2, ... \mathrm{T}_k)} [\hat{\mathrm{G}}_{\mathrm{ik}}] \right) \right) \\
&\leq \sum_{k=1}^{M} \mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_k^i) \sim (\mathrm{T}_1, \mathrm{T}_2, ... \mathrm{T}_k)} [\overline{\mathrm{y}}(\mathrm{r_{ik}})] \mathrm{h_{ik}}
\end{aligned}$$

The intuition behind the bound on information loss we show subsequently is as follows: Suppose that, in each round, the expected gain was some fixed quantity h. Suppose further that the realized score was exactly the expected gain, so that $r_{ik} = r_{i1} + (k-1)h$. Then, the expected information loss, over a very large number of items, would be approximately $\int_{r_{i1}}^{\infty} \overline{y}(x)dx = -\log(y(r_{i1})) = \log(1 + e^{-r_{i1}})$ where we have introduced a change of variable with x denoting the range of values for r_{ik}. In other words, the logistic function approaches 1 at a fast enough rate that the total deficit is bounded.

For the actual bound, we need to handle several complications. Firstly, the score $S(g)$ is not a linear function of the gain $\hat{G}_{ik}$, and the expected score is lower than the expected gain. Second, the realized score is not the same as the expected score, and so we need to handle the full distribution of possible values of r_{ik}, and use concentration results to bound the loss. Finally, we need to take into account the fact that different rounds k have different expected gains h_{ik}.

In order to prove the information loss bound, first we show that the mean and

variance of the score $S(g_{ik})$ are "well-behaved" under certain conditions on $E[G_k]$ and $\mathrm{Var}[G_k]$. When we apply this lemma in Lemma VI.5, we will show that these conditions do indeed hold.

Lemma VI.4. *Suppose that* $G_k \stackrel{\text{def}}{=} \frac{G_{ik}}{y_{ik}}$ *where* G_{ik} *is the incremental gain of expert* i *in round* k *and* y_{ik} *is his influence. Suppose further that* G_k *has mean* h_{ik} *and variance is at most* ch_{ik}*. That is,*

$$E[G_k] \geq h_{ik} \quad \textit{and} \quad Var[G_k] \leq ch_{ik}$$

If $g_{ik} = \alpha G_k$ *and* $S(g_{ik}) = g_{ik} - \frac{3}{4}g_{ik}^2$ *as defined earlier, then*

$$E[S(g_{ik})] \geq \frac{3\alpha}{4}h_{ik} \quad \textit{and} \quad Var[S(g_{ik})] \leq 0.5E[S(g_{ik})]$$

Proof. First we bound $E[S(g_{ik})]$. Recall that by choice $\alpha = \min(\frac{1}{8}, \frac{1}{4c})$. Consider two cases, based on the value of $E[G_k]$.

Case 1: $E[G_k] \geq 0.5$ The bounded gain property asserts $|\frac{1}{y_{ik}}G_{ik}| \leq 1$. This implies that $E[G_k^2] \leq 1$. Also note, $2E[G_k] \geq 1$.

Thus,

$$\begin{aligned}
\mathrm{E[S(g_{ik})] = E[S(\alpha G_k)]} &= \alpha \mathrm{E[G_k]} - \frac{3\alpha^2}{4}\mathrm{E[G_k^2]} \\
&\geq \alpha \mathrm{E[G_k]} - \frac{3\alpha^2}{4}2\mathrm{E[G_k]} = \alpha \mathrm{E[G_k]}[1 - 1.5\alpha] \\
&\geq \alpha \mathrm{E[G_k]}[1 - \frac{1.5}{8}] \\
&\geq \frac{3\alpha}{4}\mathrm{E[G_k]} \\
&\geq \frac{3\alpha}{4}h_{ik}
\end{aligned}$$

Case 2: $E[G_k] \leq 0.5$ We note that $E[G_k^2] = E[G_k]^2 + Var[G_k]$ and $Var[G_k] \leq ch_{ik}$. Now,

$$\begin{aligned} E[S(g_{ik})] = E[S(\alpha G_k)] &= \alpha E[G_k] - \frac{3}{4}\alpha^2 E[G_k^2] \\ &\geq \alpha h_{ik} - \frac{3}{4}\alpha^2[E[G_k]^2 + Var[G_k]] \\ &\geq \alpha h_{ik} - \frac{3}{4}\alpha^2[\frac{1}{4} + ch_{ik}] \\ &\geq \alpha h_{ik} - \frac{3}{4}\alpha^2 ch_{ik} \\ &\geq \alpha h_{ik} - \frac{3}{4}\alpha^2 \frac{1}{4\alpha} h_{ik} \quad (\text{since } \alpha \leq 1/4c) \\ &\geq \frac{3\alpha}{4} h_{ik} \end{aligned}$$

Next, we consider the variance of $S(g_k)$. We bound it using a result due to Tang and See (*Tang and See*, 2009, Prop. 2) that states that if $|f'(x)| \leq a$, then $\text{Var}(f(x)) \leq a^2\text{Var}(x)$. Also, recall that $\text{Var}[ax] = a^2\text{Var}[x]$ for a constant a.

We see that $S'(g_{ik}) = 1 - 1.5g_k$. The bounded gain property asserts $|\frac{1}{y_{ik}}G_{ik}| \leq 1$. This implies $\frac{1}{y_{ik}}G_{ik} \geq -1$ and hence $g_k \geq -\alpha$. Thus, $S'(g_{ik}) = 1 - 1.5g_k \leq 1 + 1.5\alpha$.

$$\begin{aligned} \text{Var}[S(g_k)] &\leq (1 + 1.5\alpha)^2\alpha^2 ch_{ik} = (c\alpha)(1 + 1.5\alpha)^2\alpha h_{ik} \\ &\leq \frac{1}{4}(1 + 1.5\alpha)^2\alpha h_{ik} \\ &\leq \frac{1}{4}(\frac{19}{16})^2\alpha h_{ik} < 0.36\alpha h_{ik} < \frac{3\alpha h_{ik}}{8} \end{aligned} \tag{6.4}$$

Thus, $\text{Var}[S(g_k)] \leq 0.5E[S(g_k)]$. □

Lemma VI.5. *Let r_{i1} denote the initial reputation. Let $H_{ik} = \sum_{t=1}^{k} h_{it}$. Denote $\overline{y}(r) = 1 - y$ for reputation r and associated influence y. For any k , we must have:*

$$E[\overline{y}(r_{ik})] \leq e^{-\frac{\alpha H_{ik}}{8}} + \overline{y}(r_{i1} + \frac{3\alpha H_{ik}}{8})$$

Proof. We will need Lemma VI.4 for this proof. First, we will show that the conditions of the lemma hold. That is, for $G_k \stackrel{\text{def}}{=} \frac{G_{ik}}{y_{ik}}$,

$$E[G_k] \geq h_{ik} \quad \text{and} \quad \text{Var}[G_k] \leq ch_{ik}$$

Then, Lemma VI.4 says that

$$E[S(g_{ik})] \geq \frac{3\alpha}{4} h_{ik} \quad \text{and} \quad \text{Var}[S(g_{ik})] \leq 0.5E[S(g_{ik})]$$

By definition h_{ik} is the gain of an honest expert when no honest expert is influence limited. By the **damage reduction property**, we can show that any influence-limiting on earlier experts only increases the incremental gain $\hat{G}_{ik}$ of an expert; this is shown in Lemma VI.10. Further, from the **concave gain property**, we have $\frac{G_{ik}}{y_{ik}} \geq \hat{G}_{ik}$. Thus, $\mathrm{E[G_k] = E[\frac{G_{ik}}{y_{ik}}] \geq E[\hat{G}_{ik}] \geq h_{ik}}$.

Now consider $\text{Var}[G_{ik}]$. By definition,

$$G_{ik} = \frac{y_{ik}(\boldsymbol{\phi}(x_k^{(i)}), 1) \cdot \boldsymbol{\beta}^* - (\psi^*(\mathbf{b}_i) - \psi^*(\mathbf{b}_{i\backsim 1}))}{D}$$

Since $\frac{(\psi^*(\mathbf{b}_i) - \psi^*(\mathbf{b}_{i\backsim 1}))}{D}$ is not dependent on the outcome $\boldsymbol{\beta}_k$,

$$\text{Var}[G_{ik}] = \text{Var}\left[\frac{y_{ik}(\boldsymbol{\phi}(x_k^{(i)}), 1) \cdot \boldsymbol{\beta}^*}{D}\right]$$

Thus,

$$\text{Var}[G_k] = \text{Var}\left[\frac{G_{ik}}{y_{ik}}\right] = \text{Var}\left[\frac{(\boldsymbol{\phi}(x_k^{(i)}), 1) \cdot \boldsymbol{\beta}^*}{D}\right] = \text{Var}[\hat{G}_{ik}]$$

But $\text{Var}[\hat{G}_{ik}]$ is identical to the variance when no expert is influence limited. This follows from the fact that the variance is independent of $\mathbf{b}_{i\backsim 1}$. Thus, by the **bounded variance property**,

$$\text{Var}[G_k] = \text{Var}[\hat{G}_{ik}] \leq ch_{ik}$$

First, we note that $r_{ik} = r_{i1} + \sum_{t=1}^{k} S(g_{it})$ by definition. Thus the expected value of r_{ik} is

$$E[r_{ik}] = r_{i1} + \sum_{t=1}^{k} E[S(g_{it})] \geq r_{i1} + \sum_{t=1}^{k} \frac{3\alpha}{4} h_{it} = r_{i1} + \frac{3\alpha H_{ik}}{4}$$

where the inequality follows from Lemma VI.4.

We split the domain of possible values of r_{ik} into two components $[-\infty, r_{i1} + \frac{3\alpha H_{ik}}{8})$ and $[r_{i1} + \frac{3\alpha H_{ik}}{8}, \infty]$. Then, we have:

$$\begin{aligned}
E[\overline{y}(r_{ik})] &= \int_{r_{ik}=-\infty}^{r_{i1}+\frac{3\alpha H_{ik}}{8}} \Pr(r_{ik})\overline{y}(r_{ik}) + \int_{r_{ik}=r_{i1}+\frac{3\alpha H_{ik}}{8}}^{\infty} \Pr(r_{ik})\overline{y}(r_{ik}) \\
&< \Pr(r_{ik} < r_{i1} + \frac{3\alpha H_{ik}}{8}) + \overline{y}(r_{i1} + \frac{3\alpha H_{ik}}{8}) \int_{r_{ik}=r_{i1}+\frac{3\alpha H_{ik}}{8}}^{\infty} \Pr(r_{ik}) \\
&\leq \Pr(r_{ik} < r_{i1} + \frac{3\alpha H_{ik}}{8}) + \overline{y}(r_{i1} + \frac{3\alpha H_{ik}}{8})
\end{aligned}$$

where in the first inequality we have used the following facts: $\overline{y}(r_{ik}) \leq 1$ and the function $\overline{y}()$ is monotonically decreasing.

Now, to bound the term $\Pr(r_{ik} - r_{i1} < \frac{3\alpha H_{ik}}{8})$, we use Bennett's concentration inequality *Bennett* (1962). This inequality states that for independent random variable $X_1 \ldots X_k$ that all have expected value 0, if for all t, $|X_t| \leq a$, and $\sum_{t=1}^{k} \mathrm{Var}[X_t] = k\sigma^2$, then for any $d \geq 0$,

$$\Pr(\sum_{t=1}^{k} X_t > d) \leq \exp\left(\frac{k\sigma^2}{a^2} h\left(\frac{ad}{k\sigma^2}\right)\right)$$

where $h(x) = (1+x)\log(1+x) - x$. Note that $h(1) > 0.38$

Note that the gain in each round k is independent of previous and subsequent

rounds. Thus, the change in reputation

$$r_{ik} - r_{i1} = \sum_{t=1}^{k} S(g_{it})$$

and is the sum of independent random variables. Define a new random variable for each t,

$$X_t = E[S(g_{it})] - S(g_{it})$$

Note that X_t are also independent random variables and further

$$E[X_t] = 0 \quad \text{and} \quad |X_t| \leq 1$$

By inequality (6.4) established in Lemma VI.4, we have $\sum_{t=1}^{k} \text{Var}[S(g_{it})] \leq \frac{3\alpha H_{ik}}{8}$. Thus,

$$\sum_{t=1}^{k} \text{Var}[X_t] \leq \frac{3\alpha H_{ik}}{8}$$

If we bound

$$\Pr\left(\sum_{t=1}^{k} X_t > \frac{3\alpha H_{ik}}{8}\right) = \Pr\left[\sum_{t=1}^{k} S(g_{it}) < \left(\sum_{t=1}^{k} E[S(g_{it})] - \frac{3\alpha H_{ik}}{8}\right)\right]$$

then we will have a bound on $\Pr(r_{ik} - r_{i1} < \frac{3\alpha H_{ik}}{8})$ since by Lemma VI.4, we have $E[S(g_{it})] \geq \frac{3\alpha}{4} h_{it}$.

By Bennett's inequality,

$$\Pr\left(\sum_{t=1}^{k} X_t > \frac{3\alpha H_{ik}}{8}\right) \leq \exp\left\{\frac{-3\alpha H_{ik}}{8} * h(1)\right\} \leq \exp\left\{-\frac{\alpha H_{ik}}{8}\right\}$$

□

Recall that expected information lost from expert i is defined as

$$\mathrm{IL}_i = \sum_{k=1}^{M} \left(h_{ik} - \mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_k) \sim (\mathrm{T}_1, \mathrm{T}_2, ... \mathrm{T}_k)} [\mathrm{G}_{ik}] \right)$$

We can prove the information loss bound as:

Theorem VI.6. *Let r_{i1} denote the initial reputation assigned to expert i. Fix a sequence of rounds, and the datapoints submitted by experts prior to i's datapoint on each round. Then, the information lost from expert i is bounded above by:*

$$IL_i \leq D \left[2 + \frac{8}{\alpha} + \frac{8}{3\alpha} \log(1 + e^{-r_{i1}}) \right]$$

Proof. Recall that from the **concave gain property** and the **damage reduction property** of the WTM, we obtain an alternate expression that is an upper bound on the information loss:

$$\mathrm{IL}_i \leq \sum_{k=1}^{M} \mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_k) \sim (\mathrm{T}_1, \mathrm{T}_2, ... \mathrm{T}_k)} [\overline{\mathrm{y}}(\mathrm{r}_{ik})] \mathrm{h}_{ik}$$

Recall that we define $H_{ik} = \sum_{t=1}^{k} h_{it}$. Let $\overline{k}$ be the lowest round such that $H_{i\overline{k}} \geq 1$. Note that $H_{i\overline{k}} \leq 2$ since each expert can have gain at most 1 per round. Also note that for all k, $\overline{y}(r_{ik}) \leq 1$. Then, accounting for all information up to round $\overline{k}$ as lost, we have

$$\mathrm{IL}_i \leq 2 + \sum_{k=\overline{k}}^{M} \mathrm{E}_{(\mathbf{x}_{\overline{k}} ... \mathbf{x}_k) \sim (\mathrm{T}_{\overline{k}}, ... \mathrm{T}_k)} [\overline{\mathrm{y}}(\mathrm{r}_{ik})] \mathrm{h}_{ik}$$

Now, consider a given $k \geq \overline{k}$. By lemma VI.5, this can be bounded by the sum:

$$\mathrm{IL}_i \leq 2 + \sum_{k=\overline{k}}^{M} e^{-\frac{\alpha H_{ik}}{8}} h_{ik} + \sum_{k=\overline{k}}^{M} \overline{y}(r_{i1} + \frac{3\alpha H_{ik}}{8}) h_{ik}$$

In each of the two sums, the terms are monotonically decreasing. Moreover, the

maximum h_{ik} is 1. Let $\overline{H}$ be the value of H_{ik} at $\overline{k}$. Thus, we can bound the sums by integrals, as:

$$\mathrm{IL}_i \leq 2 + \int_{H=\overline{H}}^{\infty} e^{-\frac{\alpha(H-1)}{8}} dH + \int_{H=\overline{H}}^{\infty} \overline{y}(r_{i1} + \frac{3\alpha(H-1)}{8}) dH$$

The two integrals have closed-form solutions:

$$\int e^{-\frac{\alpha(H-1)}{8}} dH = \frac{-8}{\alpha} e^{-\frac{\alpha(H-1)}{8}}$$

and

$$\int \overline{y}(r_{i1} + \frac{3\alpha(H-1)}{8}) dH = \frac{8}{3\alpha} \log \left[y(r_{i1} + \frac{3\alpha(H-1)}{8}) \right]$$

Substituting these functions, and setting the range of the integrals to $(0, \infty)$, we get:

$$\mathrm{IL}_i \leq 2 + \frac{8}{\alpha} + \frac{8}{3\alpha} \log(1 + e^{-r_{i1}})$$

□

6.7.3 A Combined Regret Bound

We can now use the damage reduction property of the WTM to bound the total regret in a system with honest set $\mathcal{H}$ under any attack $\mathcal{A}$.

The damage reduction property of the WTM implies that the worst case in terms of loss suffered by the algorithm is when all attacks arrive after honest data. We formally state and prove the damage reduction property below.

Theorem VI.7. (damage reduction property):
Let $P_0^* \in \mathcal{F}^*$ be the prior distribution on $\boldsymbol{\beta}$ with natural parameter $\mathbf{b}_0$. Let $\boldsymbol{\phi}(x)$ denote an observation of sufficient statistics, with $x \in \mathcal{X}$ drawn according to $\pi(x)$.

Then, if $P_x^*(\boldsymbol{\beta})$ with natural parameter $\mathbf{b}_x$ denotes the posterior hyperdistribution after observing $\boldsymbol{\phi}(x)$; we must have $\mathbf{b}_x = \mathbf{b}_0 + (\boldsymbol{\phi}(x), 1)$ Diaconis and Ylvisaker (1979). We say that P_0^* is unbiased with respect to π, if for any $\boldsymbol{\beta}$, we have $P_0^*(\boldsymbol{\beta}) = E_\pi P_x^*(\boldsymbol{\beta})$.

Consider a vector $\mathbf{a}$ (the entries of $\mathbf{a}$ may be positive or negative). $\mathbf{a}$ can be interpreted as a movement on the natural parameter of the hyperdistribution due to an attacker. Let $\tilde{P}_0$ denote the hyperdistribution if the attack is carried out on the prior. The natural parameter of $\tilde{P}_0$ is given by: $\mathbf{a}_0 = \mathbf{b}_0 + \mathbf{a}$. Likewise, let $\tilde{P}_x$ denote the hyperdistribution with natural parameter $\mathbf{a}_x = \mathbf{b}_x + \mathbf{a}$.

Then, as long as P_0^* is unbiased with respect to π, the following holds:

$$K(P_0^* || \tilde{P}_0) \geq E_\pi \left[K(P_x^* || \tilde{P}_x) \right] \tag{6.5}$$

In other words: the damage induced by a fixed vector of securities $\mathbf{a}$ purchased at the initial distribution P_0^* is greater than the expected error of the same vector of securities after an additional informative observation x.

To prove this property, we first prove two relevant lemmas.

Lemma VI.8. *Let $P_0^* \in \mathcal{F}^*$ denote an initial distribution. Suppose that $\boldsymbol{\phi}(x)$ denote an observation of sufficient statistics, distributed according to a distribution $\pi(x)$. Then, let P_x^* denote the posterior hyperdistribution after conditioning on x; we must have the corresponding natural parameter $\mathbf{b}_x = \mathbf{b}_0 + (\boldsymbol{\phi}(x), 1)$. The given P_0^* and π must be such that P_0^* is unbiased with respect to π: For any $\boldsymbol{\beta}$, we must have $P_0^*(\boldsymbol{\beta}) = E_\pi P_1^*(\boldsymbol{\beta})$.*

For any vector $\mathbf{a}$ of the same dimension as $\boldsymbol{\beta}^*$, the vector of sufficient statistics, the variance of $\mathbf{a} \cdot \boldsymbol{\beta}^*$ at P_0^* is at least as high as the expected variance at P_x^*:

$$Var_{P_0^*}(\mathbf{a} \cdot \boldsymbol{\beta}^*) \geq E_x \left[Var_{P_x^*}(\mathbf{a} \cdot \boldsymbol{\beta}^*) \right]$$

Proof. The condition that P_0^* is unbiased implies that we can treat P_0^* as a joint

distribution over $\boldsymbol{\phi}(x)$ and $\boldsymbol{\beta}^*$: $P_0^*(\boldsymbol{\phi}(x), \boldsymbol{\beta}^*) \stackrel{\text{def}}{=} \pi(x) P_x^*(\boldsymbol{\beta}^*)$ has marginal distribution $P_0^*(\boldsymbol{\beta}^*)$ on $\boldsymbol{\beta}^*$.

Now, treating $\mathbf{a} \cdot \boldsymbol{\beta}^*$ and $\boldsymbol{\phi}(x)$ as two random variables, we can use the standard result from probability theory (see, e.g., (*Gut*, 1995, p.39)) on the conditional variance:

$$\mathrm{Var}_{P_0^*}(\mathbf{a} \cdot \boldsymbol{\beta}^*) = E_x \mathrm{Var}(\mathbf{a} \cdot \boldsymbol{\beta}^* | \boldsymbol{\phi}(x)) + \mathrm{Var}_x[E(\mathbf{a} \cdot \boldsymbol{\beta}^* | \boldsymbol{\phi}(x))]$$

The second term on the right hand side is non-negative, so we get:

$$\mathrm{Var}_{P_0^*}(\mathbf{a} \cdot \boldsymbol{\beta}^*) \geq E_x \mathrm{Var}(\mathbf{a} \cdot \boldsymbol{\beta}^* | \boldsymbol{\phi}(x)) = E_x \left[\mathrm{Var}_{P_x^*}(\mathbf{a} \cdot \boldsymbol{\beta}^*) \right]$$

□

The next ingredient of the proof of Theorem VI.7 is to express the KL-divergence induced by $\mathbf{a}$ in terms of an integral over variances. This differential relationship is implicit in the literature on exponential families, but we include a self-contained proof for clarity and completeness:

Lemma VI.9. *Given any two distributions $P, \tilde{P} \in \mathcal{F}^*$ such that $\mathbf{b}_{\tilde{P}} = \mathbf{b}_P + \mathbf{a}$, the KL divergence can be expressed as follows:*

$$K(P||\tilde{P}) = \int_{t=0}^{1} \int_{u=0}^{t} Var_{P_u^*}[\mathbf{a} \cdot \boldsymbol{\beta}^*] du dt$$

(Here, P_u^* denotes the distribution with natural parameter coordinates $\mathbf{b}_{P_u^*} = \mathbf{b}_P + u\mathbf{a}$.)

Proof. We can prove this result by repeated differentiation:

$$\begin{aligned}
\frac{d}{du}K(P||P_u^*) &= -\frac{d}{du}\int_{\boldsymbol{\beta}^*} P(\boldsymbol{\beta}^*)\log P_u^*(\boldsymbol{\beta}^*)d\boldsymbol{\beta}^* \\
&= -\int_{\boldsymbol{\beta}^*} P(\boldsymbol{\beta}^*)\frac{d}{du}[\log P_u^*(\boldsymbol{\beta}^*)]d\boldsymbol{\beta}^* \\
&= -\int_{\boldsymbol{\beta}^*} P(\boldsymbol{\beta}^*)\frac{d}{du}[\mathbf{b}_{P_u^*}\cdot\boldsymbol{\beta}^* - \psi^*(P_u^*)] \\
&= -\int_{\boldsymbol{\beta}^*} P(\boldsymbol{\beta}^*)[\mathbf{a}\cdot\boldsymbol{\beta}^*]d\boldsymbol{\beta}^* + \frac{d}{du}\psi^*(P_u^*) \\
&= -\mathbf{a}\cdot\mathbf{m}_P + \mathbf{a}\cdot\mathbf{m}_{P_u^*}
\end{aligned}$$

In the last step, we used the definition of $\mathbf{m}_P$, the expected value of $\boldsymbol{\beta}^*$ under P and the well-known fact that the gradient of $\psi_{P_u^*}^*$ is $\mathbf{m}_{P_u^*}$.

Differentiating a second time, we get:

$$\begin{aligned}
\frac{d^2}{du^2}K(P||P_u^*) &= \frac{d}{du}[-\mathbf{a}\cdot\mathbf{m}_P + \mathbf{a}\cdot\mathbf{m}_{P_u^*}] \\
&= \mathbf{a}\cdot\frac{d}{du}\mathbf{m}_{P_u^*}
\end{aligned}$$

Now, we expand $\mathbf{m}_{P_u^*}$ by definition:

$$\begin{aligned}
\mathbf{a}\cdot\frac{d}{du}\mathbf{m}_{P_u^*} &= \mathbf{a}\cdot\frac{d}{du}\int_{\boldsymbol{\beta}^*}\boldsymbol{\beta}^* P_u^*(\boldsymbol{\beta}^*)d\boldsymbol{\beta}^* \\
&= \mathbf{a}\cdot\int_{\boldsymbol{\beta}^*}\boldsymbol{\beta}^*\frac{d}{du}P_u^*(\boldsymbol{\beta}^*)d\boldsymbol{\beta}^*
\end{aligned}$$

By definition of $P_u^*(\boldsymbol{\beta}^*) = \exp[\mathbf{b}_{P_u^*}.\boldsymbol{\beta}^* - \psi^*(P_u^*)]$, we have:

$$\frac{d}{du}P_u^*(\boldsymbol{\beta}^*) = P_u^*(\boldsymbol{\beta}^*).[\frac{d}{du}\mathbf{b}_{P_u^*}.\boldsymbol{\beta}^* - \frac{d}{du}\psi^*(P_u^*)] = P_u^*(\boldsymbol{\beta}^*)\cdot[\mathbf{a}\cdot\boldsymbol{\beta}^* - \mathbf{a}.\mathbf{m}_{P_u^*}]$$

Thus,

$$\begin{aligned}
\mathbf{a} \cdot \frac{d}{du}\mathbf{m}_{P_u^*} &= \mathbf{a} \cdot \int_{\boldsymbol{\beta}^*} \boldsymbol{\beta}^* [\mathbf{a} \cdot \boldsymbol{\beta}^* - \mathbf{a} \cdot \mathbf{m}_{P_u^*}] P_u^*(\boldsymbol{\beta}^*) d\boldsymbol{\beta}^*) \\
&= \int_{\boldsymbol{\beta}^*} (\mathbf{a} \cdot \boldsymbol{\beta}^*)^2 P_u^*(\boldsymbol{\beta}^*) d\boldsymbol{\beta}^* - (\mathbf{a} \cdot \mathbf{m}_{P_u^*}) \int_{\boldsymbol{\beta}^*} \mathbf{a} \cdot \boldsymbol{\beta}^* d\boldsymbol{\beta}^* \\
&= \int_{\boldsymbol{\beta}^*} (\mathbf{a} \cdot \boldsymbol{\beta}^*)^2 P_u^*(\boldsymbol{\beta}^*) d\boldsymbol{\beta}^* - (\mathbf{a} \cdot \mathbf{m}_{P_u^*})^2
\end{aligned}$$

Finally, observing that $E_{P_u^*}(\mathbf{a} \cdot \boldsymbol{\beta}^*) = \mathbf{a} \cdot \mathbf{m}_{P_u^*}$, the RHS is observed to be, by definition, $\mathrm{Var}_{P_u^*}(\mathbf{a} \cdot \boldsymbol{\beta}^*)$.

Integrating, and observing that the LHS is 0 when $u = 0$, we have:

$$[-\mathbf{a} \cdot \mathbf{m}_P + \mathbf{a} \cdot \mathbf{m}_{P_t^*}] = \int_{u=0}^{t} \mathrm{Var}_{P_u^*}(\mathbf{a} \cdot \boldsymbol{\beta}^*) du$$

Integrating a second time, and again observing that $K(P||P_t^*) = 0$ when $t = 0$, we have:

$$K(P||\tilde{P}) = \int_{t=0}^{1} \int_{u=0}^{t} \mathrm{Var}_{P_u^*}[\mathbf{a} \cdot \boldsymbol{\beta}^*] du dt$$

□

Now, we can return to the proof of Theorem VI.7:

Proof of Theorem VI.7. The proof follows from a careful application of Lemma VI.8 to the decomposition given in Lemma VI.9. We seek to prove:

$$K(P_0^*||\tilde{P}_0) \geq E_\pi \left[K(P_x^*||\tilde{P}_x) \right]$$

By Lemma VI.9, this is equivalent to proving:

$$\int_{t=0}^{1}\int_{u=0}^{t} \mathrm{Var}_{P_u^*}[\mathbf{a}\cdot\boldsymbol{\beta}^*]dudt \geq E_\pi \int_{t=0}^{1}\int_{u=0}^{t} \mathrm{Var}_{P_{xu}^*}[\mathbf{a}\cdot\boldsymbol{\beta}^*]dudt$$

where P_{xu}^* is the distribution with $\mathbf{b}_{P_{xu}^*} = \mathbf{b}_{P_x^*} + u\mathbf{a}$.

It is therefore sufficient to prove that, for every $u \in (0,1)$,

$$\mathrm{Var}_{P_u^*}[\mathbf{a}\cdot\boldsymbol{\beta}^*] - E_\pi \mathrm{Var}_{P_{xu}^*}[\mathbf{a}\cdot\boldsymbol{\beta}^*] \geq 0 \tag{6.6}$$

Consider any fixed value of u. Based on the conjugate prior nature of $\mathcal{F}^*$, if we started with prior belief P_0^* and observed a value $\mathbf{a}$ with weight u, the posterior distribution would be P_u^*. Then, conditioning P_u^* on a further observation of $\boldsymbol{\phi}(x)$ would yield the posterior distribution P_{xu}^*, because P_{xu}^* is the distribution obtained by conditioning P_0^* on observing $\boldsymbol{\phi}(x)$ and $\mathbf{a}$ with weight u. Here, we have used the property of Bayesian updating that the order of observation does not affect the final posterior. We can also verify that

$$\begin{aligned} P_u^*(\boldsymbol{\beta}^*) &= P_0^*(\boldsymbol{\beta}^* | u\mathbf{a} \text{ observed}) = \int_x P_0^*(\boldsymbol{\beta}^*, \boldsymbol{\phi}(x) | u\mathbf{a} \text{ observed}) \\ &= \int_x \pi(x) P_0^*(\boldsymbol{\beta}^* | u\mathbf{a} \text{ observed}, \boldsymbol{\phi}(x) \text{ observed}) = \int_x \pi(x) P_{xu}^*(\boldsymbol{\beta}^*) \end{aligned}$$

Thus, the conditions of Lemma VI.8 are satisfied; using this result, we have that, for every value of u, equation 6.6 is satisfied. □

In other words: the damage induced by a fixed vector of securities $\mathbf{a}$ purchased at the initial distribution P_0^* is greater than the expected error of the same vector of securities after an additional informative observation x.

A new representation of datapoint sequences For analytic purposes, we will want to represent the sequence provided to the algorithm more explicitly. This will allow us to reorder the sequence in a way that makes it easier to analyze.

Recall that in a round k, the sequence of participating experts is denoted as $E_k = \langle e_1, \ldots, e_{N_k} \rangle \subseteq \sigma(N)$. In order to analyze the effect of influence limiting of datapoints from honest experts and datapoints from attackers, we specify a different representation of the sequence of datapoints $\tilde{\mathbf{x}}_k = (\tilde{x}_k^{(e_i)})$ for $e_i \in \langle e_1, \ldots, e_{N_k} \rangle$ received by the algorithm in round k. This is solely for ease of analysis and doesn't affect the actual method by which the data sequences are generated.

First we consider honest datapoints. Consider a datapoint $\tilde{x}_k^{(e_i)}$, received from an honest expert $e_i \in \mathcal{H}$ when the current natural hyperparameter coordinates are $\mathbf{b}_{i\backsim 1}$. For succinctness we call this datapoint x_i. The optimal use of x_i would be to update the coordinates additively with $(\boldsymbol{\phi}(x_i), 1)$. In actuality, because of influence limiting, the update is $\mathbf{b}_i = \mathbf{b}_{i\backsim 1} + y_{ik}(\boldsymbol{\phi}(x_i), 1)$; in other words, there is an influence limit on the update. Noting that $\mathbf{b}_i = [\mathbf{b}_{i\backsim 1} + (\boldsymbol{\phi}(x_i), 1)] - \overline{y}_{ik}(\boldsymbol{\phi}(x_i), 1)$, we can think of the effect of influence limiting as involving an attack with *negatively weighted* data. Thus, the effect of influence-limited update can be modeled as fully updating by the data x_i, followed by updating based on negatively-weighted data. Let $\overline{x}_i$ denote this latter half; in other words, $\overline{x}_i$ corresponds to updating the natural parameter coordinates by adding $(-\overline{y}_{ik}\boldsymbol{\phi}(x_i), -\overline{y}_{ik})$. We can think of this negatively weighted datapoint as introduced by a phantom expert. Thus for every honest expert $e_i \in \mathcal{H}$ there is an corresponding phantom expert. We call the set of phantom experts $\mathbb{H}$ and refer by $\overline{e}_i$ the expert corresponding to e_i in this set.

Next we consider attack datapoints. Let $\mathbf{x}_k = \langle x_1 \ldots x_n \rangle$ denote the subsequence of $\tilde{\mathbf{x}}_k$ consisting of all and only honest datapoints. Our analysis only involves the aggregate effects of all attack identities, and the aggregate sum of all attackers' influences. Thus, any substring of attack datapoints in $\tilde{\mathbf{x}}$ may be replaced by a single

weighted datapoint. Let d_i denote the weighted attack datapoint that is injected after x_i, with the understanding that the d_i depends on $(x_1, \ldots, x_i)$. Note that the weight can capture the effect of influence limiting of the attackers as well, and so we do not need to separately model influence limiting of attackers. Note also that this weight may in fact be zero to signal no attack between to consecutive honest datapoints. We call the corresponding meta-expert $\tilde{e}_i$. Note that $\tilde{e}_i$ possibly combines multiple identities from $\overline{\mathcal{H}}$.

Thus, the extended sequence $\tilde{\mathbf{x}}_k$ can now be rewritten as $\tilde{\mathbf{x}}_k = \langle x_1 \overline{x}_1 d_1 x_2 \overline{x}_2 d_2 \cdots x_n \overline{x}_n d_n \rangle$ where $(x_1, ..., x_n)$ is the subsequence of honest datapoints in $\tilde{\mathbf{x}}$. We modify the notation for incremental gain slightly and denote by $G(e_i, \tilde{\mathbf{x}}_k)$, $G(\overline{e}_i, \tilde{\mathbf{x}}_k)$ and $G(\tilde{e}_i, \tilde{\mathbf{x}}_k)$ the incremental gains due to the datapoints x_i, $\overline{x}_i$, d_i respectively in the sequence $\tilde{\mathbf{x}}$ where $e_i \in \mathcal{H}$, $\overline{e} \in \mathbb{H}$ and $\tilde{e} \in \overline{\mathcal{H}}$ and the current round is k. Here the expectation is taken over the posterior distribution determined by the prior P_0^* and honest datapoints $(x_1, \ldots, x_n)$.

In our analysis we may need to refer to the regret of our algorithm under particular attacks. In that case, we will parameterize regret in a round k with respect to an attack strategy $\mathcal{A}$ as $\mathrm{Reg}_k(\mathcal{A})$ to make this connection explicit. We will also consider a reordering of the sequence $\tilde{\mathbf{x}}_k$ to analyze regret of the algorithm. Specifically, we consider the reordering $\tilde{\mathbf{x}}'_k$ obtained from $\tilde{\mathbf{x}}_k$ as

$$\tilde{\mathbf{x}}'_k = x_1 x_2 x_3 \ldots x_n \overline{x}_1 d_1 \overline{x}_2 d_2 \ldots \overline{x}_n d_n$$

Here, d_i depends only on $(x_1, \cdots, x_i)$. The sequence $\tilde{\mathbf{x}}'_k$ has the property that all the honest data are fully accounted for before the attack or influence-limit datapoints are received. We call this new attack $\mathcal{A}'$. Note that $\mathcal{A}'$ does not necessarily correspond to any feasible combination of attack data and influence limits, because $\overline{x}_i$ has a negative weight, unlike a real attack datapoint. However, we are using $\mathcal{A}'$ purely for

formal analysis of gain and regret, and so this does not matter.

Thus, the regret of our algorithm in a round k given attack $\mathcal{A}'$ is equal to the total error introduced after the optimal update, which is the negative of the sum of gains of all attack and influence-limit datapoints.

$$\mathrm{Reg}_k(\mathcal{A}') = -\mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_k)\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_k)}\left[\sum_{\bar{e}_i\in\mathbb{H}} \mathrm{G}(\bar{e}_i,\tilde{\mathbf{x}}'_k) + \sum_{\tilde{e}_i\in\overline{\mathcal{H}}} \mathrm{G}(\tilde{e}_i,\tilde{\mathbf{x}}'_k)\right]$$

We will now show that each honest expert has a higher expected gain under $\mathcal{A}$ than under $\mathcal{A}'$.

Lemma VI.10. *Let*

$$\tilde{\mathbf{x}}_k = \langle x_1\overline{x}_1 d_1 x_2\overline{x}_2 d_2 \ldots x_{i-1}\overline{x}_{i-1}d_{i-1}\ x_i\overline{x}_i d_i\ x_{i+1}\overline{x}_{i+1}d_{i+1}\ldots x_n\overline{x}_n d_n\rangle$$

be the sequence as input to the algorithm. Let

$$\tilde{\mathbf{x}}'_k = \langle x_1 x_2 \ldots x_{i-1}x_i x_{i+1}\ldots x_n\overline{x}_1 d_1\overline{x}_2 d_2\ldots\overline{x}_{i-1}d_{i-1}\ \overline{x}_i d_i\ \ldots\overline{x}_n d_n\rangle$$

be a reordering with all attacks coming after honest datapoints have been fully accounted for. Let $G(e_i,\tilde{\mathbf{x}}_k)$ and $G(e_i,\tilde{\mathbf{x}}'_k)$ be the respective incremental gains attributed to expert e_i for each of these sequence in round k. Recall that $\mathbf{x}_k$ is the subsequence of $\tilde{\mathbf{x}}_k$ consisting of all and only honest datapoints. If

$$\Delta_{i,k} \stackrel{\text{def}}{=} G(e_i,\tilde{\mathbf{x}}_k) - G(e_i,\tilde{\mathbf{x}}'_k)$$

then

$$\forall i : e_i \in \mathcal{H},\quad \mathrm{E}_{\mathbf{x}^{\mathrm{i}}_{\mathrm{k}}\sim\mathrm{T}_{\mathrm{k}}}[\Delta_{\mathrm{i,k}}] \geq 0$$

Proof. We will consider a particular honest expert $e_i \in \mathcal{H}$. We will define progressive

reorderings of the sequence in order to show that the statement of the lemma holds.

Recall that the actual sequence as input to the algorithm is $\tilde{\mathbf{x}}_k$. Construct a new sequence $\tilde{\mathbf{x}}_k^A$ defined as

$$\tilde{\mathbf{x}}_k^A = \langle x_1 x_2 \cdots x_{i-1} \overline{x}_1 d_1 \overline{x}_2 d_2 .. \overline{x}_{i-1} d_{i-1} \; x_i \; \overline{x}_i d_i x_{i+1} \overline{x}_{i+1} d_{i+1} \cdots x_n \overline{x}_n d_n \rangle$$

We are interested in the position of x_i in the sequence. Recall that this is the datapoint received from honest expert e_i.

Now, construct a new sequence $\tilde{\mathbf{x}}_k^B$, defined as

$$\tilde{\mathbf{x}}_k^A = \langle x_1 x_2 \cdots x_{i-1} \; x_i \; \overline{x}_1 d_1 \overline{x}_2 d_2 .. \overline{x}_{i-1} d_{i-1} \overline{x}_i d_i x_{i+1} \overline{x}_{i+1} d_{i+1} \cdots x_n \overline{x}_n d_n \rangle$$

Again note the position of x_i in the sequence.

We note the following relationships between the incremental gain attributed to e_i in the sequences defined above.

- $G(e_i, \tilde{\mathbf{x}}_k) = G(e_i, \tilde{\mathbf{x}}_k^A)$

  This is because the prefix of $\tilde{\mathbf{x}}_k$ and $\tilde{\mathbf{x}}_k^A$ before the datapoint x_i appears in each sequence is exactly

  $$\langle x_1 x_2 \cdots x_{i-1} \overline{x}_1 d_1 \overline{x}_2 d_2 .. \overline{x}_{i-1} d_{i-1} \rangle$$

  The equality follows from the definition of incremental gain.

- $\mathrm{E}[\mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}_\mathrm{k}^\mathrm{A})] \geq \mathrm{E}[\mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}_\mathrm{k}^\mathrm{B})]$

  Recall that each $\overline{x}_j d_j$ corresponds to a *weighted* update to the natural hyperparameter. Let $\mathbf{a} \stackrel{\text{def}}{=} \overline{x}_1 d_1 \overline{x}_2 d_2 ... \overline{x}_{i-1} d_{i-1}$. Note that this is a substring of both $\tilde{\mathbf{x}}_k^A$ and $\tilde{\mathbf{x}}_k^A$ and that they differ only in the relative position of the update $\mathbf{a}$ and the datapoint x_i. Further, the datapoints in $\mathbf{a}$ are independent of x_i. We assume that the prior is accurate and we observe therefore that the updates correspond-

ing to $x_1, x_2, \ldots, x_i$ represent accurate Bayesian updating. Thus, we find that the conditions of Theorem VI.7 are satisfied. $\mathrm{E}[\mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}_\mathrm{k}^\mathrm{A})] \geq \mathrm{E}[\mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}_\mathrm{k}^\mathrm{B})]$ follows as a consequence.

- $G(e_i, \tilde{\mathbf{x}}_k^B) = G(e_i, \tilde{\mathbf{x}}'_k)$

  This is because the prefix of $\tilde{\mathbf{x}}'_k$ and $\tilde{\mathbf{x}}_k^A$ before the datapoint x_i appears in each sequence is exactly $\langle x_1 x_2 \cdots x_{i-1} \rangle$. The equality follows from the definition of incremental gain.

Thus, $\mathrm{E}_{\mathbf{x}_\mathrm{k}^\mathrm{i} \sim \mathrm{T_k}}[\mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}_\mathrm{k})] \geq \mathrm{E}_{\mathbf{x}_\mathrm{k}^\mathrm{i} \sim \mathrm{T_k}}[\mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}'_\mathrm{k})]$ or $\mathrm{E}_{\mathbf{x}_\mathrm{k}^\mathrm{i} \sim \mathrm{T_k}}[\Delta_{\mathrm{i,k}}] \geq 0$ □

Next, we need to tackle the gains of the influence limit and attack datapoints. We denote by $\mathcal{A}$ the attack strategy that yields the sequence $\tilde{\mathbf{x}}_k$ as input to the algorithm. We define the *unaccounted regret* $\mathrm{UR}_k(\mathcal{A})$ as the regret solely due to influence limits:

$$\mathrm{UR}_k(\mathcal{A}) = \mathrm{Reg}_k(\mathcal{A}) + \mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_\mathrm{k}) \sim (\mathrm{T}_1, \mathrm{T}_2, \ldots \mathrm{T_k})} \sum_{\mathrm{e_i} \in \overline{\mathcal{H}}} \mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}_\mathrm{k})$$

Intuitively, the unnaccounted regret is of interest because the remainder of the regret – the attackers' gains – can be bounded in terms of the attackers' initial budgets, as in Theorem VI.2. Note that although the total regret does not depend on the particular sequence of datapoints, the unaccounted regret does. This is because the gains attributed to each attack identity may be different in different sequences.

Lemma VI.11. *Recall that for each $e_i \in \mathcal{H}$, there is a corresponding $\overline{e}_i \in \mathbb{H}$. Let $\tilde{\mathbf{x}}_k$ be the input extended sequence for round k. $\Delta_{i,k}$ is the difference in incremental gain due to reordering as defined in Lemma VI.10. Let $UR_k(\mathcal{A})$ be the unaccounted regret of round k under attack $\mathcal{A}$. Then, $UR_k(\mathcal{A})$ may also be written as:*

$$UR_k(\mathcal{A}) = -\mathrm{E}_{(\mathbf{x}_1, \mathbf{x}_2, .. \mathbf{x}_\mathrm{k}) \sim (\mathrm{T}_1, \mathrm{T}_2, \ldots \mathrm{T_k})} \sum_{\overline{\mathrm{e}}_\mathrm{i} \in \mathbb{H}} [\mathrm{G}(\overline{\mathrm{e}}_\mathrm{i}, \tilde{\mathbf{x}}_\mathrm{k}) + \Delta_{\mathrm{i,k}}]$$

Proof. Recall that $\mathrm{Reg}_k(\mathcal{A})$ is the regret of the algorithm in round k under attack $\mathcal{A}$. We note that, for any given $\mathbf{x}$, the final prediction of the algorithm is the same under both attacks $\mathcal{A}$ and $\mathcal{A}'$, because the order of the updates does not matter. It follows that, for given influence limits y_{ik}, $\mathrm{Reg}_k(\mathcal{A}) = \mathrm{Reg}_k(\mathcal{A}')$. Given the definition of $\mathrm{Reg}_k(\mathcal{A}')$, we have:

$$\mathrm{Reg}_k(\mathcal{A}) = \mathrm{Reg}_k(\mathcal{A}') = -\mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_\mathrm{k})\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_\mathrm{k})}\left[\sum_{\overline{\mathrm{e}}_\mathrm{i}\in\mathbb{H}}\mathrm{G}(\overline{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k}) + \sum_{\tilde{\mathrm{e}}_\mathrm{i}\in\overline{\mathcal{H}}}\mathrm{G}(\tilde{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k})\right]$$

Substituting this into the definition of unaccounted regret we have,

$$\mathrm{UR}_k(\mathcal{A}) = -\mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_\mathrm{k})\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_\mathrm{k})}\left[\sum_{\overline{\mathrm{e}}_\mathrm{i}\in\mathbb{H}}\mathrm{G}(\overline{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k}) + \sum_{\tilde{\mathrm{e}}_\mathrm{i}\in\overline{\mathcal{H}}}\mathrm{G}(\tilde{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k}) - \sum_{\mathrm{e}_\mathrm{i}\in\overline{\mathcal{H}}}\mathrm{G}(\mathrm{e}_\mathrm{i},\tilde{\mathbf{x}}_\mathrm{k})\right] \tag{6.7}$$

Further, from the fact that the total expected gain is the same under $\mathcal{A}$ and $\mathcal{A}'$, we have:

$$\mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_\mathrm{k})\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_\mathrm{k})}\left[\sum_{\mathrm{e}_\mathrm{i}\in\mathcal{H}}\mathrm{G}(\mathrm{e}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k}) + \sum_{\overline{\mathrm{e}}_\mathrm{i}\in\mathbb{H}}\mathrm{G}(\overline{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k}) + \sum_{\tilde{\mathrm{e}}_\mathrm{i}\in\overline{\mathcal{H}}}\mathrm{G}(\tilde{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k})\right]$$

$$= \mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_\mathrm{k})\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_\mathrm{k})}\left[\sum_{\mathrm{e}_\mathrm{i}\in\mathcal{H}}\mathrm{G}(\mathrm{e}_\mathrm{i},\tilde{\mathbf{x}}_\mathrm{k}) + \sum_{\overline{\mathrm{e}}_\mathrm{i}\in\mathbb{H}}\mathrm{G}(\overline{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}_\mathrm{k}) + \sum_{\tilde{\mathrm{e}}_\mathrm{i}\in\overline{\mathcal{H}}}\mathrm{G}(\tilde{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}_\mathrm{k})\right]$$

Rearranging, we have

$$\begin{aligned}
\mathrm{UR}_k(\mathcal{A}) &= -\mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_\mathrm{k})\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_\mathrm{k})}\left[\sum_{\overline{\mathrm{e}}_\mathrm{i}\in\mathbb{H}}\mathrm{G}(\overline{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k}) + \sum_{\tilde{\mathrm{e}}_\mathrm{i}\in\overline{\mathcal{H}}}\mathrm{G}(\tilde{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k}) - \sum_{\tilde{\mathrm{e}}_\mathrm{i}\in\overline{\mathcal{H}}}\mathrm{G}(\tilde{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}_\mathrm{k})\right] \\
&\qquad \text{(from Equation (6.7))} \\
&= -\mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_\mathrm{k})\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_\mathrm{k})}\left[\sum_{\overline{\mathrm{e}}_\mathrm{i}\in\mathbb{H}}\mathrm{G}(\overline{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}_\mathrm{k}) + \left(\sum_{\mathrm{e}_\mathrm{i}\in\mathcal{H}}\mathrm{G}(\mathrm{e}_\mathrm{i},\tilde{\mathbf{x}}_\mathrm{k}) - \sum_{\mathrm{e}_\mathrm{i}\in\mathcal{H}}\mathrm{G}(\mathrm{e}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k})\right)\right] \\
&= -\mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_\mathrm{k})\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_\mathrm{k})}\left[\sum_{\overline{\mathrm{e}}_\mathrm{i}\in\mathbb{H}}\mathrm{G}(\overline{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}_\mathrm{k}) + \Delta_{\mathrm{i,k}}\right] \quad \text{(by defintion of } \Delta_{i,k}\text{)}
\end{aligned}$$

□

Next, we bound the total gain of the influence limiting identities $\overline{e}_i \in \mathbb{H}$ by relating them to the gain of the corresponding honest entities $e_i \in \mathcal{H}$.

Lemma VI.12. *Fix reputation values, and hence influence values y_{ik}. Then, for each $e_i \in \mathcal{H}$ and corresponding $\overline{e}_i \in \mathbb{H}$,*

$$\mathrm{E}_{\mathbf{x}_\mathrm{k}\sim\mathrm{T}_\mathrm{k}}\mathrm{G}(\overline{\mathrm{e}}_\mathrm{i},\tilde{\mathbf{x}}_\mathrm{k}) \geq -\overline{\mathrm{y}}_{\mathrm{ik}}\mathrm{E}_{\mathbf{x}_\mathrm{k}\sim\mathrm{T}_\mathrm{k}}\left[\mathrm{G}(\mathrm{e}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k})+\Delta_{\mathrm{i,k}}\right]$$

Proof. Consider the sequence $\tilde{\mathbf{x}}_k$. Recall that the consecutive pair of "datapoints" $x_i\overline{x}_i$ is a model for the influence-limited report by expert $e_i \in \mathcal{H}$. By the concavity of the gain function, we have:

$$G(e_i,\tilde{\mathbf{x}}_k)+G(\overline{e}_i,\tilde{\mathbf{x}}_k) \geq y_{ik}G(e_i,\tilde{\mathbf{x}}_k)$$

This implies that $G(\overline{e}_i,\tilde{\mathbf{x}}_k) \geq -\overline{y}_{ik}G(e_i,\tilde{\mathbf{x}}_k)$.

By definition of Δ_i, we have $G(e_i,\tilde{\mathbf{x}}_k) = G(e_i,\tilde{\mathbf{x}}'_k)+\Delta_i$ and we are done. □

Putting together Lemma VI.11 and Lemma VI.12, we get the following bound on $\mathrm{UR}_k(\mathcal{A})$:

Lemma VI.13.

$$UR_k(\mathcal{A}) \leq \mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_\mathrm{k})\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_\mathrm{k})}\sum_{\mathrm{e_i}\in\mathcal{H}}\overline{\mathrm{y}}_{\mathrm{ik}}\mathrm{G}(\mathrm{e}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k})$$

Proof. From Lemma VI.11 and Lemma VI.12, we get:

$$\mathrm{UR}_k(\mathcal{A}) \leq \mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_\mathrm{k})\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_\mathrm{k})}\sum_{\mathrm{e_i}\in\mathcal{H}}\overline{\mathrm{y}}_{\mathrm{ik}}\mathrm{G}(\mathrm{e}_\mathrm{i},\tilde{\mathbf{x}}'_\mathrm{k})+\sum_{\mathrm{e_i}\in\mathcal{H}}(\overline{\mathrm{y}}_{\mathrm{ik}}-1)\Delta_{\mathrm{i,k}}$$

By Lemma VI.10, each $\Delta_{i,k} \geq 0$. Further, $0 \leq \overline{y}_{ik} \leq 1$. Thus, $\sum_{e_i \in \mathcal{H}} (\overline{y}_{ik} - 1)\Delta_{i,k} \leq 0$ and the lemma statement follows. □

This allows us to show that the regret can be bounded by the sum of the damage and information loss bounds. Recall that the hybrid stochastic-adversarial notion of *regret* of algorithm Z is defined as

$$\mathrm{Reg}(Z) = \max_{\mathcal{H},\{T_i\},\mathcal{A}} \left\{ \sum_{k=1}^{M} E_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_k)\sim(T_1,T_2,...T_k)} \left[\log \mathbf{Q}_k(\boldsymbol{\beta}_k) - \log Q_k(\boldsymbol{\beta}_k) \right] \right\}$$

Equivalently, the regret can be defined in terms of the incremental gains, as:

$$\mathrm{Reg}(Z) = \max_{\mathcal{H},\{T_i\},\mathcal{A}} \left\{ \sum_{k=1}^{M} \mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_k)\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_k)} \left[\sum_{\mathrm{i}\in\mathcal{H}\cup\overline{\mathcal{H}}} \mathrm{G}_{\mathrm{ik}} - \sum_{\mathrm{i}\in\mathcal{H}} \mathrm{h}_{\mathrm{ik}} \right] \right\}$$

Theorem VI.14. *The regret of the conjugate-prior algorithm is bounded by:*

$$D \left\{ \sum_{i\in\mathcal{H}} \left[2 + \frac{8}{\alpha} + \frac{8}{3\alpha} \log(1 + e^{-r_{i1}}) \right] + \sum_{i\in\overline{\mathcal{H}}} \frac{1}{\alpha} \log(1 + e^{r_{i1}}) \right\}$$

Proof. Consider any given attack $\mathcal{A}$. By lemma VI.13, the regret in round k is bounded by:

$$\mathrm{Reg}_k(\mathcal{A}) \leq \mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_k)\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_k)} \sum_{\mathrm{e_i}\in\mathcal{H}} \overline{\mathrm{y}}_{\mathrm{ik}} \mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}'_{\mathrm{k}}) + \sum_{\mathrm{e_i}\in\overline{\mathcal{H}}} -\mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}_{\mathrm{k}})$$

Summing over all rounds k from 1 to M, we have:

$$\mathrm{Reg}(\mathcal{A}) \leq \mathrm{E}_{(\mathbf{x}_1,\mathbf{x}_2,..\mathbf{x}_k)\sim(\mathrm{T}_1,\mathrm{T}_2,...\mathrm{T}_k)} \left[\sum_{\mathrm{k}} \sum_{\mathrm{e_i}\in\mathcal{H}} \overline{\mathrm{y}}_{\mathrm{ik}} \mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}'_{\mathrm{k}}) + \sum_{\mathrm{k}} \sum_{\mathrm{e_i}\in\overline{\mathcal{H}}} -\mathrm{G}(\mathrm{e_i}, \tilde{\mathbf{x}}_{\mathrm{k}}) \right]$$

By Theorem VI.6, and using un-scaled log loss, the first sum is bounded by

$$\sum_{e_i \in \mathcal{H}} D \left[2 + \frac{8}{\alpha} + \frac{8}{3\alpha} \log(1 + e^{-r_{i1}}) \right]$$

By Theorem VI.2, and using un-scaled log loss, the second sum is bounded by $\sum_{e_i \in \overline{\mathcal{H}}} \frac{D}{\alpha} B(r_{i1})$.

Thus, putting these two together, we have:

$$\mathrm{Reg}(\mathcal{A}) \leq D \left\{ \sum_{i \in \mathcal{H}} \left[2 + \frac{8}{\alpha} + \frac{8}{3\alpha} \log(1 + e^{-r_{i1}}) \right] + \sum_{i \in \overline{\mathcal{H}}} \frac{1}{\alpha} B(r_{i1}) \right\}$$

□

6.8 Discussion and Conclusion

In this chapter, we have defined a new model of learning which models the sequential nature of advice availability. We analyze expert behavior in a hybrid model to capture the fact that some experts behave essentially as stochastic generative processes and others may exhibit adversarial behavior. We defined a natural notion of regret in this model and proved a regret bound for our algorithm. This notion of sequentially arriving expert advice has not been exploited in previous online learning models, to the best of our knowledge. Further, the hybrid stochastic-adversarial analysis is unique in the way that it models expert behavior. Thirdly, our model illustrate how using a prediction market metaphor can inform the weight updates on experts to yield non-trivial regret bounds.

Comparison to sleeping expert models: Partial availability of expert advice has been studied in prior work. In statistics, lack of information is usually modeled as 'missing data' (see for instance *Little and Rubin* (1986)), but it is usually under

the assumption of stochasticity rather than in an adversarial model. In online learning literature, this feature has been studied previously as 'predictors that specialize' *Freund et al.* (1997) or 'sleeping experts' *Blum and Mansour* (2007b); *Kleinberg et al.* (2008); *Kanade et al.* (2009). We can highlight the difference between our sequential scoring and other models that treat agents' reports on an item as simultaneous through the following attack scenario. Suppose that there is one honest agent and n attack identities; the honest agent rates item 1, and the attack raters copy the honest agent's report on this item. Subsequently, each of the $n+1$ raters rates a different item. A model that ignored the timing of ratings would have to treat each agent symmetrically, whereas our sequential gain would give a greater score to the honest agent on the first item, and hence suffer less in the future. Our regret analysis shows that, if the attacker decided to rate before the honest agent on item 1, she would do even worse because she could not predict the honest agent's report.

On the flip side, our algorithm would reward an earlier honest agent more than a later honest agent in expectation, and hence, may create races between strategic informed agents.

Some unanswered questions: One important direction for future work is to prove general bounds on the variance in terms of the expected gain. We would conjecture that a bound of $c = 2$ holds for general exponential families, but we do not yet have a proof. One further modification that is possible in the model is if eventually we only observe one sample x^* from the distribution instead of the true $\boldsymbol{\beta}$. It will be interesting to characterize all exponential families for which we could still prove the regret bound.

CHAPTER VII

Conclusions and Future Work

In this thesis, we have looked at prediction markets from two points of view. On the one hand, we designed a prediction market mechanism that incentivizes participation financially and provides a probability estimate on the event outcome. We showed that this mechanism can be shown to perform a machine learning algorithm on the private beliefs of traders in the market. On the other hand, we used a prediction market metaphor to design machine learning algorithms for social computing. We will now briefly list the specifics of our contributions.

7.1 Summary of Contributions

Exponential Family Prediction Markets We defined an automated market maker derived from a generalized log market scoring rule. We showed that we can design these mechanisms using *exponential family distributions*, a popular and well-studied class of probability distributions used in statistics. We showed a range of benefits of defining the mechanism in this way. We drew connections between the information aggregation of market prices and the belief aggregation of learning agents that rely on exponential family distributions. We developed a natural analysis of the market behavior as well as the price equilibrium under the assumption that the traders exhibit risk aversion according to exponential

utility. We also considered similar aspects under alternative models, such as budget-constrained traders.

Interaction between Prediction Markets We proposed a technique to determine the surplus resulting from running multiple markets on the same event and showed how the market makers might split this surplus. We also designed and analyzed the effect of trades in one market on another market on a related variable. We found that we are able to precisely characterize the effect of such trades using graphical models. We were also able to characterize the interaction of a trader with the market when the trader is partially informed. Interestingly, the optimal trader behaves in accordance with the updates in the EM algorithm.

Myopic Learning with Partial Feedback We used the recommender system setting to model a learning problem. The particular challenge here was to extract as much information as possible from informative sources while limiting damage from malicious ones. We accomplished this using a hybrid sequential analytic technique based on prediction markets under partial feedback from the environment. Under these conditions and a restricted definition of regret we showed that this algorithm has a regret bound of $O(n\sqrt{T}\log T)$ for T rounds and n experts.

Bounded Regret Sequential Learning of Exponential Families We showed that learning the parameters of an exponential family using conjugate priors in an adversarial noise setting can be done with regret bounded as $O(a\log(1+e^{-r}) + b\log(1+e^{-r}))$ where r is an algorithm parameter and $a+b$ is the total number of experts. We also proposed an abstract architecture that can be used to apply this setting and analysis to any problem that satisfies certain properties.

Future Directions

Prediction markets are an emerging form of financial markets whose goal is to use the power of collective human intelligence to efficiently and accurately forecast future events. There is mounting evidence that prediction markets are better predictors than other techniques like polling and statistical estimates (*Hanson*, 1999). But, as scientists, we are not satisfied in simply knowing *that* these markets work well, but also *why* they do, whether these results are *repeatable* and to *what degree*. In other words, we would like to build a model to explain the process and thence construct sound prediction market machinery from the ground up. There seem to be several avenues of further exploration leading from the work done in this thesis. We list a few below.

Risk Measures to Model Trader Behavior We have shown that the equilibrium market state in our prediction market mechanism is a risk-tolerance-weighted average of the natural parameters of the traders and the market maker, with the more risk tolerant traders contributing more to the market state. This result is quite natural, but appears to crucially depend on the synergy between exponential families and exponential utility. Based on recent promising results (*Hu and Storkey*, 2014; *Othman and Sandholm*, 2011), Jacob Abernethy, Rafael Frongillo and I advocate using *risk measures*, previously used predominantly in financial mathematics, as a way to analyze trading decisions made by agents in prediction markets (*Abernethy et al.*, 2014a). For instance, Frongillo and Reid (*Frongillo and Reid*, 2014) show that the equilibrium result we attained in exponential family markets extends to risk-tolerance families of arbitrary risk measures: if the market maker is risk-constant and traders seek to minimize their own risk measure, then the equilibrium state is again the weighted average of trader beliefs. Is it possible that modeling trader behavior using risk measures

would allow us to generalize our other results from agents with exponential family beliefs to arbitrary beliefs?

Market Interactions Based on Graphical Models In this thesis, we have demonstrated the applicability of graphical models as a tool for formalizing the interactions between markets on multiple, possibly interrelated, events. There are various inference algorithms, called message passing algorithms, that run efficiently on graphical models by exploiting the structure of the graph. If we design markets based on graphical models, it seems likely that these messages have particular significance as trades amongst market makers. Can this be established more precisely? We have been able to specify market mechanisms for multiple events based on graphical models that represent the interdependence of these events. If traders are assumed to have knowledge of only some of these events, we have shown that their optimal trades can be understood in terms of the Expectation Maximization algorithm. If you have several such traders, can the equilibrium state also be precisely determined?

Manipulation in Prediction Markets There has been some work (both theoretical and experimental) on studying manipulation in binary outcome markets (*Dimitrov and Sami*, 2010; *Chen et al.*, 2010; *Jian and Sami*, 2012). However, these results have been largely negative. In particular, it is possible under certain information structures of the traders for some traders to profit by either strategically delaying trading or bluffing. However, the equilibrium market state under these conditions has not yet been characterized completely. In exponential family markets under exponential family beliefs, we have been able to exactly specify the effect of a trade on the trader's private belief. Is it possible to specify an optimal sequence of trades based on the updated belief of the trader? What effect would this have on the manipulation resistance of these

markets?

Designing and analyzing social computing systems based on theoretical foundations from statistics, economics and computer science will lead to a better understanding and more sound designs of social computing mechanisms in general and prediction markets in particular. This is crucial in bridging the current gap between theory and practice in this area.

BIBLIOGRAPHY

BIBLIOGRAPHY

Abernethy, J., and R. M. Frongillo (2012), A characterization of scoring rules for linear properties, in *Proceedings of the 25th Annual Conference on Learning Theory*.

Abernethy, J., Y. Chen, and J. Wortman Vaughan (2011), An optimization-based framework for automated market-making, in *Proceedings of the 12th ACM conference on Electronic commerce*, EC '11, pp. 297–306, ACM, New York, NY, USA.

Abernethy, J., Y. Chen, and J. W. Vaughan (2013), Efficient market making via convex optimization, and a connection to online learning, *ACM Transactions on Economics and Computation*, *1*(2).

Abernethy, J., R. M. Frongillo, and S. Kutty (2014a), On exponential families, market making, and risk measures, *Letter submitted to SIGecom Exchanges*, *13*(2).

Abernethy, J., S. Kutty, S. Lahaie, and R. Sami (2014b), Information aggregation in exponential family markets, in *Proceedings of the Fifteenth ACM Conference on Economics and Computation*, pp. 395–412, ACM.

Angluin, D. (1988), Queries and concept learning, *Machine Learning*, *2*(4), 319–342.

Awerbuch, B., and R. Kleinberg (2008), Competitive collaborative learning, *Journal of Computer and System Sciences*, *74*, 1271–1288.

Azoury, K. S., and M. K. Warmuth (2001), Relative loss bounds for on-line density estimation with the exponential family of distributions, *Machine Learning*, *43*, 211–246.

Banerjee, A., I. S. Dhillon, and J. Ghosh (2005a), Clustering with bregman divergences, *Journal of Machine Learning Research*, *6*, 1705–1749.

Banerjee, A., I. S. Dhillon, J. Ghosh, and S. Sra (2005b), Clustering on the unit hypersphere using von mises-fisher distributions, *Journal of Machine Learning Research*, *6*, 1345–1382.

Barndorff-Nielsen, O. (1978), *Information and Exponential Families in Statistical Theory*, Wiley Publishers.

Bell, T. W. (2009), Private prediction markets and the law, *Journal of Prediction Markets*, *3*(1), 89–110.

Bennett, G. (1962), Probability inequalities for the sum of independent random variables, *J. Amer. Statist. Soc.*, *57*, 33–45.

Blum, A., and Y. Mansour (2007a), Learning, regret minimization, and equilibria, in *Algorithmic Game Theory*, edited by N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, chap. 4, Cambridge University Press.

Blum, A., and Y. Mansour (2007b), From external to internal regret, *J. Mach. Learn. Res.*, *8*, 1307–1324.

Brier, G. (1950), Verification of forecasts expressed in terms of probability, *Monthly weather review*, *78*(1), 1–3.

Cesa-Bianchi, N., and G. Lugosi (2006), *Prediction, Learning, and Games*, Cambridge University Press.

Chen, Y., and D. M. Pennock (2007), A utility framework for bounded-loss market makers, in *In Proceedings of the 23rd Conference on Uncertainty in Artificial Intelligence (UAI)*, pp. 49–56.

Chen, Y., and J. W. Vaughan (2010), A new understanding of prediction markets via no-regret learning, in *Proceedings of the 11th ACM conference on Electronic commerce*, EC '10, pp. 189–198, ACM, New York, NY, USA.

Chen, Y., S. Dimitrov, R. Sami, D. Reeves, D. Pennock, R. Hanson, L. Fortnow, and R. Gonen (2010), Gaming prediction markets: Equilibrium strategies with a market maker, *Algorithmica*, *58*(4), 930969.

Chen, Y., M. Ruberry, and J. Wortman Vaughan (2013), Cost function market makers for measurable spaces, in *Proceedings of the 14th ACM Conference on Electronic Commerce*.

Cowgill, B., J. Wolfers, and E. Zitzewitz (2009), Using prediction markets to track information flows: Evidence from google., in *AMMA*, p. 3.

Dawid, A. P. (1998), Coherent measures of discrepancy, uncertainty and dependence with applications to bayesian predictive experimental design, *Tech. Rep. 139*, University College London, Dept. of Statistical Science.

Dawid, A. P., and P. Sebastiani (1999), Coherent dispersion criteria for optimal experimental design, *Annals of Statistics*, *27*, 65–81.

Dekel, O., F. Fischer, and A. D. Procaccia (2008), Incentive compatible regression learning, in *Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms*, SODA '08, pp. 884–893, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA.

Diaconis, P., and D. Ylvisaker (1979), Conjugate priors for exponential families, *Annals of Statistics*, *7*(2), 269–281.

Dimitrov, S., and R. Sami (2008), Non-myopic strategies in prediction markets, in *Proceedings of the 9th ACM Conference on Electronic Commerce (EC)*, pp. 200–209.

Dimitrov, S., and R. Sami (2010), Composition of markets with conflicting incentives, in *Proceedings of the 11th ACM Conference on Electronic Commerce*, EC '10, pp. 53–62, ACM, New York, NY, USA.

Föllmer, H., and T. Knispel (2011), Entropic risk measures: Coherence vs. convexity, model ambiguity and robust large deviations, *Stochastics and Dynamics*, *11*, 333–351.

Föllmer, H., and A. Schied (2002), Convex measures of risk and trading constraints, *Finance and Stochastics*, *6*(4), 429–447.

Föllmer, H., and A. Schied (2004), *Stochastic Finance: An Introduction in Discrete Time*, de Gruyter Studies in Mathematics, Walter de Gruyter.

Fortnow, L., and R. Sami (2012), Multi-outcome and multidimensional market scoring rules, *Tech. Rep. 1202.1712*, arXiv.org e-Print archive.

Freund, Y., R. E. Schapire, Y. Singer, and M. K. Warmuth (1997), Using and combining predictors that specialize, in *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, STOC '97, pp. 334–343, ACM, New York, NY, USA.

Frongillo, R. M., and M. D. Reid (2013), Convex foundations for generalized maxent models, in *Proceedings of the 33rd International Workshop on Bayesian Inference and Maximum Entropy Methods in Science and Engineering (MaxEnt)*.

Frongillo, R. M., and M. D. Reid (2014), Risk dynamics in trade networks, *arXiv:1410.0413*.

Frongillo, R. M., N. D. Penna, and M. D. Reid (2012), Interpreting prediction markets: a stochastic approach, in *Proceedings of Neural Information Processing Systems (NIPS)*.

Gao, X., Y. Chen, and D. M. Pennock (2009), Betting on the real line, in *Proceedings of the 5th International Workshop on Internet and Network Economics (WINE)*, pp. 553–560.

Gneiting, T., and A. Raftery (2007), Strictly proper scoring rules, prediction, and estimation, *Journal of the American Statistical Association*, *102*(477), 359–378.

Grünwald, P., and A. P. Dawid (2004), Game theory, maximum entropy, minimum discrepancy and robust bayesian decision theory, *Annals of Statistics*, *32*(4), 1367–1433.

Gut, A. (1995), *An Intermediate Course in Probability*, Springer-Verlag.

Hanson, R. (1999), Decision Markets, *IEEE Intelligent Systems*, *14*(3), 16–19.

Hanson, R. (2003a), Combinatorial information market design, *Information Systems Frontiers*, *5*(1), 105–119.

Hanson, R. (2003b), Combinatorial information market design, *Information Systems Frontiers*, *5*(1), 107–119, doi:http://dx.doi.org/10.1023/A:1022058209073.

Hanson, R. (2007), Logarithmic market scoring rules for modular combinatorial information aggregation, *Journal of Prediction Markets*, *1*(1), 3–15.

Helmbold, D. P., N. Littlestone, and P. M. Long (1992), Apple tasting and nearly one-sided learning, in *SFCS '92: Proceedings of the 33rd Annual Symposium on Foundations of Computer Science*, pp. 493–502, IEEE Computer Society, Washington, DC, USA, doi:http://dx.doi.org/10.1109/SFCS.1992.267802.

Hu, J., and A. J. Storkey (2014), Multi-period trading prediction markets with connections to machine learning, in *Proceedings of the 31th International Conference on Machine Learning, ICML 2014, Beijing, China, 21-26 June 2014*, pp. 1773–1781.

Jewell, W. S. (1974), Credible means are exact bayesian for exponential families, *Astin Bulletin*, *8*(1), 77–90.

Jian, L., and R. Sami (2012), Aggregation and manipulation in prediction markets: Effects of trading mechanism and information distribution, *Management Science*, *58*(1), 123–140.

Kalai, A., and S. Vempala (2005), Efficient algorithms for online decision problems, *J. Comput. Syst. Sci.*, *71*, 291–307.

Kanade, V., H. B. McMahan, and B. Bryan (2009), Sleeping experts and bandits with stochastic action availability and adversarial rewards, in *Proceedings of the 12th International Conference on Artificial Intelligence and Statistics*.

Kelly, J. L. (1956), A new interpretation of information rate, *Bell System Technical Journal*, *35*, 917–926.

Kleinberg, R. D., A. Niculescu-Mizil, and Y. Sharma (2008), Regret bounds for sleeping experts and bandits, in *21st Annual Conference on Learning Theory - COLT 2008*, pp. 425–436.

Kutty, S., and R. Sami (2010), A prediction market approach to learning with sequential advice, in *NIPS Workshop on Computational Social Science and the Wisdom of Crowds*, Vancouver, Canada.

Kutty, S., and R. Sami (2011), Bounded regret sequential learning using prediction markets, in *NIPS Workshop on Relations between Machine Learning Problems*.

Lambert, N. S., D. M. Pennock, and Y. Shoham (2008), Eliciting properties of probability distributions, in *Proceedings of the 9th ACM Conference on Electronic Commerce*, pp. 129–138.

Lay, N., and A. Barbu (2010), Supervised Aggregation of Classifiers using Artificial Prediction Markets, in *Proceedings of the 27th International Conference on Machine Learning (ICML-10)*, edited by J. Fürnkranz and T. Joachims, pp. 591–598, Omnipress, Haifa, Israel.

Little, R. J. A., and D. B. Rubin (1986), *Statistical analysis with missing data*, John Wiley & Sons, Inc., New York, NY, USA.

Littlestone, N., and M. K. Warmuth (1994), The weighted majority algorithm, *Inf. Comput.*, *108*, 212–261.

Littlestone, N., P. M. Long, and M. K. Warmuth (1991), On-line learning of linear functions, in *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, STOC '91, pp. 465–475, ACM, New York, NY, USA.

Manski, C. F. (2004), Interpreting the predictions of prediction markets, *Working Paper 10359*, National Bureau of Economic Research.

McCarthy, J. (1956), Measures of the value of information, *Proceedings of the National Academy of Sciences (PNAS)*, *42*(9), 654.

Monderer, D., and L. S. Shapley (1996), Potential games, *Games and Economic Behavior*, *14*(1), 124–143.

Ostrovsky, M. (2012), Information aggregation in dynamic markets with strategic traders, *Econometrica*, *80*(6), 2595–2647.

Othman, A., and T. Sandholm (2011), Liquidity-sensitive automated market makers via homogeneous risk measures, in *Internet and Network Economics*, pp. 314–325, Springer.

Pennock, D. M. (1999), Aggregating probabilistic beliefs: Market mechanisms and graphical representations, Ph.D. thesis, University of Michigan, Ann Arbor.

Pennock, D. M., and R. Sami (2007), Computational aspects of prediction markets, in *Algorithmic Game Theory*, edited by N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, chap. 26, Cambridge University Press.

Pennock, D. M., and M. P. Wellman (1997), Representing aggregate belief through the competitive equilibrium of a securities market, in *Proceedings of the Thirteenth Conference on Uncertainty in Artificial Intelligence*, UAI'97, pp. 392–400, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

Pennock, D. M., and M. P. Wellman (2005), Graphical models for groups: Belief aggregation and risk sharing, *Decision Analysis*, *2*(3), 148–164, doi:10.1287/deca.1050.0048.

Pennock, D. M., S. Lawrence, C. L. Giles, F. A. Nielsen, et al. (2001), The real power of artificial markets, *Science*, *291*(5506), 987–988.

Resnick, P., and R. Sami (2007), The influence limiter: Provably manipulation-resistant recommender systems, in *Proceedings of the ACM Recommender Systems Conference (RecSys07)*.

Roll, R. (1984), Orange juice and weather, *American Economic Review*, *74*(5), 861–80.

Savage, L. J. (1971), Elicitation of personal probabilities and expectations, *Journal of the American Statistical Association*, *66*, 783–801.

Shafer, G., and V. Vovk (2001), *Probability and Finance: It's Only a Game!*, John Wiley and Sons.

Sherman, J., and W. J. Morrison (1950), Adjustment of an inverse matrix corresponding to a change in one element of a given matrix, *The Annals of Mathematical Statistics*, *21*(1), 124–127.

Storkey, A. J. (2011), Machine learning markets, in *Proceedings of AI and Statistics (AISTATS)*, pp. 716–724.

Sun, W., R. Hanson, K. Laskey, and C. Twardy (2012), Probability and Asset Updating using Bayesian Networks for Combinatorial Prediction Markets, in *Proceedings of the Twenty-Eighth Conference on Uncertainty in Artificial Intelligence (UAI'12)*.

Sun, W., R. Hanson, K. Laskey, and C. Twardy (2013), Learning parameters by prediction markets and kelly rule for graphical models, in *Proceedings of the 2013 UAI Application Workshops: Big Data meet Complex Models and Models for Spatial, Temporal and Network Data (UAI2013AW)*, edited by R. Almond and O. Mengshoel, no. 1024 in CEUR Workshop Proceedings, pp. 39–48, Aachen.

Surowiecki, J. (2005), *The Wisdom of Crowds*, Random House.

Tang, H.-K., and C.-T. See (2009), Variance inequalities using first derivatives, *Statistics and Probability Letters*, *79*(9), 1277 – 1281.

Varian, H. R. (1992), *Microeconomic Analysis*, W. W. Norton and Company.

Vovk, V., I. Nouretdinov, A. Takemura, and G. Shafer (2005), Defensive forecasting for linear protocols, *CoRR*, *abs/cs/0506007*.

Wagman, L., and V. Conitzer (2008), Optimal false-name-proof voting rules with costly voting, in *AAAI'08: Proceedings of the 23rd national conference on Artificial intelligence*, pp. 190–195, AAAI Press.

Wainwright, M. J., and M. I. Jordan (2008), Graphical models, exponential families, and variational inference, *Foundations and Trends in Machine Learning*, *1*, 1–305.

Wolfers, J., and E. Zitzewitz (2006), Interpreting prediction market prices as probabilities, *Tech. rep.*, National Bureau of Economic Research.

Yu, H., C. Shi, M. Kaminsky, P. B. Gibbons, and F. Xiao (2009), Dsybil: Optimal sybil-resistance for recommendation systems, in *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, pp. 283–298, IEEE Computer Society, Washington, DC, USA.