Spring 6-10-2017

MANIPULATION IN PREDICTION MARKETS – CHASING THE FRAUDSTERS

Simon Kloker
Karlsruhe Institute of Technology, simon.kloker@kit.edu

Tobias T. Kranz
Karlsruhe Institute of Technology, tobias.kranz@gmx.de

MANIPULATION IN PREDICTION MARKETS – CHASING THE FRAUDSTERS

Research in Progress

Kloker, Simon, Karlsruhe Institute of Technology, Karlsruhe, Germany, simon.kloker@kit.edu

Kranz, Tobias T., Karlsruhe Institute of Technology, Karlsruhe, Germany, tobias.kranz@gmx.de

Abstract

Prediction markets are a common instrument in forecasting and corporate knowledge management. Based on the "wisdom of the crowd" its forecasts regularly outperform polls as well as statistical models. In addition, it offers a convenient way to collect dispersed information in organizations and incite employees to reveal private information as well as to stay informed. Although such markets are well established, there still remain open questions regarding their operation and maintenance. Especially the issue of manipulation and fraud, which are reported in many cases, is only rarely addressed; if so, only very theoretical or with complex algorithms, hard to implement for practitioners. Yet, a rigid framework, uncovering weaknesses of prediction markets and offering applicable prevention and detection strategies is missing. We propose the Fraud Cube, a concise framework unveiling fraudster's thought process and thus potential attack vectors. Additionally, we present an easy to implement detection algorithm based on state of the art detection heuristics. Finally, we show not less than comparable detection rates to established detection algorithms whilst providing superior applicability.

Keywords: Prediction markets, Manipulation, Fraud detection, Knowledge management, Forecasting.

1 Introduction

Forecasting the outcomes of future events is essential in managerial and political decision-making. In recent years new methods, which forecast by relying on the „wisdom of the crowd", have emerged. Such are, e.g., prediction markets, which are suggested and used for corporate decision making (Buckley, 2016, Klein & Garcia, 2015) as Yahoo, Google, or Microsoft have shown. They use them to collect dispersed information, create or evaluate new ideas and products, or forecast project milestones (Mangold et al., 2005, Cowgill, Wolfers, & Zitzewitz, 2009, H. Berg & Proebsting, 2009). Prediction markets provide a simple and convenient way of revealing and aggregating information accumulated by a large set of people. Participants are motivated by monetary incentives, lotteries or gamification elements that prediction markets add to the forecasting tasks. Moreover, prediction markets are suitable for various contexts. Recent studies report applications of prediction markets in politics, sports, economic development, market research in media and entertainment, science and technology forecasting, or forecasting events (J. E. Berg, Forsythe, & Rietz, 1997, Luckner, Kratzer, & Weinhardt, 2005, Teschner, Stathel, & Weinhardt, 2011, Laskey, Hanson, & Twardy, 2015, Servan-Schreiber, Wolfers, Pennock, & Galebach, 2004). Especially in play-money prediction markets, the intrinsic motivation of participants to trade competitively against each other on a market, or just the excitement of trading, leads to the collection and aggregation of a vast amount of information (Buckley, 2016, Luckner & Weinhardt, 2007). As a key advantage in contrast to polls or other forms of surveys, prediction mar-

kets can be used to get a continuous forecast for basically anything that can be modelled in contracts. The basic idea behind prediction markets is, that the revelation of truthful information is incited by a market mechanism. Participants can trade probabilities or absolute numbers of events in the market and are paid off according to their performance (Luckner & Weinhardt, 2007). Thus, successful (e.g. informed) traders gain money and impact while bad (e.g. uninformed) traders lose money and impact.

Wolfers and Zitzewitz (2006) identified manipulative and fraudulent actions as one of the five open questions about prediction markets. Various authors report cases of manipulation and addressed this topic since then (and even before), e.g. Blume, Luckner, and Weinhardt (2010), Deck, Lin, and Porter (2013), Hansen, Schmidt, and Strobel (2004), Hanson, Oprea, and Porter (2006), Jian and Sami (2012), Rhode and Strumpf (2008). Nevertheless, we feel a lack of an applicable to protect prediction markets and unveil vulnerable points. Thus, we provides both: i) a framework to organize and understand fraudulent actions as well as ii) an easy to implement detection heuristic. The remainder of this work is structured as follows: First, we summarize the literature about market manipulation and fraud. Second, we introduce the "Fraud Cube", a concept enabling prediction market engineers to better understand fraud in prediction markets and uncover weak points. Third, we investigate common attacking patterns. Finally, we present, based on our findings, an easy to apply detection heuristic and evaluate it against the backdrop of state of the art approaches.

2 Related Work

2.1 Manipulation in Prediction Markets

Manipulation in prediction markets has been considered by various authors in the last decades. Rhode and Strumpf (2008), p. 6 define a (successful) manipulation in the context of prediction markets as *"[...] a speculative attack that achieves its objective of changing prices"*. Accordingly, this can only be achieved, if that speculative trade is able to influence the beliefs of the other traders. Hence, a speculative attack is a trade that is uninformed by fundamentals intended to change prices, whereas a "fundamental" is information that changes the value of the underlying contract. Based on the observation of real-world data from TradeSports prediction market, Rhode and Strumpf (2008) *"[…] find little evidence that political stock markets [(PSM)] can be systematically manipulated beyond short time periods."* This, however, is the prevailing opinion in literature (i.a. shared by Wolfers and Zitzewitz (2004), Wolfers and Leigh (2002), Camerer (1998), Hansen et al. (2004)). Oprea, Porter, Hibbert, Hanson, and Tila (2007) and Hanson et al. (2006) came to the conclusion that manipulation affects information aggregation, while not reducing the predictive accuracy of the forecasts. Hanson and Oprea (2009) even highlight the liquidity-providing effect of manipulation. However, Deck et al. (2013) showed in a similar setting as Oprea et al. (2007) that, indeed, manipulators that are highly incited for inaccurate predictions, can diminish the predictive power of the markets down to a level that is no better than random guessing – provided that inexperienced traders exist in the market.

Recent studies on manipulation in prediction markets focus on markets featuring a market scoring rule. In this context Buckley and O'Brien (2015) conclude in line with literature in traditional market settings: manipulation has no lasting impact on market prices. However, Chen, Gao, Goldstein, and Kash (2015) demonstrated a successful manipulation in a market featuring a Logarithmic Market Scoring Rule (LMSR). Their setting included only two traders and an outside incentive for an erroneous price of the asset. In the context of horse racing, Brown and Yang (2017) realized manipulation using the anchoring effect in low liquidity markets.

Summing up, we conclude that prediction markets can be manipulated to (at least) some extent. This is also what anecdotal evidence taught us during the last decades. Rothschild and Sethi (2016) found suggestive evidence in the 2012 US presidential elections in favor of Romney on Intrade prediction market. A manipulator opened orders with a volume exceeding the rest of the order book on the election day. Luskin (2004) reports a similar case in the 2004 US Presidential elections in favor of Kerry.

A manipulator spent $20.000 on TradeSports prediction market to manipulate the odd, knowing that the market has a huge impact on the public opinion. Hardford (2007) and Wolfers (2007) report a case in the same year in favor of Clinton. The last case was such a controversial one, that Koleman Strumpf, a well-known researcher on prediction markets, was not even sure, if there was really manipulation (Newman, 2010, Wolfers, 2007).

2.2 Fraud in Prediction Markets

Most of the literature on manipulation in prediction markets considers traders playing according to the rules (Blume et al., 2010). Participants, however, that are incited to manipulate may not only stick to the rules, but create other ideas how to cheat the market. Among others, fraud in prediction markets is discussed in Schröder (2009) and Blume et al. (2010). Fraud – playing against the rules – can have manifold forms. Two examples are "insider trading" or forming coalitions. First may occur in all prediction markets, second probably only in play-money prediction markets. The reason here is that play-money prediction markets do usually not require an initial personal investment. If one account suffers for the benefit of another does actually not "hurt" the first account holder. There are some reported cases of fraud in academic literature.

Hansen et al. (2004) reports of a case of fraud in prediction markets, which happened during the federal state election of Berlin in 1999. Two prediction markets run parallel, both showed a significant overpricing of the FDP, a liberal party usually around 5%. Later investigation uncovered an email form the FDP headquarters asking the members to trade on the platforms, as *"[m]any citizens do not think of the PSM as a game, but consider it a result of opinion polls"* (Hansen et al., 2004, p. 5).

Blume et al. (2010) and Schröder (2009) report of fraud in the STOCCER sports prediction market, using a data set of the FIFA world cup 2006. In contrast to the first example, the fraud did not happen in favor of a specific team but only to enrich the fraudster. This happened to an extent that other traders recognized unusual behavior and complained at the administrator. Solely the hints by the community lead to the identification of 36 fraudulent accounts. These accounts belonged to coalitions or a single person using diverse mechanisms to transfer money to selected accounts, which therefore improved in the list of top-scorer.

Bohm and Sonnegard (1999) observed fraud in a side competition of a PSM in the context of a referendum: The Swedish referendum about joining the European Union. The research project actually compared the prediction quality of a PSM to polls and whether polls induce market activity. The side competition offered the participation fee of all participants to the trader with the best performance. This should not influence market accuracy as long as there are no coalitions built. However, coalitions were formed that no longer pursued the goal to strike the most accurate probability, but transfer money between the accounts, not caring what happened to the market price. Though the regular market is strong, it was possible to distort the prices, at least for some short period.

2.2.1 Why and where Fraud in Prediction Markets occurs

To uncover manipulative behavior and fraud, it is important to understand, what and how fraudsters think. Wolfe and Hermanson (2004) describe a fraudsters thought process in the "fraud diamond", which is an extension of the "fraud triangle" (Cressey, 1953, Lou & Wang, 2011). The fraud diamond states four conditions for fraud to occur: the right person (1. capability) must realize an opportunity (2. weakness in the system) and be planning to do so (3. want to or have to commit); finally this person has to be convinced (4. rationalization) that it is worth the risk. In a prediction market, a willing person's intention can be described in three dimensions: (i) Desire/objective (whether to disrupt the market or to enrich itself), (ii) temporal horizon (immediately or in the long-run), and (iii) source of incentive (the issuing incentive is caused by an inner incentive scheme outside the market). In the following we want to focus on these three dimensions organized in the Fraud Cube (see Figure 1).

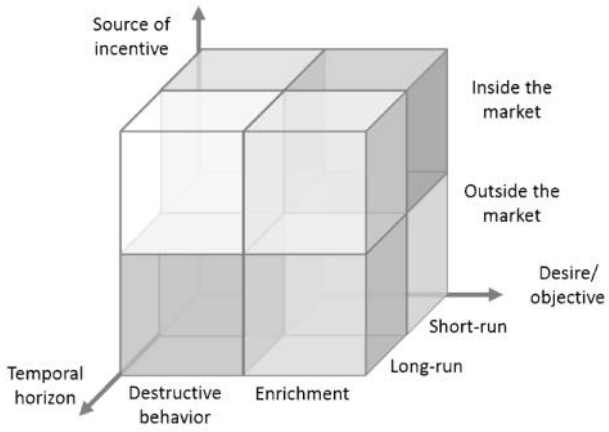

Figure 1. The Fraud Cube: Framework to understand and uncover where a prediction market may be manipulated or cheated.

The desire of a fraudster can be (self-) enrichment, destructive behavior, or both. In the first case, the traders want to improve their own results (Bohm and Sonnegard, 1999) and realizes, that it is possible by playing against the rules. In the second case, the desire is to destroy the prediction, which can have different sources of motivation. At the on hand, according to Brüggelambert (1999), destructive participants take a delight in nonsensical decisions or are glad about sabotaging. At the other hand, they may have incentives for bad predictions. Such incentives may not only be monetary and may lay outside the market, such as in the Berlin election 1999 example mentioned earlier.

The temporal horizon of fraudulent behavior can be short- or long-run. Short-run attacking usually intends to realize quick profits or to destroy market prediction for only a short period of time. There is no distinct threshold which time period is needed to be considered short- or long-run. Long-run fraudulent behavior takes a greater interest in the outcome of the event. They want to either manipulate the outcome or the information (and decisions) that are derived from the market prediction.

Finally, fraudsters with the incentive to cheat and manipulate may have two manifestations: It may come from inside or outside the markets. The examples mentioned earlier show both cases: While the manipulation of the election forecasts have been incited from the outside, the fraud that occurred in the world cup example was incited from the incentive scheme of the market itself.

At this point we want to mention that it is of great importance, thinking trough the parts of the cube, to consider both: attacks from the inside (trading) or outside (manipulate the information or outcome).

The DARPA Policy Analysis Market provides a good example, how to elaborate risks of fraud and manipulation in prediction markets, which is reported by Hanson (2006b, 2006a). The market was discussed on July 2003, but quickly dropped for the reason of unpredictable risks. The project intended to forecast assassinations and terror strikes. Comprehensibly, such a market has, besides of the regular inside incentive to perform well, strong outside incentives to be manipulated. Moving through the fraud cube we can identify several attacking points: The attack vector [Enrichment & Long-run & Outside], e.g., may motivate a company/organization selling products for security or earning money with the fear of an attack to write threatening letters to the government that a terror strike will occur soon (Hanson, 2006a). [Enrichment & Long-run & Inside], even worse, may incite to conduct terrorist attacks to make the "prediction" come true. [Destruction & Long-run & Outside] may encourage, e.g., people to artificially trade prices down as a preparation for a terror strike. Hanson (2006b) states that attacks from outside are easily forgotten when thinking about threats to the sustainable and correct operation of the market. However, due to the manifold expressions of attacking points and the fact that they are often not under the reach of a market engineer, it is hard to protect against them (Hanson, 2006b). Incentives may play a key role (Schröder, 2009).

2.2.2 How Fraud in Prediction Markets occurs

To classify the attacks and manipulation strategies in more detail, we use categories from Allen and Gale (1992) which originated in stock markets: (i) Action-based manipulation, (ii) information-based manipulation, and (iii) trade-based manipulation.

Action-based manipulation and information-based manipulation are not always easy to differentiate. In general, action-based manipulation is a manipulation of the value of the contract. Allen and Gale (1992) are drawing near the example of the American Steel and Wire Company from 1901. The managers of the company shortened their stock positions and then closed the steel mills. The price fall from $60 to $40. The managers covered their short positions and reopened the mills, which lead to a price rise and to a large profit of the managers. Bagnoli and Lipman (1996) developed another model of action-based manipulations. Here a participant in the market pools with an external partner who is giving a takeover bid for the company the manipulator is holding stocks. After the manipulator has realized his profits, the partner unwinds his takeover bid. A similar model was presented by Vila (1989) besides that the roles are switched, so that the initiator is the giver of the takeover bid. Prediction markets are a common instrument to predict project milestones or product releases. Hanson (2006b) states here the problematic that employees, trading on the market, may take influence on the outcome. Ottaviani and Sørensen (2007) showed in an experiment that employees had indeed taken the opportunity, if given so, to manipulate the outcome in such a context. Chakraborty and Das (2016) investigate this problem from a Game-theoretic perspective and conclude also that the opportunity lead to manipulation or fraud.

Information-based manipulation is related to the spreading of false information or deceptive rumors. Exemplarily for this kind of manipulation are the “trading pools” that emerged in 1920 in the US, the Enron, and the WorldCom frauds in 2001 (Unerman & O’Dwyer, 2004). According to Benabou and Laroque (1992) an opportunistic trader with privileged information could profitably manipulate markets by making misleading announcements in case he is believed to be credible by other investors. Recently, Casas, Fawaz, and Trindade (2016) demonstrated this effect in prediction markets in the con text of elections.

Trade-based manipulation is manipulation playing within the rules. This is especially researched in stock markets (Allen & Gale, 1992). The basic consent is that trade-based manipulation is possible given some preconditions (usually true in prediction markets: low liquidity, nonlinear demand functions). However, profits are low and if such behavior in play-money prediction markets lead to higher engagement we do not consider it as fraudulent behavior.

In the context of play-money prediction markets, these three types of manipulation and fraud have to be extended by one more type: (iv) Multiple accounts and coalitions. Blume et al. (2010) and Blume (2012) presented several strategies that are used by participants which have created multiple (or hacked) accounts. This is usually done to trade between the accounts and transfer money from one to the other (Schröder, 2009). Similar problems can arise if participants start to form coalitions. This may be the case if participants are incited by prices for the top ranks. If coalitions can somehow share the price, they are able to increase the probability over the average level of winning the price, if they transfer money (or stocks) to one account. This is possible, if the spread is greater or equal to 0.03 Virtual Currency Units (VCU). This strategy to transfer money is called “ping-pong” or circular trading, which is also described in Hansen et al. (2004) and even in real stock markets (Reuters, 2010). The strategy is more successful, the higher the spread is, so sometimes the spread is aggressively widened before the circle trading (Blume et al., 2010).

2.3 Fraud Detection and Trading Patterns

Fraud detection means to identify suspicious fraudulent transfers, orders and other illegal activities (Ferdousi & Maeda, 2006). In literature we find two popular approaches of fraud detection in (prediction) markets: (a) Detection of Strategies and (b) Peer Group Analysis (PGA).

The detection of fraudulent strategies in trading patterns is among others investigated by Blume et al. (2010). The first is the "ping-pong indicator", which characteristic feature is the transfer of money. The second is the "prominent-edge indicator", which key feature is the transfer of stocks. To elicit these two strategies on data, Blume et al. (2010) created graphs with nodes representing participants and directed edges representing transactions. Afterwards a heuristic detected suspicious patterns and an indicator test was used to prove if the patterns are recognizable manipulation strategies.

The ping-pong trading heuristic was able to detect cycles in the graph. The algorithm holds a trading history on every possible cycle and updated it after every transaction. Afterwards, the algorithm calculated average prices for all transactions on an edge within a certain time span and compared it to the related edges (same nodes, other direction). If the time in between the last transaction of the two edges was below a certain limit and the average price for the sell transaction was lower than of the previous buy transaction for one participant, the case was reported to the market operator. Hence, the heuristic was able to detect obvious losing deals of one account within a short time period. Blume et al. (2010) was able to detect 33 cases in his data set, whereas three were false positives. However, Blume et al. (2010) noted that it is hard to develop strategies without false positives and that he also has no benchmark how many unreported fraudulent traders remained in the data set.

Blume et al. (2010) also developed a heuristic for the prominent-edge indicator. Here a supporting account buys stocks from the market for the given price and then sells it to the supported account for a low price. Therefore, the heuristic of Blume et al. (2010) searched for nodes where one edge had a significantly higher volume. However, this embodies two problems: First, the calculation has to be relative to the financial means of every account. Second, as in Blume et al. (2010)'s data the endowment for each stock was different, a threshold for "significance" had to be defined. It is remarked, that both fraud strategies get less applicable if the liquidity is very high.

Stock exchanges use machine learning approaches and expert systems for fraud detection (Bolton & Hand, 2002). PGA is an unsupervised method for stock markets and not yet used in prediction markets. Its objective is to characterize participants by expected patterns of behavior around the target sequence by monitoring the behavior of similar objects and subsequently to detect any differences between the expected pattern and the target (Kim & Sohn, 2012). Such methods are not in need of prior knowledge and detect changes in behavior or unusual transactions (Ferdousi & Maeda, 2006). In contrast to supervised methods it is possible that previously undiscovered types may be detected. The basic proceeding can be explained in two steps: First, peer groups are built. Such peer groups can be created by comparing all targets (participants) according to internal or external criteria based on summarized data of earlier behavior of each target (Ferdousi & Maeda, 2006). In a second step, the summaries are subsequently updated and all objects are compared to the group. If one target exhibits different behavior from the peer group behavior, it is flagged as meriting closer investigation. Ferdousi and Maeda (2006) are recommending to take known patterns into consideration, such as seller are more likely to be involved in fraud (especially with high variance in their trades). The adaptability of PGA for prediction markets is not yet investigated. Though it is a promising approach, as it does not rely on thresholds and parametrization, problems may occur due to the (relatively) small number of participants in prediction markets. In addition, when a trader has to be locked, it may be not only of interest that the trader cheated, but how the trader cheated (Blume et al., 2010).

3 Rule-based Fraud Detection

In section 2.3 we explained fraud detection approaches. The fraud detection heuristics from, e.g., Blume et al. (2010), however, have some shortcomings. The heuristics only take the trading behavior into account. In prediction markets we usually do have more information on the participants that may help to detect fraud. In addition the heuristics of Blume et al. (2010) are quite complex and therefore less applicable, as is it represents the markets in the form of graphs. In the following we want to introduce a rule-based algorithm for fraud detection in play-money prediction market that is capable to combine the idea behind the indicators of Blume et al. (2010) and other criteria e.g. based on the par-

ticipants attributes. Traders receive "suspicious points" for conspicuous features. We test the algorithm post-hoc on a data-set collected by the prediction market "Kurspiloten" that ran in 2011. This was a collaborative project of the "Handelsblatt" (a large German-based newspaper), the IISM at the Karlsruhe Institute of Technology, and the IW Köln. During a data collection period of 12 weeks, participants traded twelve financial indicators. 2,111 participants conducted 112,386 transactions. Participants received an initial amount of play-money and stocks for each asset. The assets were paid out weekly. At the end of the running period, the best ranked trader won a luxury watch, worth €50,000. The market operators put information sources at disposal. Thus, participants were able to conceive an opinion, whether the price came up to their expectations and to acquire information on all financial indicators. The outcomes of the market were not used nor there was another similar market, so we had no conflicting incentives. Hence, our detection heuristic focuses on the detection of manipulative behavior driven by enrichment.

3.1 Algorithm

Our algorithm is based on the idea of Blume et al. (2010), however, does not use graphs, but a simple scoring system where traders receive "suspicious points" for each indicator test in the heuristic that evaluates to true. As a result of the heuristic we receive a ranking of suspect traders, accompanied by its "suspicious score", whereas we claim that the top ranks have the highest probability to be a fraudster. As recommended by Ferdousi and Maeda (2006) we concentrated on the sales of participants. The algorithm is basically built upon four indicator tests. In step one all participants are checked whether they sold to the same person extensively. First, we only considered participants who sold more than twice to the same person. For each of these relationships we checked, if the traded amount is significant for the participant (>10%). However, this parameter should be considered carefully. A low threshold rises the sensitivity, but lowers the precision of the indicator test. If the test returns true, both seller and buyer received a suspicious point and are listed as suspects. Thereafter, in step two of the algorithm, we checked suspicious traders, whether there were differences between the exchange rates in the trades between the suspicious accounts. Accounts receive a suspicious point if rates differ by 5%. This threshold should be adapted regarding the liquidity. If liquidity is high and spread is low, it is possible to decrease this threshold. In a third step the heuristic tested if the trades between suspicious accounts were conducted in a short period, in fact 15 minutes. If this test evaluates to true, both accounts received two suspicious points. In a last step we compared the personal data of the accounts - in our case we chose the password (hash) and the street. If the password was similar, both accounts received 4 suspicious points, another 4 for similar streets. We use this as an example, as we found, that 236 street names appeared more than once. In other prediction markets, it may also be worth to get an impression of the nature of the data and create another step in such an algorithm. Finally 484 suspects were found. Six traders had more than 200 suspicious points, the highest score was 551 points.

3.2 Evaluation

To evaluate the heuristic we looked at the trading behavior and the account data manually more in detail. We also compared the personal data of suspects to get an insight how precise the heuristic was. The first ranked trader only traded to six partners, whereas two of them ranked on place six and seven. All of them lived in the same city, the zip code was equal, two street names were equal and the surnames were equal. All accounts had been created within two days. The forth trading partner traded 169 times, 128 times with the highest ranked trader, 16 times with the other two. It is very likely that all four accounts belong to the same person. A comparable picture draws for the second placed. He traded with only four partners, all listed in the ranking, two of them in the top 20. Two of the partner traded exclusively with the second placed, all four at least 55% of their overall trading volume. Three of the four "partnering accounts" were created within four hours and the zip code was resembling. All accounts were registered at the same mail provider. Almost all transactions took place within 48 hours.

We also claim these five accounts to belong to the same person. In the top ten of the detected suspects we can relatively sure say, that we detected nine manipulative accounts belonging to six fraudsters.

To evaluate our algorithm further, we compared our performance to the heuristics and indicators from Blume et al. (2010). In fact, these are the "ping-pong" and the "prominent-edge" indicator. In Blume et al. (2010) different parametrization is tested; we used the parametrization that was finally suggested: time span of 60min and number of repetitions of ≥ 5 for the „ping-pong indicator", and Gini coefficient of ≥ 0.75 and no time span for the „prominent-edge indicator". Blume et al. (2010) did not report if these values were summed over all products, so we assumed this to be true. Another problem is that Blume et al. (2010) do also not report how and based on which criteria suspicious cases could be validated as fraudsters (if they did not admit). We end up with 192 suspects. 54 of them were not listed in the list of suspicious accounts of our algorithm. However, 346 traders found suspicious by our algorithm were not in the list of the suspicious accounts produced by the heuristic of Blume et al. (2010). Hence, we conclude that our algorithm is, in regard to finding suspicious accounts, at least as well as state of the art heuristics. Further comparisons of performance and quality are very hard, as there is no "ground truth" to which to compare (Blume et al., 2010). Another approach would be to set up a laboratory experiment and control for "who" is a fraudster, but this approach obviously would lack of diversity and creativity of fraudsters in real prediction markets.

Without doubt, there are several issues which can be enhanced in the heuristic. However, our aim was to create a heuristic, which is easily applicable for practitioners. In retrospective, we can conclude on the heuristic, that it detected several fraudulent accounts with a relatively high precision. The list of suspects can serve as a shortlist of accounts which require deeper attention. The "difference in exchange rate" step did not distribute a lot of suspicious points, which was surprising as it is a key strategy of manipulators. We would not recommend skipping this step, but have a closer look on the performance of the asset and calibrate the threshold accordingly. The personal data was one of the strongest indicators as the fraudsters obviously did not put much effort in varying their personal data. One may prevent the creation of such fraudulent accounts during registration. However, if it is not prevented, the "lack of creativity" of fraudsters can be successfully used as a "trap"; at least in the context of play-money prediction markets. The "trading period" step distributed a lot of points also to probably rightful traders. We assume that the trading period of 15 minutes may be adjusted to a smaller value.

4 Conclusion

The work at hand contributed in several ways, especially to practitioners who face the task of designing or protecting a prediction market. By introducing the Fraud Cube we provide an encompassing framework to uncover potential attacking points in prediction markets and help market engineers to take the stand of fraudsters and comprehend their thoughts. Empathizing with the manipulator is an important step to get a better understanding of manipulation. Second, we explained some of the most prevalent attacking strategies which can be found in prediction market literature and related fields. The experiences of others, which were outlined anecdotal, can help to get an impression of the threats and strategies that are prevalent. Finally, we introduced an algorithm to spot fraud in prediction markets, which is capable to create a valid list of suspects and does not rely on complicated methods. In addition, its rule-based character makes it easily applicable for practitioners. A limitation of our approach is, that only known attacking patters can be detected, while more creative attacks may still be conducted. This has to be addressed in future research. In addition, it has to be noted, that research on social networks also deals with the possibility of "Sybil attacks". Findings in this stream may be evaluated in context of prediction markets in future work as well. Next steps will be to implement this algorithm in a prediction market in cooperation with the "Frankfurter Allgemeine Zeitung", a large German-based newspaper and online magazine, http://orakel.faz.net, and to understand more what drives manipulative behavior. The question how fraudsters react to early warnings is also still open and subject to further research. Using prediction markets for corporate decision making or in politics is an emerging field (Klein & Garcia, 2015) and, hence, should be accompanied by research on fraud.

References

Allen, F., & Gale, D. (1992). Stock-price manipulation. *Review of Financial Studies*, *5*(3), 503–529.

Bagnoli, M., & Lipman, B. L. (1996). Stock price manipulation through takeover bids. *The RAND Journal of Economics*, 124–147.

Benabou, R., & Laroque, G. (1992). Using privileged information to manipulate markets: Insiders, gurus, and credibility. *The Quarterly Journal of Economics*, 921–958.

Berg, H., & Proebsting, T. A. (2009). Hanson's Automated Market Maker. *Journal of Prediction Markets*, *3*(1), 45–59.

Berg, J. E., Forsythe, R., & Rietz, T. A. (1997). What makes markets predict well? Evidence from the Iowa Electronic Markets. In *Understanding Strategic Interaction* (pp. 444–463). Springer.

Blume, M. (2012). *Behavior identification in markets using visualization and network analysis*. Karlsruhe Institute of Technology. Retrieved from http://digbib.ubka.uni-karlsruhe.de/volltexte/1000026214

Blume, M., Luckner, S., & Weinhardt, C. (2010). Fraud detection in play-money prediction markets. *Information Systems and E-Business Management*, *8*(4), 395–413.

Bohm, P., & Sonnegard, J. (1999). Political stock markets and unreliable polls. *The Scandinavian Journal of Economics*, *101*(2), 205–222.

Bolton, R. J., & Hand, D. J. (2002). Statistical Fraud Detection: A Review. *Statistical Science*, *17*(3), 235–249. Retrieved from http://www.jstor.org/stable/3182781

Brown, A., & Yang, F. (2017). *Anchoring in Speculative Markets: A Field Experiment*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2898142

Brüggelambert, G. (1999). *Institutionen als Informationsträger: Erfahrungen mit Wahlbörsen*. Metropolis-Verl., Marburg. Retrieved from https://www.econbiz.de/Record/institutionen-als-informationsträger-erfahrungen-mit-wahlbörsen-brüggelambert-gregor/10001350839

Buckley, P. (2016). Harnessing the wisdom of crowds: Decision spaces for prediction markets. *Business Horizons*, *59*(1), 85–94. http://doi.org/http://dx.doi.org/10.1016/j.bushor.2015.09.003

Buckley, P., & O'Brien, F. (2015). The effect of malicious manipulations on prediction market accuracy. *Information Systems Frontiers*, 1–13. http://doi.org/10.1007/s10796-015-9617-7

Camerer, C. F. (1998). Can Asset Markets Be Manipulated? A Field Experiment with Racetrack Betting. *Journal of Political Economy*, *106*(3), 457–482. http://doi.org/10.1086/250018

Casas, A., Fawaz, Y., & Trindade, A. (2016). Surprise Me If You Can: The Influence of Newspaper Endorsements in U.S. Presidential Elections. *Economic Inquiry*, *54*(3), 1484–1498. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2777778

Chakraborty, M., & Das, S. (2016). Trading on a rigged game: outcome manipulation in prediction markets. *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence*, 158–164. Retrieved from http://dl.acm.org/citation.cfm?id=3060644

Chen, Y., Gao, X. A., Goldstein, R., & Kash, I. A. (2015). Market Manipulation with Outside Incentives. *Autonomous Agents and Multi-Agent Systems*, *29*(2), 230–265. http://doi.org/10.1007/s10458-014-9249-1

Cowgill, B., Wolfers, J., & Zitzewitz, E. (2009). Using Prediction Markets to Track Information Flows: Evidence from Google BT - Auctions, Market Mechanisms and Their Applications: First International ICST Conference, AMMA 2009, Boston, MA, USA, May 8-9, 2009, Revised Selected Papers. In S. Das, M. Ostrovsky, D. Pennock, & B. Szymanksi (Eds.), (p. 3). Berlin, Heidelberg: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-642-03821-1_2

Cressey, D. R. (1953). *Other people's money; a study of the social psychology of embezzlement*. Free press. Retrieved from https://books.google.de/books/about/Other_People_s_Money.html?id=FgAFAAAAMAAJ&redir_esc=y

Deck, C., Lin, S., & Porter, D. (2013). Affecting policy by manipulating prediction markets: Experimental evidence. *Journal of Economic Behavior & Organization*, *85*, 48–62.

Ferdousi, Z., & Maeda, A. (2006). Unsupervised Outlier Detection in Time Series Data. *22nd International Conference on Data Engineering Workshops (ICDEW'06)*. http://doi.org/10.1109/ICDEW.2006.157

Hansen, J., Schmidt, C., & Strobel, M. (2004). Manipulation in political stock markets: preconditions and evidence. *Applied Economics Letters*, *11*(7), 459–463.

Hanson, R. (2006). Foul play in information markets. In *Information markets: A new Way of Making Decisions* (pp. 126–141). AEI Press.

Hanson, R. (2006). Designing real terrorism futures. *Public Choice*, *128*(1), 257–274. http://doi.org/10.1007/s11127-006-9053-9

Hanson, R., & Oprea, R. (2009). A Manipulator Can Aid Prediction Market Accuracy. *Economica*, *76*(302), 304–314. http://doi.org/10.1111/j.1468-0335.2008.00734.x

Hanson, R., Oprea, R., & Porter, D. (2006). Information aggregation and manipulation in an experimental market. *Journal of Economic Behavior & Organization*, *60*(4), 449–459.

Hardford, T. (2007). Undercover Economist: Tote that vote. Retrieved April 6, 2017, from https://www.ft.com/content/242d5378-22c4-11dc-ac53-000b5df10621

Jian, L., & Sami, R. (2012). Aggregation and Manipulation in Prediction Markets: Effects of Trading Mechanism and Information Distribution. *Management Science*, *58*(1), 123–140.

Kim, Y., & Sohn, S. Y. (2012). Stock fraud detection using peer group analysis. *Expert Systems with Applications*, *39*(10), 8986–8992. http://doi.org/10.1016/j.eswa.2012.02.025

Klein, M., & Garcia, A. C. B. (2015). High-speed idea filtering with the bag of lemons. *Decision Support Systems*, *78*, 39–50. http://doi.org/http://dx.doi.org/10.1016/j.dss.2015.06.005

Laskey, K. B., Hanson, R. D., & Twardy, C. (2015). Combinatorial prediction markets for fusing information from distributed experts and models. In *Information Fusion (Fusion), 2015 18th International Conference on* (pp. 1892–1898).

Lou, Y., & Wang, M. (2011). Fraud Risk Factor of the Fraud Triangle Assessing the Likelihood of Fraudulent Financial Reporting. *Journal of Business & Economics Research (JBER)*, *7*(2). http://doi.org/10.19030/jber.v7i2.2262

Luckner, S., Kratzer, F., & Weinhardt, C. (2005). STOCCER-A Forecasting Market for the FIFA World Cup 2006. In *4th Workshop on e-Business (WeB 2005), Las Vegas, USA*.

Luckner, S., & Weinhardt, C. (2007). How to Pay Traders in Information Markets: Results from a Field Experiment. *Journal of Prediction Markets*, *1*(2), 147–156. Retrieved from http://econpapers.repec.org/RePEc:buc:jpredm:v:1:y:2007:i:2:p:147-156

Luskin, D. L. (2004). Who'S Behind The Bush-Futures Attacks? Retrieved April 6, 2017, from http://www.nationalreview.com/article/212580/whos-behind-bush-futures-attacks-donald-l-luskin

Mangold, B., Dooley, M., Flake, G. W., Hoffman, H., Kasturi, T., Pennock, D. M., & Dornfest, R. (2005). The Tech Buzz Game: stock market prediction. *Computer*, *38*(7), 94–97. http://doi.org/10.1109/MC.2005.243

Newman, A. L. (2010). Manipulation in Political Prediction Markets. *Journal of Business, Entrepreneurship & the Law*, *3*(2), 205–235. Retrieved from http://digitalcommons.pepperdine.edu/jbel/vol3/iss2/1/

Oprea, R., Porter, D., Hibbert, C., Hanson, R., & Tila, D. (2007). *Can Manipulators Mislead Prediction Market Observers*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.215.148&rep=rep1&type=pdf

Ottaviani, M., & Sørensen, P. N. (2007). Outcome manipulation in corporate prediction markets. *Journal of the European Economic Association*, *5*(2 3), 554–563.

Reuters, E. (2010). Hong Kong warrants traders guilty of market manipulation: SFC. Retrieved April 6, 2017, from http://www.reuters.com/article/us-hongkong-sfc-idUSTRE6462GN20100507

Rhode, P., & Strumpf, K. (2006). *Manipulating political stock markets: A field experiment and a century of observational data*. Retrieved from https://ideas.repec.org/p/feb/natura/00325.html

Rothschild, D. M., & Sethi, R. (2016). Trading Strategies and Market Microstructure: Evidence from a Prediction Market. *Journal of Prediction Markets*, *10*(1), 1–29. Retrieved from http://www.redi-bw.de/db/ebsco.php/search.ebscohost.com/login.aspx%3Fdirect%3Dtrue%26db%3Dbuh%26AN%3D118713442%26site%3Deds-live

Schröder, J. (2009). *Manipulations in prediction markets: analysis of trading behaviour not conforming with trading regulations*. KIT Scientific Publishing.

Servan-Schreiber, E., Wolfers, J., Pennock, D. M., & Galebach, B. (2004). Prediction Markets: Does Money Matter? *Electronic Markets*, *14*(3), 243–251. http://doi.org/10.1080/1019678042000245254

Teschner, F., Stathel, S., & Weinhardt, C. (2011). A prediction market for macro-economic variables. In *Proceedings of the Annual Hawaii International Conference on System Sciences* (pp. 1–9). http://doi.org/10.1109/HICSS.2011.23

Unerman, J., & O'Dwyer, B. (2004). Enron, WorldCom, Andersen et al.: a challenge to modernity. *Critical Perspectives on Accounting*, *15*(6–7), 971–993. http://doi.org/http://dx.doi.org/10.1016/j.cpa.2003.04.002

Vila, J.-L. (1989). Simple games of market manipulation. *Economics Letters*, *29*(1), 21–26.

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, *74*(12), 38.

Wolfers, J. (2007). Is there manipulation in the Hillary Clinton prediction market? Retrieved April 6, 2017, from http://www.overcomingbias.com/?s=manipulation+prediction+market

Wolfers, J., & Leigh, A. (2002). Three Tools for Forecasting Federal Elections: Lessons from 2001. *Australian Journal of Political Science*, *37*(2), 223–240. http://doi.org/10.1080/10361140220148115

Wolfers, J., & Zitzewitz, E. (2004). Prediction Markets. *Journal of Economic Perspectives*, *18*(2), 107–126. http://doi.org/10.3386/w10504

Wolfers, J., & Zitzewitz, E. (2006). *Five Open Questions About Prediction Markets* (Working Paper Series). Retrieved from http://www.nber.org/papers/w12060