SCALABILITY & BUSINESS OUTCOMES:

ESSAYS ON MANAGING TRADE-OFFS WHEN FRINGE TECHNOLOGIES GO MAINSTREAM

A Dissertation

Submitted to the Faculty

of

Purdue University

by

Abhishek Ray

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

December 2019

Purdue University

West Lafayette, Indiana

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF DISSERTATION APPROVAL

Dr. Karthik Kannan, Chair

Krannert School of Management

Dr. Hossein Ghasemkhani, Chair

Krannert School of Management

Dr. Mario Ventresca

School of Industrial Engineering

Dr. Thanh Nguyen

Krannert School of Management

Approved by:

Dr. Yanjun Li

Krannert School of Management

To my son Ishaan & my wife Pallavi, for shining a light through dark times.

ACKNOWLEDGMENTS

First, I would want to thank my advisors, Professor Karthik Kannan and Professor Hossein Ghasemkhani for their timely support and thoughtful guidance throughout my Ph.D. Their mentorship and support has helped me shape this dissertation and research outcomes therein.

Additionally, I would like to thank Professor Mario Ventresca, Professor Thanh Nguyen, Professor Shai Vardi and Professor Christopher Quinn for their considerate feedback, advice and suggestions during the phases of the thesis and the job market. I would also like to express my gratitude to Professor Kemal Altinkemer, Professor Prabuddha De, Professor Alok Chaturvedi, Professor Mohammad Rahman and Professor Zaiyan Wei for their thought-provoking PhD seminars. Such workshops helped me to formulate my own research questions.

I would also like to thank the senior graduates of the Krannert MIS Ph.D. program, Fisher Wu, Na Zhang and Warut Khern-am-Nuai; my amazing friends, Mohammed Alyakoob, Anaparasan Mahalingam, Yipu Deng, Viplove Arora, Bryan Chong, Oscar Rincon and Vandith Pamuru Subramanya Rama, for their friendship and support throughout this cycle.

Ultimately, I can't give my parents and wife enough thanks for their help, support and love. I'm blessed with an amazing family. It would be difficult to obtain a Ph.D. without you all.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

ABSTRACT

Ray, Abhishek Ph.D., Purdue University, December 2019. Scalability & Business Outcomes: Essays on Managing Trade-Offs when Fringe Technologies go Mainstream. Major Professors: Karthik Kannan, Hossein Ghasemkhani.

This dissertation consists of three essays that study problems that decision-makers face when hitherto niche technologies scale up. Typically, scaling up involves market expansion with participation from a variety of agents with complex preferences, using the technology to maximize their utility. A major problem for the decision maker then is either one or a combination of the following: deciding policy for optimal business or social outcomes, implementing efficient demand allocation mechanisms or improving market design.

The first essay studies policy implications in the context of burgeoning ad-blocking technology. This research problem is important since increased usage of ad-blockers has caused an estimated loss of $21.8 billion in global ad revenues since 2015 and is projected cause $35 billion loss by 2020. The objective of this research is to inform industry and policy-makers on the following questions: (1) what should be the dominant business model of ad-blocking? (2) what are the implications when no such dominant model exists and ad-blockers compete? We consider answering these questions from perspective of three agents: users, a content provider and an ad-blocker. For the first question, we model a monopoly with one ad-blocker and a content provider serving a mass 1 of users. Our model shows under appropriate assumptions, users have a clear preference ordering wherein freemium is the most and paid is the least preferred business model. However content providers and ad-blockers have conflicting preferences on business models, largely dependent on trade-off between advertising revenue and charging users for blocking ads. Further, competition among ad-blockers with same or different business models makes users worse-off and ad-blockers better off, in every case. More generally, from an outcome perspective, our analysis shows that it is impossible to have a dominant ad-blocking business model that satisfies both users, content providers and ad-blockers.

The second essay studies optimizing allocations in the context of the growing application of iterative combinatorial auctions in industry. Combinatorial auctions (CA) are increasingly being used to allocate bundles of items among interested bidders. However, with CA being conducted iteratively to ease preference elicitation problems, the volume, variety and velocity of bundles and bids has become complex. It therefore takes exponentially longer to solve for winners in such auctions. As expected, regular solvers such as IBM CPLEX or AMPL have been demonstrably ineffective. We propose an Ant Colony-based algorithm (TrACA) that produces optimal or near-optimal results within specified time. Experiments are performed on 94 instances to show and compare the performance of TrACA to the current state-of-the-art memetic algorithm (MA) & ant colony based heuristic (ACLS) and a recent exact algorithm. Results indicate that in a given run-time of maximum 10 minutes, the median of results from TrACA statistically significantly outperforms MA results in 87% & ACLS 47% of the cases. Further, in the same time, the best value from TrACA is at least as good as MA & ACLS values in 100% of the cases. Further, TrACA achieves the optimal in 74 out of 94 cases in ${\frac{1}{6}}^{\text{th}}$ of the time taken by an exact algorithm. Additionally, empirical hardness of tested instances is analyzed using a standard supervised learning method to better understand variable run-times and to build a predictive model of TrACA run-times. Using the predictive model, we highlight factors that make winner determination in combinatorial auctions computationally hard to estimate and show why TrACA is better suited to handle such hard instances when resolving trade-off between speed and accuracy.

The third essay, which is in early stages, explores the problem market design that tackles centralization of mining power in cryptocurrencies. Our analysis looks at designing a mechanism that tackles the core issue of mining power centralization: selfish mining problem in cryptocurrencies. Specifically, we address the problem of designing incentive compatible consensus mechanism for cryptocurrencies. Taking Bitcoin as the context for our methodology We use automated mechanism design (AMD) and a supervised learning algorithm to discover the relationship between optimal payoffs and miner actions that incentivize honest behavior. Using notions from the discovered relationship, we further generalize the approach and establish three new incentive schemes make honest mining dominant and incentive compatible.

1. INTRODUCTION

Technology is constantly evolving to allow businesses to discover markets, prices and deliver value. Delivering value typically requires technologies to function at scale. Although functioning at scale implies improvements in value delivered, demand volume & variety with participation of strategic end-users has given rise to inevitable problems. Majority of these problems can be broadly classified into three categories: determining optimal economic policies, computing efficient allocations and designing better market mechanisms. In this dissertation, I tackle a problem from each such category, in the context of a recent technology that is dealing with either increased market size or increased strategic end-user participation or both.

In the first essay, we study the case of the ad-blocking technology. The rise of ad-blockers as platforms delivering free, paid or freemium blocking services has prompted discussions on whether ad-blockers are good for the online ecosystem (Digiday, 2016; Foster, 2016; Vallade, 2008). With increasing competition for market share between ad-blockers (Mansfield-Devine, 2015; Vastel et al., 2018a), we answer two important questions: what should be the dominant business model of ad-blocking and what happens if there are no dominant models and ad-blockers compete. Specifically, using a game-theoretic model with notions from club theory we formulate monopoly and duopoly models to analyze welfare implications of different ad-blocker models. In doing so, we address concerns from policy-makers such as FTC, CEPR (Niemand et al., 2015), regarding the burgeoning ad-blocking industry and its impact on users and content providers. The main insights we derive from the model are related to impact on users and content providers due to ad-blocker business models (e.g., Freemium vs. Paid) and due to competition among ad-blockers for providing ad-blocking services to users. Our analysis shows impossibility in reconciling preferences in ad-blocking models among content providers and users and evidence of increasing price competition among ad-blockers that implies reduction in user surplus.

In the second essay, we study the problem of fast approximation of winner determination in iterative combinatorial auctions (CA) conducted on e-commerce exchanges. Winner Determination Problem (WDP) in CA is an NP-Complete problem (Sandholm and Suri, 2000; Sandholm et al., 2002)[1]. In the age of big data – increased velocity, volume and variety of bundles and bids – WDP is increasingly becoming intractable within limited time (Karaenke et al., 2015). In scenarios such as spectrum auction, the computational issues are not as problematic because they often involve only a few bidders. However, in cloud computing, transportation & logistics auctions conducted on e-commerce exchanges, there is a trend towards iterative combinatorial auctions to accommodate increase in market size, items and complex preferences of participants (Bichler, 2010; Bichler et al., 2006; Lau and Goh, 2002). Traditional solvers such as IBM CPLEX or AMPL have been ”demonstrably ineffective” (Adomavicius and Gupta, 2005) in producing the optimal solution when faced with big data scenarios in auctions (Boughaci et al., 2009; Lau and Goh, 2002). Instead, heuristic solutions are used (Bichler, 2010; Guo et al., 2006). We tackle this challenge by proposing a graphical formulation amenable to heuristic search. We use this formulation to design an ant-colony based heuristic capable of finding optimal or near optimal solutions in maximum 10 minutes and better than the best-in-class heuristic and as good in 78% of cases as the best exact algorithm. We show the effectiveness of our approach and establish reasons why large instances of CAs are becoming intractable using empirical hardness techniques.

In the third essay, we focus on designing better market mechanisms for preventing centralization of power in mining in cryptocurrencies. Selfish mining is the evidence of incentive *in*compatibility in cryptocurrency mining (Böhme et al., 2015; Eyal and Sirer, 2018; Ray et al., 2018b). Designing incentives is important because a prevalence in selfish mining can threaten the very nature of decentralized cryptocurrency

[1] It means that the difficulty in identifying the winner increases as the number of market participants and/or the set of items to bid on increases.

(Kroll et al., 2013; Ray et al., 2018b). Evidenced in recent developments, it has been observed that once a mining pool reaches a threshold of hash power, rational miners will preferentially join the mining pool to reap the higher revenues compared to mining alone (Eyal and Sirer, 2018; Sapirshtein et al., 2016). Such a mining pool can rapidly increase to majority hash power and threaten attacks such as DoS, DDoS or Goldfinger attacks (Babaioff et al., 2012; Böhme et al., 2015; Narayanan et al., 2016). Through mechanism design, we design better incentives for mining in cryptocurrencies. Specifically, we propose a new incentive system that rewards honest behavior and punishes dishonest behavior. From a policy perspective, mechanisms with rewards and punishments have been proven to be more effective in incentivizing desired behavior (Andreoni et al., 2003). Specifically, one might expect less cooperation in scenarios where good behavior is rewarded than in those where poor behavior is punished (Sutter et al., 2010). Designing a mechanism around rewards only and omitting an option for punishments may be a mistake, even if punishments are rarely used (Sefton et al., 2007). Better mechanisms for cryptocurrencies therefore rely on a balance of rewarding honest while punishing dishonest behavior(Casey and Vigna, 2018; Eyal and Sirer, 2018), all the while incentivizing participation in contributing to the system. Our designed mechanisms aims at maintaining this balance by introducing equity improving reward schemes.

The objective of this dissertation is to produce significant contribution to both academic research and industry practice. Our papers contribute to existing work in economics of information systems, club theory for digital goods, online advertising, meta-heuristics, combinatorial auction design, cryptocurrency economics and mechanism design. We also provide insights into the effectiveness of freemium models in the context of ad-blocker platforms, the economic value of ad-exchange models in ad-blocking and empirical hardness of time consuming combinatorial auctions. Moreover, we offer a formal analysis of the role of the incentive policies in cryptocurrencies – a recent but important industry initiative (Babaioff et al., 2012; Narayanan et al., 2016). These insights could help decision-makers in policy-making, business process improvements and market design.

2. THE ECONOMIC IMPLICATIONS OF AD-BLOCKERS

2.1 Introduction

Advertising is a primary source of revenue for digital media and, in some cases, it is in fact the *only* source. On the other hand, ad avoidance and, consequently, its revenue implications have become more significant in the digital realm. In the traditional media, access/content providers generally controlled the extent of ads visible to the consumers. On the Internet, however, the control primarily rests with the consumers – who have the option of using intrusion prevention tools such as ad-blockers and privacy-focused browsers. With increase in intrusive advertising practices, adoption and usage of intrusion prevention tools such as AdBlock-Plus, AdBlock, Brave etc. has increased dramatically. For instance, the number of people in US using ad-blockers grew by 45% between 2015 and 2018 (Shankland, 2018). Demographic findings show all generations, but especially millennials - 67% of them - have installed ad-blockers to combat loss of privacy and/or malware attacks (Karsenty, 2016; Wielki and Grabara, 2018). Desktops & laptops, with smartphones coming a close second, are the main venue for ad blocking. The proportion of desktop/laptop users who deploy ad-blockers is higher than smartphone users but the gap is closing steadily (Katona and Sarvary, 2018). These trends have important implications for digital media. It is estimated that, even with only 6% of the global Internet population using ad-blocking software in 2015, revenue loss for content providers was $21B or approximately 14% of the global ad spend (Walls et al., 2015). Further, with 11% of the global internet population using ad-blockers software by 2018 end (Brinkmann, 2017), projected annual loss in ad-revenues is approximately $35 billion by 2020.

In order to alleviate increasing revenue concerns of content providers (Digiday, 2016; Katona and Sarvary, 2018) and to keep pace with the increasing demand for ad-blocking (Karsenty, 2016), market for ad-blockers has evolved rapidly. While 2015 saw free ad-blockers such as AdBlock Plus hold the dominant market share (Shiller et al., 2017), introduction of whitelisted ads through ‘Acceptable Ads’ and ‘Coalition for Better Ads’ initiatives gave firms offering to block all ads for a price, a rapid rise in user base (Katona and Sarvary, 2018). Consequently, paid ad-blocking services such as AdGuard, AdBlock Pro[1] had a rapid rise in market share (Fedorko, 2018; Zambrano and Pickard, 2018). Currently, three major business models for ad-blockers exist. First, free ad-blockers that are mainly browser plugins and expose users to some form of whitelisted ads (e.g., Acceptable Ads, Better Ads Coalition etc.) to generate revenue e.g., AdBlock Plus, Google Chrome Ad Filter, Brave. Second, paid ad-blockers that exist across devices – smartphone to laptops – and have a subscription or licence based payment model and block all ads for a price e.g., AdGuard, Cleanweb, CyberSec, CyberGhost. Third, freemium ad-blockers that have a free and a paid version offering similar benefits, e.g., AdBlock (Free & Premium), Robert by Windscribe, Google Contributor (paid version of Google adblocker), AdLock (free version as plugin, paid version as software install). The free versions typically use ‘Acceptable Ads’ in some cases (AdBlock) or Better Ads listed domains (AdLock).

Rise in market shares of each type of ad-blocker has raised concerns from different stakeholders (Barbacovi, 2016; Miller, 2018; Saluke, 2008). First, consumer rights groups (including Electronic Frontier Foundation) argue that free ad-blockers do not solve the ad-intrusion problem but introduce another avenue for advertisers to target users (Fedorko, 2018). Moreover, Walls et al. (2015) has shown that ad-whitelists have grown rapidly with limited transparency on its governance and with addition of dubious set of advertisers (e.g. 2.6 Parked Domains[2]). Besides, since *Do-Not-Track* service is not supported, privacy isn’t guaranteed in any ad-blocking model and some amount of tracking by whitelisted companies is inevitable (Katona and Sarvary, 2018; Walls et al., 2015). Second, content provider advocates (e.g., Interactive Advertis-

[1] See https://www.vpnmentor.com/blog/the-best-and-worst-ad-blockers/

[2] Recent research has shown that malicious domains once discovered often end up being parked, i.e. temporarily hosted by some domain parking services(Alrwais et al., 2014)

ing Bureau) argue that since advertising revenue pays for content creation, blocking all ads hurts business viability. Moreover, constructing paywalls or introducing subscription fee for consuming content has not proved popular with users of all types, further endangering availability of free online content (Barbacovi, 2016). Besides, in some cases, content providers have accused free ad-blockers of extortion by taking up a fraction of advertising revenue through whitelisted ads (Commission et al., 2015; Fedorko, 2018; Katona and Sarvary, 2018). Consequently, industry regulators and policy-makers acknowledge that web advertising has become an unwieldy problem, exacerbated by the conflict between users, content providers and ad-blockers (Evans, 2009; Johnson, 2013). Policy-makers such as FTC, International Chamber of Commerce etc., are unsure of the right way forward to resolve these concerns (Malandrino et al., 2013; Miller, 2018). Our work aims to inform policy-making in this context. Specifically, through a game-theoretic model studying a monopoly and duopoly of ad-blockers, we analyze economic and welfare implications of different forms of ad-blocker business models. Our analysis shows which business model is ideal from the perspective of different stakeholders: users, content providers and ad-blockers and characterizes the conditions under which the models are preferred. Further, we show how competition in the ad-blocking industry implies users are always worse off. Insights from our analysis can be used to answer two important questions: which ad-blocker model should be dominant in the industry and what happens when no such model is dominant and ad-blockers compete for market share.

2.2 Literature Review

Our work is related to three streams of literature - ad avoidance technologies, online advertising and two-sided platforms.

2.2.1 Ad Avoidance Technologies

Ad avoidance technologies were initially studied in context of the print and broadcast media (e.g., Drèze and Hussherr, 2003; Elliott and Speck, 1998; Speck and Elliott, 1997). The methodology in these papers is empirical, using data collected from various leading newspapers and broadcasting companies. The scope of research was further broadened with analysis using theoretical models of advertiser - content provider interactions (e.g., Anderson and Gans, 2011; Johnson, 2013; Tåg, 2009). The main objective of these models was to investigate content provider responses to ad avoidance. The main insights were related to - (1) how increasing user subscriptions for content with reduced ads could disproportionately increase ad clutter on non-subscribers(Johnson, 2013), (2) increasing targeting intensity on subscribers would benefit content provider but reduce overall welfare of users (Anderson and Gans, 2011) and (3) how paying to reduce advertisements model itself incentivizes content providers to increase ad intensity thereby hurting user welfare (Johnson, 2013; Tåg, 2009). However, ad-blockers and the model of acceptable ads has introduced a different set of problems in the context of online media consumption. Ad-blockers have evolved into a unique multi-sided platform. This presents a two-fold opportunity for research. Firstly, ad-avoidance using memberships on a two sided platform presents an opportunity to further add to the burgeoning literature on online two sided platforms. Second, it becomes interesting to analyze how using ad-avoidance online can have different implications for welfare of users, advertisers and content providers. As explained in Cho (2004), avoiding ads on the Internet differs from traditional media in several ways. First, many people consider the Internet a tool rather than an entertainment medium, which may make users take measures to avoid Internet ads more actively, especially when time constraints exist to perform specific tasks. Second, in general Internet users prefer a faster connection for transacting online, which is less applicable to traditional media. This implies that Internet users react negatively towards Internet ads when they perceive slowing down of speed of data access due to ads. Till now, the main advances in academic research into ad-blocking and ad-blockers has come from the engineering and technology academia with papers such as Krammer (2008), Hemmer (2005), Pujol et al. (2015). What has been missing is research into the economic implications of rise in behavior such as adoption and usage of ad-blocking from users. Recent research in this space points to works that look at content provider responses to ad-blocking (Aseri et al., 2018) and impact of ad-blocking on content provision overall (Shiller et al., 2017). We aim to fill this gap and contribute in a situation where - (1) ad-avoidance has evolved into a *quality-certifying* platform with membership notions for users and advertisers, (2) content providers suffering reduction to payoff due to different business models. Further, we aim to contribute by analyzing participation patterns of users and advertisers given that both reap benefits due to membership on the ad-blocker platform.

2.2.2 Online Advertising Ecosystem

In the early 90s, online advertising was mainly in the form of static banner ads on static web-pages (Lee, 2001). With the arrival of search intermediaries, firms found a new medium for targeting users. The idea that search results could be the new ‘real-estate’ that has potential for better responses from the target audience became more relevant as time went by. Seminal papers that contributed to the understanding of newer methods of auctions in online search advertising are primarily due to Varian (2007), Varian et al. (2006), Varian (2009) and Edelman et al. (2007). The primary mechanism behind success in this enhanced online ecosystem became use of keywords to target users, bidding for better positions on search results and minimizing costs of displaying ads by strategizing on which schemes to bid under - cost per click/impression or action. Many papers such as Balachander et al. (2009) and Aggarwal et al. (2006) have studied various aspects of these decisions and strategies. However, with the arrival of ad-exchanges, which became a critical cog in the chain of flow between users and advertisers, things have become more involved. As analyzed in Stone-Gross et al. (2011) and Muthukrishnan (2009), ad-exchanges present an opportunity to the advertisers (supply-side) to game the system in order to optimize their payoffs. This translates to the probability of fraudulent activities increasing which decreases surplus not only for the users but for the ad exchange intermediary. One fallout of this situation has been an increase in insidious advertising that although has better user targeting but is, in expectation, more intrusive than before. One can argue that the natural progression in response to this situation has been the rise of ad-blocking technology, which to some extent, has helped in mitigating the effects of such intrusive advertising.

2.2.3 Club Theory

Club theory deals with goods that are excludable but non-rival. Essentially, club goods are derived from excludable public goods where consumers of the good form a voluntary group to enjoy mutual benefits from consumption (Sandler, 2013). In forming such groups, consumers share production costs or consumption characteristics. Interest in analyzing how club goods impact economy at large and markets in particular is not new. In fact, the earliest paper on club theory was by Buchanan (1965). Since then, more refinements have been made to studying variations in club structures and the applications of such structures to society. To cite a few examples, clubs have been refined to include sharing of goods among a group of clubs (Sterbenz and Sandler, 1992). In other works, when groups of users take advantage of using club resources by reputation of their membership, club goods and overall welfare are impacted (Scotchmer, 1997). In order to remedy effects from such reputation driven herding, costs to joining clubs that enable excluding certain members have been studied too (Helsley and Strange, 1994). Further, to enable a variety of members joining clubs and improving overall revenue for clubs, models have considered analyzing club models offering multiple club goods under the same membership form (Brueckner and Lee, 1991; Sandler and Tschirhart, 1997). Finally, in order to improve joining decision under availability of imperfect information, models have included asymmetric information to motivate how clubs can take advantage of membership sizes (Lee, 1991; Silva and Kahn, 1993). Club theory has been developed using two important premises. First, it is assumed that membership in clubs requires restrictions to group size, to an extent where membership size is an endogenous variable in many formulations. In some models, toll or congestion price acts as controlling variable to membership size. In other models, the utilization of club facilities fixes membership size. Second, it is assumed that both membership size and club good provision are related allocation decisions faced by any profit-maximizing club. Club theory is therefore considered as an important development in Economic Theory wherein, public and private goods provision is considered complete with the addition of an intermediate class of goods – club goods.

2.3 Model

Consider a game consisting of three types of agents - a website or content provider (CP), an ad-blocker (AB) and users. CP offers content bundled with ads to users. AB exists as an option for users to join to avoid ads. Further, AB uses one of the following business models to deliver services: (1) ad-exchange, (2) paid or (3) freemium. Users – non-members and AB members – value content sufficiently high ($v > 2$) such that even on suffering marginal disutility $t \in (0, 1)$ from being exposed to ads, earn a positive marginal utility from consumption. A non-member is exposed to mass 1 advertisers, an ad-exchange/free AB member is exposed to $m_w \in (0, 1)$ mass of whitelisted ads and a paid/premium AB member is exposed to no ads by paying p_a. All AB members enjoy non-rival but excludable benefits $z \in (1, v)$ at a marginal congestion cost $c \in (0, 1)$. Excludable benefits are assumed to be valuable enough to offset the highest possible disutility from exposure to whitelisted ads ($tm_w = 1$) but still valued lower than content v. These benefits are primarily related to secure browsing (e.g., HTTPS everywhere), anti-tracking (e.g., browser fingerprinting) or monetary incentives for being exposed to select ads (e.g., Brave Attention Token or BAT) (Eyeo, 2013; Li et al., 2017b; Palant, 2011). Congestion costs exist due to disutility from performance issues of ad-blockers due to multiple user-generated domain filter-lists[3] (Newman and Bustamante, 2019; Vastel et al., 2018a,b; Wills and Uzunoglu, 2016) or due to frequent user-feedback driven changes in ad-blocking standards (Huang and Cheng, 2017; Lashkari et al., 2017; Palant, 2011; Pujol et al., 2015). Essentially, congestion costs help capture the disutility that ad-block members face when consuming content, due to increased member participation in updating ad-filtering rules and standards. Typical examples of disutility include increased time to first paint (TTFP)[4] (Newman and Bustamante, 2019) and increased vulnerability to spyware (Tucker, 2019).

We assume a two-stage game structure. In the first stage AB either sets a price for premium membership and price of whitelisting (paid/freemium models) or enjoys revenue from free AB users (ad-exchange). Given the optimal premium membership price (paid/freemium models) or mass of whitelisted advertisers (ad-exchange), in the second stage, users decide to join or not join the AB based on respective payoffs. Assume all users and advertisers interact with each other, either through the AB or outside of it. Specifically, all advertisers interact with non AB users whereas whitelisted advertisers interact with everyone except premium members. Club theoretic notions are used to model AB and AB member payoffs. Classical club theory models consider user heterogeneity along various member characteristics such as rate of club usage or price sensitivity (Ellickson et al., 2001; Sandler and Tschirhart, 1997; Scotchmer, 1997). In our case, we consider usage heterogeneity in content consumption/internet usage hours. Recent survey by PageFair suggests that time spent consuming content coupled with content valuation drive users to keep using ad-block or disabling it, given CP reactions such as consumption blocking (Foster, 2016).

[3] See AdBlock Plus: https://adblockplus.org/en/getting˙started

[4] First paint (FP) and first contentful paint (FCP) are metrics that mark points on a website immediately after navigation. Specificslly, when the browser renders pixels to the screen these metrics measure user experience perspective.

2.3.1 User Problem

Users are differentiated by $\alpha \in (0,1)$ – internet usage hours. Assume that irrespective of user type, each user in this model earns a positive marginal utility from content consumption. That is, assume a user $\alpha \in (0,1)$ in this model receives utility $v > 2$ from consumption and disutility $t \in (0,1)$ from exposure to mass 1 intrusive ads, such that

$$u_1 = \alpha(v - t), \quad \text{Non ad-block user} \tag{2.1}$$

In order to improve consumption experience, users resort to using AB to enjoy browsing benefits $z \in (1, v)$. By joining AB, users may consider free or paid usage. In free usage, users are exposed to select mass $m_w \in (0,1)$ of ads whereas in paid usage, users are not exposed to any ads. So, utilities for free and paid usage are:

$$u_2 = \underbrace{\alpha(v + z - tm_w)}_{\text{Benefit from CP + AB}} - \underbrace{c(n_2 + n_3)}_{\text{AB Congestion Costs}}, \quad \text{Free AB usage} \tag{2.2}$$

$$u_3 = \underbrace{\alpha(v + z)}_{\text{Benefit from CP + AB}} - \underbrace{c(n_2 + n_3)}_{\text{AB Congestion Costs}} - \underbrace{p_a}_{\text{Membership Price}}, \quad \text{Paid AB usage} \tag{2.3}$$

where $c \in (0,1)$ is the congestion cost, n_1 is mass of non-members, n_2 is mass of free ad-block users and n_3 is mass of paid users such that $n_1 + n_2 + n_3 = 1$. The user's problem can then be formulated as:

$$V_\alpha = \begin{cases} \max\{u_1, u_2\} \ \forall\, \alpha \in (0,1), & \text{Ad-Exchange AB} \\ \max\{u_1, u_3\} \ \forall\, \alpha \in (0,1), & \text{Paid AB} \\ \max\{u_1, u_2, u_3\} \ \forall\, \alpha \in (0,1), & \text{Freemium AB} \end{cases} \tag{2.4}$$

Risk-neutral (linear) assumption of user utility, when consuming ad-supported content online has been used in past works dealing with advertising & privacy (Anderson and Gans, 2011; De Corniere and De Nijs, 2016; Iyer et al., 2005; Johnson, 2013). Specifically, consumption's linear relation to ad-disutility has been used to model users in analyzing online ad-targeting strategies (Athey and Gans, 2010; Iyer et al., 2005; Johnson, 2013; Vratonjic et al., 2013). We use same notions to formulate the user model.

2.3.2 Ad-Blocker Problem

Assume a single ad-blocker AB that provides basic service of blocking intrusive ads and providing additional benefits $z \in (1, v)$ such as malware protection[5]. The basic problem of for AB is as follows:

$$\underset{p_a, p_w}{\text{Maximize}} \quad k m_w \int_{\text{ad-ex}} \alpha d\alpha + p_w m_w + p_a \int_{\text{paid}} d\alpha \tag{2.5}$$

where to $k m_w \int_{\text{ad-ex}} \alpha d\alpha$ is the revenue from free members under Ad-Exchange model, $p_a \int_{\text{paid}} d\alpha$ is the revenue from paying members under Paid model and $p_w m_w$ is the revenue from whitelisting. When choosing a business model, AB maximizes revenue by deciding: both price of premium membership p_a and price of whitelisting p_w (freemium), or either price of membership p_a (paid) or price of whitelisting p_w (ad-exchange). When deciding on p_w, for simplicity we assume AB essentially sets an entry barrier for advertisers, by comparing free member sizes to non-member (Ad-Exchange) or paid member sizes (Freemium). Therefore, for the ad-exchange model, following is the decision problem for AB:

$$\begin{aligned} &\underset{p_w}{\text{Maximize}} \quad \underbrace{k m_w \int_{\alpha_1}^{1} \alpha d\alpha + p_w m_w}_{\text{Ad-Exchange Revenue}} \\ &\text{subject to} \quad p_w = \begin{cases} \gamma_w^L, & n_2 \geq n_1 \\ \gamma_w^H, & n_2 < n_1 \end{cases}. \end{aligned} \tag{2.6}$$

[5] z as AB benefit is assumed to always be valued lesser than content v, by users

For the freemium model, following is the decision problem for AB:

$$\begin{aligned} \underset{p_a, p_w}{\text{Maximize}} \quad & \underbrace{p_w m_w + p_a \int_{\alpha_2}^{1} d\alpha}_{\text{Freemium Revenue}} \\ \text{subject to} \quad & 0 \leq p_a \leq t m_w \\ & p_w = \begin{cases} \gamma_w^L, & n_2 \geq n_3 \\ \gamma_w^H, & n_2 < n_3 \end{cases}. \end{aligned} \tag{2.7}$$

Finally, for the paid model, following is the decision problem:

$$\begin{aligned} \underset{p_a}{\text{Maximize}} \quad & \underbrace{p_a \int_{\alpha_2}^{1} d\alpha}_{\text{Paid Revenue}} \\ \text{subject to} \quad & 0 \leq p_a \leq t m_w \end{aligned} \tag{2.8}$$

where α_1, α_2 are indifference points for free and paying members of AB respectively, n_2, n_3 are membership sizes of free and paying members, p_w is price of whitelisting such that $\gamma_w^H > \gamma_w^L; \gamma_w^H, \gamma_w^L \in (0, 1)$ and k is revenue shared with CP. Further, $k m_w \int_{\alpha_1}^{\alpha_2} \alpha d\alpha$ is revenue from whitelisted ads and free member interactions (ad-exchange model), $p_a \int_{\alpha_2}^{1} d\alpha$ is revenue from paid membership (freemium/paid model) and $p_w m_w$ is the revenue from charging for whitelisting (ad-exchange/freemium). Similar to 'Acceptable Ads' or 'Better Ads Coalition' type programs[6], we assume ad-exchange AB is able to monetize free members using whitelisted advertiser interactions. Relatedly, it is assumed that a mass $m_w \in (0, 1)$ of whitelisted advertisers exist and is exogenous to the model. In line with whitelisting trends across major platforms (e.g., AdBlock Plus, Brave) price of whitelisting p_w is either zero or is fixed by AB given membership size (Iqbal et al., 2017). Therefore, decision to whitelist by advertisers is a combination of a variety of parameters e.g., ad-blocker platform revenue share parameters, content environment of ad, design features, ad-campaign historic trends etc (Iqbal et al., 2017; Shankland, 2018). We simplify our analysis by assuming such a

[6] See Acceptable Ads: https://acceptableads.com/

mass of advertisers m_w is exogenous. Additionally, ad-exchange AB retains a fraction $k \in (0, 1)$ of free user monetization revenue – a model in line with existing revenue sharing arrangements for AdBlock Plus, Brave etc. (Eyeo, 2013; Palant, 2011; Vastel et al., 2018a). Note that the revenue structure of freemium AB is also in line with profit maximizing club models (Ellickson et al., 2001; Sandler and Tschirhart, 1997), where clubs are able to earn revenue from all its members – free or premium.

2.3.3 Content Provider Problem

Assume a single content provider CP. The CP provides users access to content valued at $v > 2$ and sustains content through ad revenue. Without ad-blockers, the content provider earns from interaction of mass 1 users and advertisers. Presence of ad-blocker restructures the revenue for CP. As per different models of AB, the revenue for CP is as follows:

$$\pi_{CP}^{\text{ad-ex}} = (1-k)m_w \int_{\alpha_1}^{\alpha_2} \alpha d\alpha + \int_{0}^{\alpha_1} \alpha d\alpha \tag{2.9}$$

$$\pi_{CP}^{\text{frm}} = m_w \int_{\alpha_1}^{\alpha_2} \alpha d\alpha + \int_{0}^{\alpha_1} \alpha d\alpha \tag{2.10}$$

$$\pi_{CP}^{\text{paid}} = \int_{0}^{\alpha_1} \alpha d\alpha \tag{2.11}$$

where α_1, α_2 are indifference points for free and paying members of AB respectively and $1 - k$ is revenue retained from free AB users (ad-exchange). Note that marginal ad revenue from users is assumed to be a function of their internet usage α and mass of ads m_w, and is assumed to be independent of AB membership.

2.4 Equilibrium Analysis

Analysis is done for each type of ad-blocker revenue model, beginning with the ad-exchange type AB. Recall the two stage game where second stage users decide between joining and not joining and first stage, AB maximizes revenue and either shares with CP (k) or allows CP to enjoy payoff from free members.

Consider the Ad-Exchange model and the user stage 2 problem. Given a mass of whitelisted advertisers m_w, users decide whether to join AB. Mass of free AB members is therefore $n_2 = 1 - \left(\frac{c}{c+z+t(1-m_w)}\right)$ while non-members is $n_1 = \left(\frac{c}{c+z+t(1-m_w)}\right)$. Given these masses, in the first stage, AB & CP enjoy revenues from advertising. Following is a characterization of the equilibrium under Ad-Exchange AB.

Lemma 1 *For $c, t, m_w \in (0,1)$, $z \in (1,v)$, following characterizes the equilibrium under the Ad-Exchange AB model:*

- *Mass of users joining AB $\in (\frac{1}{2}, 1]$.*
- *Price of whitelisting $p_w^* = \gamma_w^L$*

Intuitively, equilibrium under ad-exchange is determined by AB benefits z and mass of whitelisted ads m_w. The higher the benefits offered, the more incentive for users to join AB. Conversely, an increase in mass of whitelisting increases disutility while using AB, causing a decrease in membership size. In the limiting case where $m_w \approx 1$, the indifferent user is still below $\frac{1}{2}$. Hence, under a monopoly ad-exchange model, more users tend to join the AB than not, implying revenues for CP and AB are now a function of revenue sharing fraction k. Interestingly, since mass of free users is higher than non-members, AB chooses a lower price of whitelisting γ_w^L. In practice, whitelisting prices by AdBlock Plus, Brave etc. reflect similarities with derived insights. Specifically, AdBlock Plus whitelists 94% of the entities in Acceptable Ads for free while larger entities such as Google, Yahoo etc. pay to be whitelisted (Palant, 2011).

Now consider the Paid AB model and the second stage user problem. Given a price of membership p_a, mass of paid members is $n_3 = 1 - \left(\frac{c+p_a}{c+t+z}\right)$. In the first stage, AB solves for premium price for optimizing revenue as per Equation 2.8. The following characterizes equilibrium under Paid AB model.

Lemma 2 *For $c, t, m_w \in (0,1)$, $z \in (1, v)$, following characterizes the equilibrium under the Paid AB model:*

- *Mass of users joining $AB \in (0, \frac{1}{2}]$.*
- *Price of membership $p_a^* = \frac{t+z}{2}$.*

Under the Paid model, it is clear that price of membership determines the indifferent user location in $\alpha \in (0,1)$. Further, the absence of whitelisting ads implies greater utility from membership, the higher the usage intensity α of users. Hence, given AB benefits z delivered and marginal ad-disutility t, AB sets price of membership $p_a^* = \frac{t+z}{2}$ so that it captures a portion of surplus created from improvement in consumption and removal of disutility from exposure to mass 1 ads. Since it is assumed that users enjoy positive marginal utility from consumption, users at higher consumption intensities would enjoy non-negative utility, given the price. Hence membership size is at most $\frac{1}{2}$ and could be as low as zero.

Finally, consider the Freemium AB model and the second stage user problem. Recall, n_2 denotes mass of free members, n_3 mass of premium members while n_1 is mass of non-members. Given the price of premium membership p_a, mass of free members in stage 2 is $n_2 = \frac{p_a}{tm_w} - \frac{c}{c+z+t(1-m_w)}$ and mass of premium members is $n_3 = 1 - \frac{p_a}{tm_w}$. In the first stage, AB solves for optimal p_a, p_w as per Equation 2.7. The following characterizes equilibrium under the Freemium AB model.

Lemma 3 *For $c, t, m_w \in (0,1)$, $z \in (1, v)$, following characterizes the equilibrium under the Freemium AB model:*

- *Mass of premium users is $n_3^* = \frac{1}{2}$ while mass of free users is $n_2^* = \frac{1}{2} - \frac{c}{c+z+t(1-m_w)}$.*
- *Price of premium membership $p_a^* = \frac{tm_w}{2}$.*
- *Price of whitelisting $p_w^* = \gamma_w^H$.*

Under freemium, AB has to consider maximizing revenue given that the price it sets for premium membership impacts both free and premium membership sizes. Hence, in the first stage AB has a trade-off: choose p_a that increases free membership size but decreases whitelisting revenue or that decreases free membership size but increases whitelisting revenue. From Lemma 1 and stage 2 n_2, it is clear that since mass of free members is bounded below by $\frac{1}{2}$, AB is guaranteed some positive mass of free members even on selecting a high price of premium membership. Hence, AB goes for higher price of whitelisting and p_a that decreases free membership size. In practice, freemium models are popular in the smartphone space with popular ad-blockers such as Disconnect, 1Blocker enjoying wide popularity based on its freemium pricing and limited whitelisting practices (Greenberg, 2016). Interestingly, note that freemium pricing of AB is a function of negative externality tm_w. Similar to insights from Nan et al. (2018) and Geng and Chen (2019) that consider freemium under threats of piracy, optimal pricing in context of ABs is susceptible to price increases the greater the negative externality from ads.

2.5 Welfare Analysis

We now conduct comparisons of user welfare, CP & AB payoffs at equilibrium under different AB models. We begin with user welfare analysis under different models and conclude with comparisons of payoff for CP & AB.

Proposition 1 *Considering user welfare, for $c, t, m_w \in (0, 1)$, $z \in (1, v)$ welfare under Freemium is highest when compared to Ad-Exchange and Paid models. Further, under Paid, user welfare is the lowest.*

Proof is in Appendix A. This interesting result follows from the combined effects of price discrimination and the freemium benefit of higher quality offerings at higher usage levels. First, note that when comparing Freemium to Ad-Exchange, the absence of premium membership option in Ad-Exchange, for users at the upper end of usage levels, leaves the opportunity to capture user surplus. In fact, for the same mass of whitelisted ads m_w, although market coverage is same in both Ad-Exchange and Freemium, the overall increase in welfare from upgrade to premium membership in

Freemium offsets welfare under Ad-Exchange. In addition, since price of premium membership in Freemium is less than that in pure paid, welfare from blocking all ads under Freemium exceeds that under Paid. Second, similar to the increasing percentage differences condition (Anderson and Dana Jr, 2009), we show than an increase in negative externality t, m_w impacts only one segment under Freemium whereas under Ad-Exchange or Paid, impacts entire user base. Therefore, even though prices increase with increase in ad-intrusiveness or whitelisting activities, users are better off under Freemium than under other models.

Implications from Proposition 1 are also extendable to freemium pricing models. Runge et al. (2017); Wagner et al. (2014) establish that freemium pricing charges users for value-add features which are typically absent in the free version of the product. While value in the premium product and intensity of free product usage drive free to premium conversion (Wagner et al., 2014), price paid for premium version is offset by additional product features, additional content, or an otherwise improved product experience (Hamari et al., 2017). Considering AB, free users convert to premium driven by higher intensity of content consumption (α) and to escape 'price' of free services – (tm_w) – exposure to m_w advertisers at marginal disutility t. Given benefits z in free and premium versions are essentially the same, premium pricing extracts part of the cost of providing 'additional' benefit of removing whitelisted ads that is lower than cost of free membership. Effectively, the user improves consumption on conversion to premium.

We now consider comparing payoffs for CP under the three AB models.

Lemma 4 *For* $k \in (0, 1 - \left(\frac{2c+t+m_w}{2(c+t+m_w)}\right)^2)$ *&* $m_w \in (\widehat{m_w}, 1)$ *where* $\widehat{m_w}$ *satisfies:*

- $m_w + (1 - m_w)\left(\frac{c}{c+z+t(1-m_w)}\right)^2 \geq \left(\frac{2c+t+z}{2(c+t+z)}\right)^2$
- $m_w((c + z + t(1 - m_w))^2 - c^2)(k - 1) + \left(\frac{2c+t+z}{2(c+t+z)}\right)^2 (c + z + t(1 - m_w))^2 - c^2 \leq 0$

CP is better off under Ad-Exchange than under Paid model.

First, note that when comparing revenues under Ad-Exchange and Paid, CP earns from advertising to non-members and free members under Ad-Exchange, as opposed to earning only from non-members under Paid. Further, recall from Lemmas 1, 2 that market coverage for AB under Ad-Exchange exceeds that under Paid. Indirectly, CP has a larger user segment to earn from under Paid than under Ad-exchange. Hence, for CP to earn higher under Ad-Exchange model, the revenue sharing k has to bounded from above and the mass of whitelisted ads has to be higher than a minimum value. Our result essentially characterizes this condition.

Lemma 5 *For $k \in (0, \frac{3}{4})$, & $m_w \in (0, \widehat{m_{w1}}) \cup (\widehat{m_{w1}}, 1)$, where $\widehat{m_{w1}}, \widehat{m_{w2}}$ satisfy:*

$$\frac{(c + z + t(1 - m_w))^2 - 4c^2}{4\left((c + z + t(1 - m_w))^2 - c^2\right)} \leq 1 - k$$

CP is better off under Ad-Exchange than under Freemium model.

In comparing Ad-Exchange with Freemium, note that under both models, CP has the option of earning advertising revenues from free and non-members. However, for a given mass of whitelisted ads, the amount of revenue would differ under these two models. Further, changes in mass of whitelisted ads would determine the free and non-member populations and so, an increase in m_w doesn't necessarily imply improvement in revenues from these user segments. Our result basically shows that although revenue sharing has an upper bound, mass of whitelisted ads has a range within which CP is worse off but above and below which CP is better off under Ad-Exchange. Interestingly, our insight can help explain how the well-known strategy of limiting memberships and maintaining a separate ad-network of advertisers on whitelisting platforms such as Acceptable Ads or Coalition of Better Ads firms such as AdBlock Plus & Brave has been touted to improve revenues for participating content providers and websites (Katona and Sarvary, 2018; Manjoo, 2015). However, with increased competition from Freemium firms, content providers have an option to earn higher revenues if mass of whitelisted ads are lower than a threshold or if revenue sharing agreements are amenable (Vastel et al., 2018b).

Proposition 2 *For $c, t, m_w \in (0, 1)$, $z \in (1, v)$, CP is always better off under Paid than under Freemium model.*

Proof is in Appendix A. Intuitively, under Freemium, AB covers a larger market than under Paid model. Hence, for CP potential advertising revenues from non-members under paid exceeds ad-revenues under ad-exchange, for the same mass of whitelisted advertisers. Further, revenue from free member mass under Freemium is lower than revenue from non-members. This is because free members under Freemium are characterized by internet usage intensity $\alpha < \frac{1}{2}$ such that under Paid, CP earns more from such users as non-members, by exposure to mass 1 advertisers. From an industry standpoint, it is known that paid ad-blocking enjoys low popularity among users, in comparison to free or freemium ad-blockers such as AdBlock Plus and AdBlock Pro (Ikram and Kaafar, 2017). This doesn't bode well for content providers since price sensitivity of users can help in generating more revenue from ad exposure to non ad-block users than ad-block users. Hence, from CP's perspective, paid blocking of all ads would actually work out better than Freemium, something that contradicts what users prefer.

Finally, we consider AB payoffs under different models.

Lemma 6 *For* $k \in ((1-\frac{2c+t+z}{2(c+t+z)})(z+t)-2\gamma_w^L, 1)$ *and* $m_w \in \left(\underline{m_w}, \min\left\{1, \frac{(t+z)\left(1-\frac{2c+t+z}{2(c+t+z)}\right)}{2\gamma_w^L}\right\}\right)$ *where* $\underline{m_w}$ *satisfies:*

$$\frac{(t+z)(1-\frac{2c+t+z}{2(c+t+z)})}{m_w\left(1-\frac{c^2}{(c+z+t(1-m_w))^2}\right)} \leq 1 + \frac{2\gamma_w^L}{\left(1-\frac{c^2}{(c+z+t(1-m_w))^2}\right)}$$

AB is better off with Ad-Exchange than Paid as its business model.

Under Ad-Exchange, AB is earning both from whitelisted advertisers and free members while under paid, AB only earns from paying users. Further, since the mass of users in Paid is bounded from above by $\frac{1}{2}$, it would seem intuitive that Ad-Exchange should have more revenue than Paid for AB. However, AB has to resolve a trade-off – increasing mass of whitelisted advertisers while earning higher revenue from free members. This is because an increase in m_w impacts free membership size negatively, leading to a decrease from free member ad revenues while whitelisting revenues increase. Under paid, this trade-off is non-existent due to no whitelisting. Therefore, there exists a range of $m_w \in (0,1)$ within which AB earns higher from Ad-Exchange than from Paid. Further, note that AB revenue sharing has a lower bound for AB, as opposed to an upper bound for CP under the same comparison (Lemma 4). This suggests presence of conflicting objectives and that use of bargaining power could impact either AB or CP adversely (Karsenty, 2016; Mansfield-Devine, 2015).

Proposition 3 *Comparing Freemium to Ad-Exchange and Paid business models:*

- *For* $m_w \in \left(\left(\frac{t+z}{(\frac{t}{2}+2\gamma_w^H)}\right)\left(1-\left(\frac{2c+t+z}{2(c+t+z)}\right)\right),1\right)$ *AB is better off with Freemium than Paid as its business model.*

- *For* $k \in (\frac{t}{2},1)$ *and* $m_w \in (\underline{m_w},\overline{m_w})$ *where* $\underline{m_w},\overline{m_w}$ *satisfy:*

$$2k - \frac{2kc^2}{(c+z+t(1-m_w))^2} - t \geq 0$$

AB is better off with Ad-Exchange than with Freemium as its business model.

This proposition characterizes conditions under which the Freemium business model is preferred by AB, compared to the other two – Paid and Ad-Exchange. First note that for Freemium to be better than Paid, AB benefits from an increase in whitelisting above a threshold. This is because from an increase in m_w, AB earns higher from premium members and advertisers, who pay γ_w^H. Further, an increase in club benefits z only serves to decrease the lower bound of mass of whitelisting, above which AB prefers Freemium to Paid. Taken together with insights from users and CP, it is clear that for AB to prefer Freemium to Paid, users will have to suffer higher whitelisted ad exposure while CP will always have lower revenues compared to Paid. Comparing Freemium with Ad-Exchange, note that although market coverage for Freemium and Ad-Exchange are the same, AB earns higher from Freemium only when mass of whitelisters is either too high or too low $\Rightarrow m_w \in (0,\underline{m_w}) \cup (\overline{m_w},1)$. For the same reasons as explained in Lemma 5, an increase in m_w does not have a monotonic impact on revenues from Ad-Exchange when compared to Freemium. Hence, when m_w is lower or higher than a threshold, free membership sizes decrease and Freemium model outperforms Ad-Exchange with revenue from whitelisted advertisers and premium members exceeding free member revenues from Ad-Exchange.

Considering the welfare implications in totality, for any AB business model to be a dominant model in the industry, preferences of any one or two agents might not be enough to ensure an improvement in overall welfare. For instance, if user preferences are considered paramount, then for Freemium to be the dominant model in the industry, CP will always be worse off while AB would be better off only when mass of whitelisting is either too low or too high. From a practical recommendation perspective, this implies that it is impossible to reconcile preferences of all three stakeholders in a way that improves overall welfare (Barbacovi, 2016). On one hand, it is well know that users care more about transactions and value from content consumption than being exposed to ads. In fact, it is now known from various marketing studies that adoption of ad-blockers has been primarily driven by this user frustration. Even so, usage of ad-blockers has led to users primarily being responsible for the loss of revenue of content providers. Our revenue model analysis takes this tension into account and sheds light on attempts at finding workable solution to this 'stand-off' between AB, CP and users. As we show, this problem of blocking ads while ensuring minimum revenue loss for content providers may have irreconcilable differences between stakeholders.

2.6 Competition in Ad-Blocker Market

We now shift to the scenario where the market for ad-blocking has competing ad-blockers. Using competition among ad-blockers, we analyze how the market for such disutility removing tools can result in consumers getting lower benefits at higher costs. Consider a duopoly with complete market coverage by competing ABs. Incomplete market coverage is considered as an extension to this model, in a later section. Using the same game structure as in monopoly model, in first stage, the ABs (AB_1, AB_2)

provide club good $z_1, z_2 \in (1, v)$ to members using either an ad-exchange, freemium or paid model with prices p_1, p_2 respectively. Additionally, ABs provides access to content $v > 2$, whitelisted advertiser masses $m_i \in (0,1),\ \forall\ i \in \{1,2\}$ (assume $m_1 > m_2$) at marginal disutility $t \in (0,1)$ and consumption with congestion costs c_1n_1, c_2n_2 (marginal congestion $c_i \in (0,1)\ \forall\ i \in \{1,2\}$), where $n_1, n_2 \in (0,1)$ are membership sizes in the respective clubs. In second stage, a user i faces choice of utilities between membership in clubs $i, j\ \forall\ i, j \in \{1,2\}, i \neq j$ which is expressed as,

$$u_i = \begin{cases} \underbrace{v + z_i}_{\text{CP + AB 1 Benefit}} - \underbrace{c_i n_i}_{\text{AB 1 Congestion Costs}} - \underbrace{p_i}_{\text{Membership Price 1}} - \underbrace{k_p x}_{\text{Adoption Costs Paid}}, & \text{Paid AB} \\ \underbrace{v + z_i - tm_i}_{\text{CP + AB 1 Benefit}} - \underbrace{c_i n_i}_{\text{AB 1 Congestion Costs}} - \underbrace{k_f x}_{\text{Adoption Costs Free}}, & \text{Free AB} \end{cases} \tag{2.12}$$

$$u_j = \begin{cases} \underbrace{v + z_j}_{\text{CP + AB 1 Benefit}} - \underbrace{c_j n_j}_{\text{AB 1 Congestion Costs}} - \underbrace{p_j}_{\text{Membership Price 1}} - \underbrace{k_p(1-x)}_{\text{Adoption Costs Paid}}, & \text{Paid AB} \\ \underbrace{v + z_j - tm_j}_{\text{CP + AB 2 Benefit}} - \underbrace{c_j n_j}_{\text{AB 2 Congestion Costs}} - \underbrace{k_f(1-x)}_{\text{Adoption Costs Free}}, & \text{Free AB} \end{cases} \tag{2.13}$$

Note that the given formulation allows modeling Freemium as a choice for a user between paid or free usage, when analyzing competition between ABs. Similar to Hotelling Model, assume that the two AB firms at opposite end of line $x \in [0,1]$. Users are homogeneous except for their marginal adoption costs/preferences, for each AB. In contrast to monopoly case, in duopoly we consider adoption cost or preferences as a heterogeneity parameter for users. Adoption costs can be understood to be brand loyalty for an ad-blocker, interoperability with user devices, backward compatibility issues etc.,(Garimella et al., 2017; Malloy et al., 2016; Post and Sekharan, 2015; Walls et al., 2015). Assume marginal adoption costs are sufficiently high such that complete market coverage by any one AB is impossible, $k_p, k_f > 2, k_p - k_f > 1$. Further, suppose that ABs have minimally differentiated offerings such that $|z_1 - z_2| \in (0,1)$ which is practically the case (Karsenty, 2016; Mansfield-Devine, 2015; Nithyanand et al., 2016; Vallade, 2008). That is, we consider cases the offerings are similar in benefits with the major differences being in congestion costs and mass of whitelisted advertisers. To analyze competition, we consider 6 cases – each case being a duopoly with each club having the same or different business model. The simplified revenue model for AB in each model is as follows:

$$\pi_{AB} = \begin{cases} p_i n_i, & \text{Paid} \\ m_i n_i, & \text{Ad-Exchange} \\ p_i n_i + \gamma_i m_i, & \text{Freemium} \end{cases} \tag{2.14}$$

where γ_i is price of whitelisting at each AB for advertisers. The game remains the same where in stage 1, each AB sets price of premium membership. To analyze impact of competition on user welfare, we conduct comparative statics on parameters impacting price and/or membership sizes. The cases considered are listed as follows.

Table 2.1.: Competition Cases for Analysis

Case	**AB1**	**AB2**	**Example Scenario**
1	Ad-Exchange	Ad-Exchange	AdBlock Plus vs. Brave
2	Ad-Exchange	Paid	AdBlock Plus vs. AdGuard
3	Ad-Exchange	Freemium	AdBlock Plus vs. 1Blocker
4	Paid	Paid	AdGuard vs. CleanWeb
5	Paid	Freemium	AdGuard vs. 1Blocker
6	Freemium	Freemium	1Blocker vs. Disconnect

Lemma 6 *For cases 1,2,3,5 & 6, at equilibrium, following is the effect of an increase in c_1, c_2, z_1, z_2 on profits:*

- $\frac{\partial \pi^{i*}_{AB}}{\partial z_i} \geq 0, \frac{\partial \pi^{i*}_{AB}}{\partial z_j} \leq 0 \; \forall \; i, j \; \in \{1,2\}, i \neq j$

- $\frac{\partial \pi_{AB}^{i*}}{\partial c_i} \leq 0, \frac{\partial \pi_{AB}^{i*}}{\partial c_j} \geq 0 \ \forall \ i,j \ \in \{1,2\}, i \neq j.$

This is intuitive from the fact that user demands in all cases are a function of congestion costs and AB benefits. Any increase in AB i benefits stimulates demand for that AB while decreasing demand for the other AB, thereby increasing revenue. For congestion costs, since the costs contribute to user disutility, an increase in membership sizes or marginal congestion costs implies decrease in utility. Hence, an increase in AB i's marginal congestion costs increases demand for AB j and vice versa. This leads to increase in profits for AB i when AB j's congestion costs increase. More generally, competition among ad-blockers (ABs) is impacted by value of benefits and congestion costs. While the former is a function of ad environment, the latter is dependent on the technology used by the AB to block all or some ads. In that relation, Lemma 6 essentially argues for improving ad-blocking technology (better z at lower c) to improve user welfare, as opposed to increasing mass of whitelisted advertisers compared to competition – which seems to be the current strategy of both these companies (Nithyanand et al., 2016; Walbesser, 2011). Anecdotal evidence suggests that ad-blocking companies with improved ad-blocking technology that reduces congestion costs for users, have performed better in competition (Brinkmann, 2017; Shankland, 2018). For instance, Brave's AdGraph, that improves ad-blocking performance from user generated filter lists (using machine learning) better than Adblock Plus and other free ad-blockers, has been key in increasing Brave user base on an average 45% from 2017 to 2018 (Shankland, 2018).

Proposition 4 *For all cases except case 4, an increase in mass of whitelisted advertisers at any one ad-blocker never harms but benefits both ad-blockers.*

Our result essentially shows how ad-blockers can benefit from competition in the market, at the expense of users. For a given AB i, an increase in mass of whitelisted ads m_i increases disutility for users and impacts demand negatively. However, demand for the other AB j is increased at the margin and so, AB j earns from an increase in membership size while AB i earns from an increase in mass of whitelisted ads. Overall, users at both ABs suffer a decrease in utility – from an increase in whitelisted ads or from an increase in congestion costs due to membership size increase. Hence, although ABs reap higher revenues, users suffer. Evidence from industry shows how competition in whitelisting platforms has adversely impacted membership numbers. For instance, in the past 5 years, both Brave and AdBlock Plus have established platforms for enabling whitelisting from advertisers (Palant, 2011; Vastel et al., 2018a). With increase in membership and release of ad-blocking services for mobile, both companies have sought to increase whitelisted advertising revenues (Cohen, 2012). However, usage numbers reveal a different story. Specifically, it has been established using data analysis on software downloads average daily user numbers and average daily downloads of ABP are decreasing quite steadily (Brinkmann, 2017). As an example, daily usage of ABP decreased from an average 21.4 million users[7] in 2016 to 15.4 million in 2017. Additionally, ABP had an average daily download count of 181,000 on September 26, 2016 which reduced to 89,000 on year later (Foster, 2016; Katona and Sarvary, 2018). Different analysis studies conducted by industry stalwarts such as PageFair suggests that this decrease in ABP download and usage was primarily due to the Acceptable Ads program. Users found Acceptabel Ads as a violation of the ad-blocking promise and hence, migrated to other blockers that had either no whitelisted ads (uBlock Origin) or seemingly lower whitelisted ads (Brave) (Brinkmann, 2017; Vastel et al., 2018b).

Proposition 5 *Consider Case 4, where ad-blockers compete based on prices. At equilibrium, an increase in marginal congestion cost c_i, c_j increases price and profit for AB_i $\forall\ i, j\ \in\ \{1, 2\}$, $i \neq j$.*

Case 4 looks at competition between paid ad-blockers such as AdLock, AdGuard or Google Contributor. Our analysis shows similarity between this case and competition with increasing prices (Chen and Riordan, 2008; Cowan and Yin, 2008; Zhou, 2006). Specifically, when firms are faced with consumers of different elasticities of demand,

[7] See: https://www.ghacks.net/2017/09/29/firefox-adblock-plus-lost-millions-of-users-in-the-past-year/

price discrimination becomes easier and in competition, charging higher prices becomes best response (Zhou, 2006). In the case 4 scenario, each user's demand for AB services is characterized by congestion costs $c_i \; \forall \; i \in \{1, 2\}$. Since $c_1 \neq c_2$, each user i's net cost of enjoying either AB_1 or AB_2 services is $z_i - (p_i + c_i n_i) \; \forall \; i \in \{1, 2\}$. Further, each AB sets price that is a function of both c_1, c_2. Hence, any change in c_1 is met with price adjustments from AB_1 and AB_2 such that: (1) user surplus across members of both AB's decreases and (2) none of the AB's are worse off. For instance, an increase in c_1 is met with an increase in price of membership p_1 while AB_2 responds with increase in p_2. In other words, impact of increased congestion cost of one AB is tackled by both ABs using pricing as tools that discourage switching from one AB to another. However, the net effect of increase in congestion costs is a decrease in user surplus. Similar to Chen and Riordan (2008); Zhou (2006), the context of ad-blockers shows that competition in increasing prices makes users worse off when firms price discriminate.

We now extend the model to the case with incomplete market coverage by AB1 & 2. That is, in addition to utilities in Equations 2.12, 2.13, we assume users have the option of not joining either AB and enjoying

$$u_k = v - t, \;\; k \neq i, j, \;\; \text{Non-member}$$

Essentially, incomplete market coverage introduces an additional segment similar to the monopoly case. Analyzing all 6 cases using three possible user segments produces the same insights for all cases except case 4. Specifically, for those cases where AB has an option of earning from whitelisting, an increase in whitelisted advertisers benefits either one or both ABs. Further, increase in benefits and congestion costs have the same effects on equilibrium profits. However, for case 4, following is the insight.

Proposition 6 *Consider Case 4, where ad-blockers compete based on prices only. At equilibrium, with incomplete market coverage, prices are independent of marginal congestion costs $c_i, c_j \; \forall \; i, j \in \{1, 2\}, i \neq j$ but are increasing in benefits z_i and marginal* *disutility t. Further, increase in marginal congestion cost c_i has negative impact while increase in z_i, t has positive impact on profits for AB_i.*

This result counters the insight from Proposition 5. More precisely, presence of an option to leave either AB has the following effect on users and ABs: first, since paid model removes all ads, users demand for paid blocking depends on benefits received z_i and disutility removed t. Further, an outside option allows users to improve utility by leaving the AB, when congestion costs increase. Hence, for competing ABs, presence of an outside option for users combined with demand elasticity for blocking all ads results in equilibrium prices that are increasing z_i, t without depending on c_i, c_j. Interestingly, an increase in prices due to increase in either z_i, t increases demand for ad-blocking services. Further, unlike complete market coverage case, prices in this case are lower, independent of the difference in AB benefits but rather depend directly on benefit z_i from AB_i. Therefore user welfare and overall welfare (user + AB) is higher under the condition that an outside option is present at all times. More generally, it is clear that user welfare in an ad-blocker market changes with complete or incomplete market coverage. In an ad-blocker market with complete coverage, changes in congestion costs lead to competing ABs displaying increasing price competition, where prices are increased to benefit from more 'loyal' users ($x \rightarrow 0$ or $x \rightarrow 1$) at the expense of more indifferent users ($x \rightarrow \frac{1}{2}$), even when member size increases (McChesney et al., 2015; Zhou, 2006). However, incomplete market coverage presents a situation where users have an option to leave AB. Hence improvement in benefits through z_i or removal of ad disutility t provides incentive to ABs to improve profits by improving market coverage, thereby improving user welfare.

2.7 Conclusion

Ad-blockers are the ad avoidance tool for content consumption online. However, evolution of ad-blockers to platforms that provide users choice of blocking all ads has implications for memberships of users and advertisers. Specifically, when ad-blockers started sustaining their business using ads, users found this to be a violation of the ad-blocking promise and hence, started preferring other models of ad-blocking. This gave rise to intense competition in the ad-blocking industry and an swift escalation of conflict between content providers and ad-blockers (Digiday, 2016). Our model intends to analyze this conflict from the point of view of users, content providers and ad-blockers. Using a game theoretic model for a monopoly and a duopoly model, we show that when considering users, the dominant business model in ad-blocker industry should be Freemium. Further, when considering all stakeholders in the conflict there is no single revenue model that makes everyone better off. Further, when analyzing competition with all major business models of ad-blocking, we find that competition in the ad-blocker market heating up, ad-blockers could benefit at the expense of users. With incentives to increase whitelisted advertisers and existence of increasing price competition, competition among ad-blockers will only serve to introduce other avenues to target users rather than improve user welfare online.

3. A GRAPH BASED ANT ALGORITHM FOR THE WINNER DETERMINATION PROBLEM IN COMBINATORIAL AUCTIONS

3.1 Introduction

Technology explosion has resulted in sophisticated mechanisms being increasingly adopted internal to organizations to improve efficiency. An example of such a mechanism is combinatorial auctions. They were originally employed to award cellphone spectrum, and also for transportation logistics. However, of late, many companies have used combinatorial auctions to improve procurement efficiencies. For instance, consulting companies such as AT Kearney provide this mechanism to their clients. An example from Kearney's "collaborative optimization"[1] claims 10% savings by a telecommunication company using this mechanism to manage its handset portfolio. Similarly, companies in retail logistics spending \$300M on procurement (Elmaghraby and Keskinocak, 2004; Karaenke et al., 2015) used this mechanism to improve costs by 15-20 %.

While both industry and academia recognize that combinatorial auctions improve efficiency, computational limitations are quite severe for this mechanism. For instance, between the rounds of the auction and before the bidders can resubmit their bids, identifying the tentative winners based on bids submitted thus far is known as Winner Determination Problem (WDP) and it is NP-complete (Sandholm, 2002a). In the age of big data – increased velocity, volume and variety of bundles and bids – WDP is increasingly becoming intractable within limited time (Karaenke et al., 2015). In scenarios such as spectrum auction, the computational issues are not as problematic because they often involve only a few bidders. However, in cloud comput-

[1] Collaborative optimization in the academia refers to an entirely different domain on aircraft design.

ing, transportation & logistics auctions conducted on e-commerce exchanges, there is a trend towards iterative combinatorial auctions along with increase in market size of participants and items (Bichler, 2010; Bichler et al., 2006; Lau and Goh, 2002). Typical transportation auctions involve 250 bidders bidding on 1000 routes and it takes a day or so to solve WDP between the rounds of the auction. Even then, often, WDP is not solved to optimality because of time constraints (Karaenke et al., 2018; Leyton-Brown et al., 2000; Zaman and Grosu, 2013). Additionally, IBM CPLEX or AMPL have been ”demonstrably ineffective” (Adomavicius and Gupta, 2005) in producing the optimal solution when faced with big data scenarios in auctions (Boughaci et al., 2009; Lau and Goh, 2002). Instead, heuristic solutions are used (Guo et al., 2006).

In this context, our paper makes the following three contributions:

- We convert the Integer Programming formulation of WDP into a directed cyclic graphical formulation. Unlike previous work (Sandholm and Suri, 2003; Sandholm et al., 2005), we use a directed cyclic graph to represent WDP. Our formulation is especially useful since: a) it is suitable for formulating WDP when items per bid and bids per item are large (typical for intractable WDP problems (Boughaci et al., 2009; Fujishima et al., 1999; Lau and Goh, 2002)), b) it is suitable for optimal search using other graph search algorithms or heuristics and, c) it can be extended to the multi-unit multi-item auctions (e.g., virtual machine instances auction in cloud computing, (Bichler et al., 2009)).

- We develop a swarm intelligence based algorithm (TrACA-**Tr**aveling **A**nts for **C**ombinatorial **A**uctions) and prove the convergence property of our algorithm. This property simply states that, if the auctioneer has more computational capacity, they are able to converge to the optimal over the same predetermined time by increasing the intensity of the search – intensity meaning larger number of artificial ants in this case. In line with previous applications of ant-colony heuristics in path finding problems (Dorigo and Birattari, 2011; Gan et al., 2007;

Gutjahr, 2000), our theoretical result establishes the benefits of using swarm intelligence search on a graphical search space. Further, time-bound convergence helps in tackling problem of auction data velocity, given such auctions are being conducted iteratively (Adomavicius and Gupta, 2005; Parkes and Ungar, 2000).

- We use standard large test beds (Lau and Goh, 2002) and show that our algorithm generates significantly better outcomes than the best-in-class memetic algorithm (Boughaci et al., 2009). We also compare our results to time-bound results from CPLEX and a recent exact algorithm (Wu and Hao, 2016) and show usefulness of our approach for such large problem instances. Prior work has primarily attempted to solve WDP using either: a) exact but more efficient methods for small problems (Sandholm, 2002a) or b) heuristics such as memetic algorithms for fast and approximate estimation of large problems (Boughaci et al., 2009, 2010; Guo et al., 2006). Exact methods (e.g., CPLEX based solvers) do not solve WDP efficiently when the size of the market increases. At the same time, heuristics are fast but never guarantee the optimal for such large problems. We aim to bridge this gap between heuristics and exact approaches, using our algorithm that has a theoretical convergence property as well as superior practical performance.

In light of recent work in designing computational mechanisms to simplify conducting of combinatorial auctions (e.g., Adomavicius and Gupta, 2005; Bichler et al., 2009) our work aims to fundamentally add to efficient methods of solving winner determination when dealing with big data scenarios. The remainder of the paper is organized as follows. In Section 3.2 we give a brief overview of the past work in solving WDP. In Sections 3.3 we explain our approach by going through a basic overview of the winner determination problem, our formulation using ant colony heuristics principles and involved mathematical basis for faster convergence implementation. In Section 3.4 we explain the nature of the testbeds used for testing the metaheuristic and the experimental results. In Section 3.6, we build a predictive model for predicting TrACA runtimes and determining aspects of combinatorial auctions that generally make estimation of winner determination difficult. In Section 3.7, we demonstrate the utility of our approach by extending it from single-unit multi-item to multi-unit multi-item WDP. In conclusion, in Section 3.8 we demonstrate the relevance of our approach in the context of recent applications of heuristics for solving combinatorial auctions in the industry.

3.2 Literature Review

Winner determination approaches have been an active area of research in the recent past. Essentially, WDP approaches are classified as either exact or inexact algorithms. Exact algorithms use deterministic search techniques to solve mathematical programming formulations of WDP. Inexact algorithms use heuristics to search for optimal or near-optimal solutions.

3.2.1 Previous Approaches for WDP

Exact methods always find an optimal solution, given enough time. Exact algorithms for the WDP initially were proposed as Branch-and-Bound(B-o-B) (Sandholm, 2002a; Sandholm et al., 2002) approach. Other work has involved approaches such as Branch-on-Items (BoI) (Sandholm and Suri, 2000), Branch on Bids (BoB) (Sandholm and Suri, 2003), and Combinatorial Auctions BoB (CABoB) (Sandholm et al., 2005). Exact methods are able to compute optimal allocation for instances containing hundreds of items. Alternatively, Fujishima et al. (1999) proposed CASS (Combinatorial Auction Structural Search) as a Branch-and-Bound algorithm. Further, Leyton-Brown et al. (2000) improved CASS and proposed CAMUS (Combinatorial Auctions Multi-Unit Search) to solve general multi-unit combinatorial auctions. Additional attempts at solving the WDP used more traditional robust approaches. Rothkopf et al. (1998) used a dynamic programming approach and Andersson et al. (2000) proposed an integer programming approach. Holland and O'Sullivan (2005) used constraint programming to formulate and solve a Vickrey combinatorial auction problem. Generally, it has been observed that exact algorithms find the optimal within reasonable time when number of items is between 45 and 250. Nevertheless, when the size of the search tree is high, solving those instances can become time-consuming due to an exponentially large number of search bids.

In contrast, inexact methods do not guarantee finding optimal solutions. More generally, inexact methods (e.g., heuristics) are helpful in solving instances of WDP with large number of bids and bundles. For example, auctions where the number of bids are between 1200 to 1450 bids or higher. In shipping routes and asset planning auctions these cases occur regularly in industry (Cramton et al., 2007). Many inaccurate algorithms for the WDP have been developed: Hybrid Simulated Annealing SAGII Guo et al. (2006), Casanova (Hoos and Boutilier, 2000), stochastic local search (Boughaci et al., 2010) and memetic algorithms (Boughaci et al., 2009). Overall, the memetic algorithm approach outperforms SAGII, Casanova and stochastic local search and uses lesser CPU time for given set of instances (Boughaci et al., 2009). However, MA approach relies on solution representation that may increase space complexity, which Identifies the need for stronger WDP heuristics.

3.2.2 Ant Colony Optimization

Ant Colony Optimization or ACO is a nature inspired population based stochastic search heuristic. Artificial ants are swarm-intelligent agents that build a solution using a probabilistic decision rule, by adding solution components iteratively to partial solutions. It does so by accounting for two parameters - (1) information about the problem instance, and (2) pheromone values in the search space, that change at run-time to reflect the solution search experience in past iterations (Maniezzo and Carbonaro, 2002). Since ACO is a population based metahueristic, pheromones and heuristic information about problem allows these search agents to build a wider variety of solutions and thereby, explore a larger set of feasible solutions than other greedy heuristics. Use of heuristic information for given problems can guide the ants towards the most promising solutions. More importantly, the ants' search history can be utilized to influence, similar to reinforcement learning, solution constructions in future iterations of the algorithm. The first algorithm that can be classified within this framework was presented in 1991 (Dorigo et al., 1991) and then 1999 (Dorigo and Di Caro, 1999). Since then, many diverse variants of the basic heuristic have been reported in past works. Stützle and Hoos (1997) first introduced the idea of bounding pheromone levels on edges in a given ant system. Specifically, Stutzle and Dorigo (2002); Stützle and Hoos (1997) proposed MMAS (Max-Min Ant System) methodology. This methodology basically ensures that ants better explore the search space, by enforcing only those solutions update pheromone values that have delivered more promising results in the past. Further, by bounding the level of pheromones on each edge, reinforcement of best ant solutions in the past iterations that promotes bias in search is prevented. In effect, when only one ant serves the purpose of updating pheromones search exploitation in MMAS is more effective. This is because when one ant is used for pheromone update, the solution components (edges in the case of graphs) that frequently occur in the best solutions in past iterations are promoted while newer components from other ants are found and added, as case may be. However, the challenge in MMAS is basically balancing the choice for update between the iteration-best and global-best ants. More precisely, exploration vs exploitation is controlled using update iteration-best vs global-best. We extend this fundamental concept of pheromone update to a randomized pheromone update between global best, iteration best and a mathematically derived fixed maximum and minimum level. For earlier versions of the derived minimum and maximum level of pheromones please refer Stützle and Hoos (1997).

3.3 WDP Formulation

3.3.1 Preliminaries

Consider the simplest version of WDP as described in Lehmann et al. (2006). Let there be k items represented by the set $S = \{1, 2, 3, 4..., k\}$ that are set for auction. Interested bidders are invited to bid on bundles (combinations/subsets) of items from S. The auctioneer conducts this auction in multiple rounds, wherein at the end of each round, winning bids are provisionally allocated before bidders are re-invited to bid again (Adomavicius and Gupta, 2005; Parkes and Ungar, 2000). Two key constraints are maintained throughout all the auction rounds: 1) an item can be at most allocated to one bidder, 2) all items need not be sold to bidders in each round. Suppose for the given round, a set of l bids, $B = \{b_1, b_2, ..., b_l\}$ is received. A bid $b_j \in B \ \forall \ j \in l$ is a tuple defined as (S_j, q_j), where $S_j \subseteq S$ is a unique subset of items (or bundles) and $q_j > 0$ is the maximum bid price associated with S_j. Further, consider a matrix $A_{k \times l}$, such that $A_{ij} = 1 \ \forall \ i \in k, j \in l$ if item $i \in S_j$. Finally, the decision variables are $x_j = 1$ if bid b_j is accepted as winning and $x_j = 0$ otherwise. The formulation for maximizing auctioneer's revenue is equivalent to the weighted set packing problem and is as follows.

$$\text{WDP-IP:} \qquad \max_{x_j} \sum_{j=1}^{l} q_j x_j \tag{3.1}$$

$$\text{subject to} \quad \sum_{j=1}^{l} A_{ij} x_j \leq 1 \ \ \forall \ \ i \in \{1, 2, 3, 4...., k\} \tag{3.2}$$

$$x_j \in \{0, 1\} \ \ \forall \ \ j \in \{1, 2, 3, 4..., l\} \tag{3.3}$$

Equation (2) ensures that each item can be allocated at most once. This formulation also relaxes the assumption of selling all items every round. This formulation is NP-complete (Andersson et al., 2000; Sandholm et al., 2005). As described in Section 3.2, previous attempts at solving WDP using this formulation used exact approaches (e.g., CPLEX solver). However, an increase in volume and variety of bundles, exact approaches either fail completely (Boughaci et al., 2009) or take too long to solve for winners (Guo et al., 2006).

3.3.2 Graphical formulation of WDP

In this section, we transform the IP formulation into a graphical one where the set of bundles and associated bids are represented on a directed cyclic graph. For a previous version of this procedure, refer Ray and Ventresca (2018). The transformation consists of two steps: preprocessing & construction. For preprocessing, the auction data-set is analyzed to extract unique bundles and their associated maximum prices. This follows Sandholm (2002a) where it is shown that when maximizing revenue, an auctioneer is better off accepting the highest bid for a bundle. Using preprocessed data, a directed cyclic graph is constructed in 4 steps, described as follows:

1. Consider $G(V, E)$ with vertices as exclusive auction bundles. Specifically, if m is the number of unique auction bundles, for which an associated maximum bid price exists, then, $V = \{v_j \mid v_j = S_j \subseteq S \;\forall\; j = 1, 2, 3, 4...m\}$.

2. Construct a directional edge between two vertices $(v_i, v_j) \in V$ if and only if the subsets represented by the vertices are disjoint. Specifically,

$$E = \{(v_i, v_j) \mid v_i \cap v_j = \emptyset \;\forall\; v_i, v_j \in V\}. \tag{3.4}$$

3. Introduce a source s and target t vertex to existing set of vertices. Such artificial vertices represent a point of departure and end for a path crossed by each ant. Additionally, a directed edge is added from s to every vertex in $V \backslash \{t\}$. Similarly, a directed edge is added from every vertex in $V \setminus \{s\}$ to t. No direct edge exists between s and t.

4. Each edge has an edge weight. The weight of an edge (v_i, v_j) is the bundle v_j total bid price. Similarly for (v_i, v_j) edge weight is total bid price for v_i. Weight for any edge incoming to vertex t is zero.

$$w : E \mapsto \mathbb{R}_j^+ \text{ s.t. } w(v_i, v_j) = q_j \;\forall\; i, j = 1, 2, 3...m \;\text{ and } i \neq j \;\text{ but } q_j = 0 \text{ for } v_j = t \tag{3.5}$$

Example Construction: Consider the set of bundles $(b_1 = \{A\}, b_2 = \{B\}, b_3 = \{A, B\})$. Let the total bid amounts associated with these bundles be $\{3, 4, 9\}$, respectively. In the graphical formulation, let vertices as indexed as $V = (s, \{A\}, \{B\}, \{A, B\}, t)$. Then let edges be added following the procedure outlined above. For instance, a valid path on the graph is $s \rightarrow b_1 \rightarrow b_2 \rightarrow t$. The revenue the auctioneer enjoys is 7. However as obvious, the optimal revenue is on the path $s - b_3 - t$ which is 9. Note also that $s - b_1 - b_2 - t$ and $s - b_2 - b_1 - t$ are equivalent as expected.

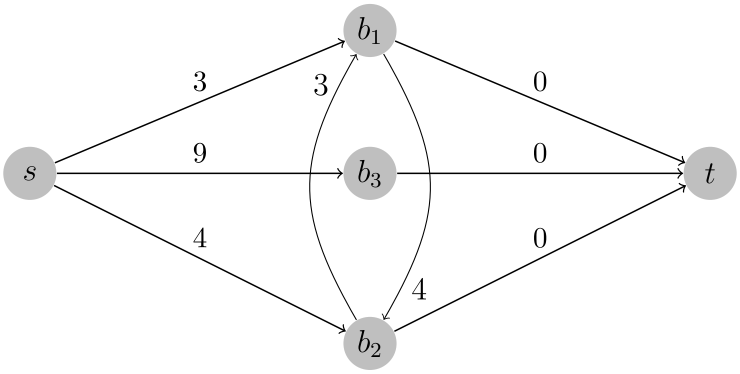

Figure 3.1.: $G(V, E)$ constructed from bundles $\{A, B, AB\}$

Definition 3.3.1 *A path on $G(V, E)$ is a sequence of vertices starting at s and ending at t.*

Definition 3.3.2 *A feasible path of the graph $G(V, E)$ is a path such that for bid bundles b_j associated with each vertex v_j, $b_i \cap b_j = \emptyset \;\; \forall \;\; i, j = 1, 2, .., n$ and $i \neq j$.*

Definition 3.3.3 *An optimal path is a maximum weight feasible path starting at s, ending at t and containing each node of $V = \{v_1, v_2, v_3, ..., v_m\}$ at most once.*

Note that by construction, edges exist between nodes only when bundles (represented by nodes) are disjoint (refer Equation 3.4). Infeasible paths would therefore be those that exist between nodes without any connecting edges and those paths on the graph that have more than one visits on any node. Hence, any search algorithm using this directed cyclic representation will need to maintain feasibility separately (e.g., using a tabu list) such that each node is visited at most once. In the following proposition, we show, given feasibility, how our graphical formulation is equivalent to WDP-IP problem in Section 3.3.1.

Proposition 2 *Directed cyclic graphs G(V,E) constructed using the preprocessing step have the following properties:*

1. *A feasible path from s to t represents a feasible solution to the WDP-IP problem.*

2. *A feasible path of maximum weight on the graph represents an optimal solution to the WDP-IP problem.*

Proofs are in Appendix B. Proposition 1 basically allows use of the graphical formulation of WDP in Section 3.3.4 to search for solutions to the WDP-IP in Section 3.3.1. Having established equivalence, Algorithm 1 in Section 3.3.4 gives a basic overview of the graph based ant algorithm that uses the graph for searching for optimal solutions.

3.3.3 Nature-inspired Metaheuristics for solving WDP

Nature-inspired metaheuristics are a form of search heuristics that use nature-inspired ways of searching for for global optimal in complex optimization problems (Yang, 2010). These heuristics essentially mimic activities of organisms such as ants, fishes, bees etc. to inspire more sophisticated search methodologies. These methodologies basically use a population agents that interact with each other, to conduct search. In practice, such heuristics are classified under the swarm Intelligence based algorithms (Blum and Li, 2008).

A number of swarm intelligence based algorithms can be used to search for the optimal in our graphical formulation (Blum and Roli, 2003) of WDP. [2] The choice of ant colony metaheuristic is motivated by three salient features. First, ant colony heuristics fundamentally rely on iterative construction of solutions, wherein the best solution can be built from the strongest segments identified across various search iterations. Cordón García et al. (2002) note that as a major distinguishing feature of the ant colony algorithm. For example, when applied to solving the traveling salesman problem, it is irrelevant that an ant actually travels the shortest route. The shortest route can be constructed from the strongest segments of the best solutions found.

Second, ant colony heuristics that use a graphical search space demonstrate convergence to global optimal under certain values of the heuristic parameters (Gutjahr, 2000). Essentially, these parameters can be set to values that minimize the probability of not finding the optimal solution within a specified time. From data velocity perspective, this is valuable. As noted in Sheffi (2004), higher likelihood of better quality results within specified time is desirable for decision-makers, when using search heuristics.

Third, solution construction agents (ants) use exchange of information about search space (*stigmergy*) to search through the solution space. This exchange is facilitated by the use of artificial pheromones on graph edges (Dorigo et al., 2000). Stigmergy makes search of solution space more efficient (Stützle and Hoos, 1997). Specifically, stigmergy provides a mechanism using which ants can better explore the solution space rather than exploit a local optimal. This property has contributed to wide applicability of ACO algorithms to NP-Hard problems.

[2] E.g., See other Swarm Intelligent algorithms such as Artificial Bee Colony, Fish Swarm Algorithms.

3.3.4 Graph Based Ant System - TrACA

This section highlights the main aspects of the algorithm. Our algorithm contributes to ant colony metaheuristic literature in two ways: 1) improved exploration of search space using modified pheromone updates and, 2) increased speed of search using graph pruning (search space reduction).

Input & Initialization: The input to Algorithm 1 is the directed cyclic graph $G(V, E)$ from Section 3.3.2 (Line 1). We initialize the following parameters: number of ants N; Traversed list TL that maintains a list of vertices visited by each ant during one iteration; iteration counter MaxIter; pheromone parameters such as initial pheromone level $\tau_0 > 0$ on all graph edges, and ant system parameters α, β (Line 2). τ_0 ensures that each edge has a non-zero and equal probability of being selected during the first iteration for the first ant (Line 4). Parameters α and β are relevant when dealing with the search mechanism, mentioned in the following paragraph.

Search Mechanism: At the start of an iteration, each ant is positioned at vertex s and chooses the next vertex $v_h \notin TL$ using a probabilistic choice rule p_{jh} $\forall$ $(v_j, v_h) \in E$ that is standard (Dorigo and Di Caro, 1999) (Line 8). The p_{jh} is a function of α, β, pheromone levels τ_{jh} and weight w_{jh} of the edge $(v_j, v_h) \in E$. The influence of either pheromones or edge weight is modified by the exponents α, β respectively. Once a vertex is chosen, the Traversed List TL is updated with the chosen vertex (Line 9). By choosing vertices till t is reached, ants construct feasible paths (Lines 8-11).

Pheromone Evaporation & Update: Once a feasible path is searched by each of the N ants, pheromone levels are updated on each edge of $G(V, E)$. First, pheromone levels are reduced by some pre-decided fraction $(1 - \rho)$ from every edge an ant has traversed. This is called pheromone evaporation and is a useful form of decaying unused solution paths (Dorigo and Di Caro, 1999).

Second, post evaporation, pheromone levels are increased on ant-traversed edges. Typically, these increments are a function of the solution quality discovered thus far (i.e., for $t \leq$ MaxIter) that helps in resolving exploration vs. exploitation trade-off

Algorithm 1 GBAS for WDP

```
Input - Directed cyclic graph $G(V, E)$ constructed as per Section 3.3.2
Initialization Step - No. of ants $(N)$, Initial pheromone values $\tau_0$, maximum iterations MaxIter, Ant system parameters $\alpha, \beta$, Traversed List $TL$.
Output - $S_a^{Best}$ - Best solution constructed by Ants
while $t \leq$ MaxIter do
    Ants begin at $a_i \; \forall \; i = 1, 2, 3 ... N$ at vertex $s$
    Initial value $\text{TL}_i = \emptyset$
    for Each ant $a_i$ until vertex $t$ is reached do
        Choose vertex $v_h$ from $v_j$ using $p_{jh} = \frac{\tau_{jh}^{\alpha}[w_{jh}]^{\beta}}{\sum_{h \in \mathbb{N}(j) \setminus TL_i} \tau_{jh}^{\alpha}[w_{jh}]^{\beta}}$.
        $TL_i := TL_i \cup v_h$    ▷ Update Traversed list with chosen vertex $v_h$.
        $S_{a_i} := S_{a_i} + w(e_{jh})$    ▷ Update solution with bid value of chosen vertex $v_h$.
        $v_j = v_h$    ▷ Resetting choice node.
    $TL_{\text{Best}} = \{TL_i \mid i \text{ s.t. } S_{a_i} > \max\{S_a^{\text{Best}}\}\}$; $S_a^{Best} = \max\left\{S_a^{Best}, S_{a_i}\right\}$
        ▷ Global Best Solution Path till iteration $t$
    $TL_t^{max} = \{TL_i \mid i \text{ s.t. } S_{a_i} = \max\{S_{a_i}\}\}$
        ▷ Iteration Best Solution Path in iteration $t$
    Pheromone evaporation on $G(V, E)$: $\tau_{jh}(t) = (1 - \rho)\tau_{jh}(t) \; \forall \; (v_j, v_h) \in E$
    With $\frac{1}{3}$ probability, Pheromone Update Parameters $\{\Delta(\tau), \tau_{max}, \tau_{min}\} :=$
    Option 1: $\left\{\delta(S_a^{Best}), \frac{\delta(S_a^{Best})}{\rho}, \frac{\tau_{max}}{|TL_{\text{Best}}|}\right\}$
        ▷ Global Best Pheromone update parameters
    Option 2: $\left\{\delta(\max(\{S_{a_i}\})), \frac{\delta(\max(\{S_{a_i}\}))}{\rho}, \frac{\tau_{max}}{|TL_t^{max}|}\right\}$
        ▷ Iteration Best Pheromone update parameters
    Option 3: $\left\{\frac{\delta(S_a^{Best}) + \delta(\max(\{S_{a_i}\}))}{2}, k\tau_0, \frac{\tau_0}{k}\right\}$ where $k > 1$
        ▷ Fixed upper and lower pheromone limit
    for each edge $(v_j, v_h) \in \{TL_i\}$ do
        $\tau_{jh}(t + 1) = \tau_{jh}(t) + \Delta(\tau)$    ▷ Pheromone Update
        if $\tau_{jh}(t + 1) > \tau_{max}$ then $\tau_{jh}(t + 1) = \tau_{max}$
        else if $\tau_{jh}(t + 1) < \tau_{min}$ then $\tau_{jh}(t + 1) = \tau_{min}$
Return $S_a^{Best}$
End Procedure
```

(Dorigo and Di Caro, 1999). Our approach to pheromone increment is an extension of Dorigo et al. (2000); Stutzle and Dorigo (2002); Stützle and Hoos (1997). We find that our approach significantly improves performance of Algorithm 1. Specifically, the pheromone levels are increased by $\Delta(\tau) > 0$, which may take one of the three following values randomly: $\Delta(\tau) = \delta(S_a^{Best})$; $\Delta(\tau) = \delta(\max\{S_a\})$; or $\Delta(\tau) = \frac{\delta(S_a^{Best})+\delta(\max\{S_{a_i}\})}{2}$, where $\delta(.)$ is a non-decreasing function of ant solution values. Note that $\max\{S_{a_i}\}$ is the best solution discovered in iteration t; and S_a^{Best} is the best solution among all previous iterations. After both evaporation and increment, the pheromone levels are retained to be within the range $[\tau_{max}, \tau_{min}]$.

Pheromone lower bounds τ_{min} can either be fixed values (Hoos and Boutilier, 2000) or can be changed to vary with search quality. We use both forms for τ_{min}. For options 1 and 2, we assume τ_{min} varies with search and is a function of the maximum threshold:

$$\tau_{min} = \frac{\tau_{max}}{|L|}, \tag{3.6}$$

where $|L|$ is the number of edges created by ants on the best path. For option 1, $|L| = |TL_{\text{Best}}|$; option 2, $|L| = |TL_t^{max}|$. For option 3, we assume a fixed value of $\tau_{min} = \frac{\tau_0}{k}$.

We next discuss the rationale behind setting $\tau_{max} = \frac{\Delta(\tau)}{\rho}$ (based on a previously derived proposition in Ray and Ventresca (2018)). Refer Algorithm 1 Line 20. Pheromone updates starting from $t = 1, 2, 3...$ on any edge are $\tau_{jh}(1) = (1-\rho)\tau_{jh}(0) + \Delta(\tau)$ for $t = 1$, $\tau_{jh}(2) = (1-\rho)^2\tau_{jh}(0) + (1-\rho)\Delta(\tau) + \Delta(\tau)$ for $t = 2$ and so on. Since $0 < \rho < 1$, as $t \to \infty$, $\tau_{jh}(t)$ converges to $\frac{\Delta(\tau)}{\rho}$. For each update option (Algorithm 1, Lines 16-18), the value of $\Delta(\tau)$ determines the upper bound τ_{max}. For option 1, $\tau_{\max} = \frac{\delta(S_a^{Best})}{\rho}$; $\tau_{\max} = \frac{\delta(\max(\{S_{a_i}\}))}{\rho}$ for option 2; $\tau_{\max} = k\tau_0$ where $k > 1$ is user defined, for option 3.

Randomized Graph Pruning

Randomized Graph Pruning is used to approximate solutions effectively and easily for very large instances of problems. Our approach differs in two ways from deterministic graph pruning that is used to remove infeasible edges (Codenotti et al., 1996; Martens et al., 2007). First, we do not enforce feasibility using pruning; we use a Traversed List TL for that (Algorithm 1, Line 9). Second, using randomized pruning we remove a subset of those edges that are likely part of local optima. Randomly removing such edges reduces the likelihood of convergence to different local optima and speeds up search.

Algorithm 2 Randomized Graph Pruning for GBAS

```
Input - $G(V, E)$, Iteration instances $t_c \subset t$ when pruning should be done, count matrix $C$ of size $(|V| - 2) \times (|V| - 2)$.
Output - $G(V, E \setminus E_c)$ where pruned edge set is $E_c$
for Each $t_c \in t$ do
    Construct candidates for pruning edge set $F = \left\{(v_j, v_h) : C_{jh}(t_c) = \left\lceil f\left(\frac{(t_c)\times(t_c+1)}{2}\right)\right\rceil\right\}$
    Remove edges connected to nodes on best path from pruning consideration $F \setminus (v_j, v_h) \in m_{Best}(t)$    ▷ Recall $m_{Best}(t)$ is best path constructed by ants in iteration $t$
    $E = E \setminus E_c$ where $E_c \subseteq F$ is randomly selected and $|E_c| = n$
```

The following is an intuitive explanation of Algorithm 2. Pruning edges is accomplished using a count matrix C. Essentially, in each iteration, the count matrix preserves count number of times an edge is visited by ants. Those edges on the global optimal path would have the highest count. Those edges on local optima would have less than global optimal but greater than one. We identify such edges using the count matrix and randomly prune a subset of those edges.

For measurement, the count matrix C has size $(|V|-2) \times (|V|-2)$ (Line 1) and is initialized as

$$C_{jh} = \begin{cases} 1 \quad \forall \ \ (v_j, v_h) \in G(V \setminus \{s,t\}, E) \\ 0 \qquad\qquad\quad \text{otherwise} \end{cases} \tag{3.7}$$

at $t = 1$. Remember that any non-negative number can be initialized with the default value of each edge on the map. We're using 1 as the initial value. Each time an ant traverses an edge $(v_j, v_h) \in E$ during iteration $t > 1$, $C_{jh}(t) = C_{jh}(t) + 1$. Since edge visits are probabilistic, we use an approximation for identifying edges to prune. Specifically, edges with count $C_{jh}(t_c) = \left\lceil f\left(\frac{(t_c)\times(t_c+1)}{2}\right)\right\rceil$ are considered for pruning. Here, $t_c \subset t$ are iterations when pruning is done and $f(.)$ is the log function. From this set of edges F, we randomly remove a subset of edges E_c (Line 6).

Theoretical Convergence to Optimal

Theoretically, graph-based ant model formulations converge to the optimal global under certain parameter values (Gutjahr, 2000). Proof of such convergence has been previously shown for TSP formulations (Gutjahr, 2000; Stutzle and Dorigo, 2002). In this section we show convergence for WDP formulation. First, recall the following equations: p_{jh} from Algorithm 1 (Line 8); Equation 3.5 for edge weights. Additionally, recall that only a vertex $v_h \notin TL$ can be selected to construct a feasible path. Lastly, in line with our approach to pheromone updates and graph pruning we assume the following. First, we assume that in any given iteration pheromone levels on edges are bounded, $\tau_{jh}(t) \in [\tau_{min}, \tau_{max}]$. Second, an ant at any node $v_h \neq \{s,t\}$ during any iteration will have at least one edge to choose from.

Let iteration on the set of paths created by the ants t be $M(t)$ and the path representing the global optimal be M_{opt}. Further, let L denote the set of edges on the global optimal path M_{opt} and let $|L|$ be the cardinality of L, i.e. the number of edges in the path M_{opt}. Let there be N ants $(a_1, a_2, a_3..., a_N)$ traversing the graph in each iteration $t = \{1, 2, 3...\}$. The following proposition characterizes the convergence property of our algorithm.

Proposition 3 *The probability P_{opt} during iteration t, at least one ant crosses the optimal path can be made arbitrarily close to one for values of $\tau_{min}, \alpha, \beta, N > 0$.*

Proof is provided in Appendix A. This proposition highlights usefulness of TrACA as a search algorithm for WDP. In light of big data and increasing computational capabilities in business, this indicates that using our approach, convergence can be achieved within a specified amount of time, rather than increasing length of time. This is because pheromone values on edges can be used to adaptively learn and improvise the construction of optimal solution. With higher intensity of search there is improved learning of search space which helps to converge onto the optimal solution. Convergence proofs for other heuristics, such as Genetic or Memetic Algorithms rely on finding better solutions as number of iterations are increased. However, we show our graph-based system as having convergence close to optimal for specified iterations, but driven by number of ants.

3.4 Setup

We are interested in testing our algorithm by conducting experiments on open test instances. We considered CATS (Leyton-Brown et al., 2002) and the ones developed by Lau and Goh (2002). The instances in Lau and Goh (2002) are believed to be more realistic than CATS, and have been used, for example, in Guo et al. (2006), Boughaci et al. (2009), and Boughaci et al. (2010). Specifically, these instances have been artificially constructed by modeling bidder related attributes such as price sensitivity and preference. Price sensitivity models a bidder's acceptable price range for each bid and preference takes into account bidder's preferences among bids (Lau and Goh, 2002). Further, these instances are large (more than 500 bids) and unsolvable using CPLEX (CPLEX solvers usually run out of memory due to the large search tree). Testing with such realistic instances would be useful in demonstrating real value of our approach, in light of recent work in improving combinatorial auction applications in industry overall (Bichler, 2010; Bichler et al., 2006, 2009).

In our analysis, we focus only on 94 of these instances – the same ones used in Boughaci et al. (2009). We chose those specific instances so that we can execute a fair comparison with memetic algorithm results. This is because memetic algorithm is currently considered as the best-in-class heuristic for solving WDP on such hard instances and outperforms genetic algorithm implementation, Casanova and SAGII (Guo et al., 2006; Hoos and Boutilier, 2000). Table 3.1 gives a summary of these instances. Each row of Table 3.1 corresponds to one set of test instances characterized by number of items and bids (column 2 & 3). Columns 4 & 5 provide further insight into the structure of bids in each set of instances. Structure corresponds to average size of each bid (number of items per bid, column 4) and average number of bids that request each item (column 5). Structure of bids gives information regarding problem complexity (De Vries and Vohra, 2003). Problem complexity critically affects the choice of the heuristics for WDP (Leyton-Brown et al., 2000; Sandholm et al., 2005) which is why we investigate empirical hardness (Leyton-Brown et al., 2009) of TrACA in Section 3.6.

Table 3.1.: Overview of Test Instances

Test Instance Lau and Goh (2002)	# Items	# Bids	# Items/Bid (Avg.)	# Bids/Items (Avg.)	Time (1500 iterations) (Max in sec)
in101-in120	500	1000	46	57	665
in201-in220	1000	1000	76	56	402
in401-in430	1000	500	40	28	162
in501-in504	1000	1500	79	119	410
in601-in620	1500	1500	66	84	450

We set the parameters of TrACA following anytime performance measures for ant colony heuristics (Dorigo and Birattari, 2011; Dorigo and Di Caro, 1999; Dorigo and Stutzle, 2003). The standard procedure is to tune the parameters so that they achieve the known optimal. In our case, we used information theoretic method to update dynamically values of α, β. Specifically, each iteration TrACA computes an information theoretic measure (e.g., entropy) of the pheromone graph. If pheromone deposition shows increased entropy, it implies a developing bias in search and so, β (exploration) is encouraged. Conversely, decreased entropy implies increasing exploitative behavior (α). The starting parameters we obtained from benchmarking with CATS testbeds Leyton-Brown et al. (2002): $\alpha = 2, \beta = 1.5$; the number of iterations per trial run for the ant system is 1500; pheromone value on the graph at $t = 0$ is $\tau_0 = 1$ and pheromone evaporation factor is $\rho = 0.05$. Each experiment is repeated for 30 trials, with 400 for each trial and problem ant population size instance. Table 3.1 Column 6 gives the maximum runtime for TrACA for 1500 iterations, in each set of instances.

We compare solutions generated by TrACA with memetic algorithm (MA) which, to the best of our knowledge, is currently the best-in-class heuristic solving WDP for these instances. We do not have access to the code for MA and so we take the best results generated by MA, corresponding to each test instance, as mentioned in Boughaci et al. (2009), to compare. We also conduct comparison with CPLEX, although most heuristics do not compare their performance to CPLEX. For comparison with CPLEX, to keep the comparisons consistent, we solve the test instances using CPLEX solver with a specified time-limit. This time-limit is the maximum time TrACA takes to solve each set of instances. We use the solution generated by CPLEX at the end of the time-limit for comparison with TrACA. Results of comparison to CPLEX are shown in Appendix B.9.

3.5 Results & Analysis

Table 3.2.: Summary: TrACA vs Memetic Algorithm (MA). For Median Test we use Wilcoxon Rank Sum test.

Test Instance	Median Test	ISP	Z Score	Solution Quality
Lau and Goh (2002)				
in101-in120	15	0.81	-3.13	6.72%
in201-in220	17	0.89	-2.82	5.75%
in401-in430	28	0.93	-6.57	3%
in501-in504	4	0.99	-4.53	3.67%
in601-in620	18	0.95	-4.25	8.9%

Table 3.3.: Summary: TrACA vs ACO-Local Search (ACLS). For Median Test we use Wilcoxon Rank Sum test.

Test Instance	Median Test	ISP	Z Score	Solution Quality
Lau and Goh (2002)				
in101-in110	1	0.25	-0.09	3.42%
in201-in210	3	0.57	-0.47	2.54%
in401-in410	8	0.76	-0.79	0.86%
in501-in504	4	0.83	-1.53	3.65%
in601-in610	5	0.65	-0.85	4.5%

We compare TrACA performance to the benchmark algorithm MA along four specific measures. Our first measure counts the median solution – out of the 30 iterations that TrACA is run – is statistically significantly better than benchmark algorithm results. We refer to it as the Median Test. This test essentially measures the number of instances where median from TrACA results is at least as good as benchmark algorithm result. Second, we compute the probability that TrACA produces better solutions than benchmark algorithm (which we call Improved Solution Probability or ISP). We compute this by measuring the total number of times, across all iterations over a set of instances (for example, there are 20 test instances in the set in101-in120 times the 30 iterations of TrACA generates 600 solutions), TrACA produces a better result than benchmark algorithm. Third, we compute the average Z score of benchmark algorithm result. Using the standard definition of Z Score, we measure how many standard deviations the benchmark result is from the mean of TrACA results. Finally, we measure average percentage by which TrACA best solution exceeds benchmark algorithm result (which we call Solution Quality). All these measures together provide insights that help comparing TrACA against each of those benchmarks.

These measures are shown in Table 3.2 when comparing TrACA to MA. At the aggregate level, for total 77 out of 94 instances, median results from TrACA are better than best MA result.[3] Further, ISP values imply that when TrACA and MA are run for the same set of instances, likelihood of TrACA producing a better result is higher across all instances. In addition, repeated runs of TrACA produces a better distribution of results compared to the best MA result, across all instances. This result is significant from the perspective of online combinatorial auctions (Prasad et al., 2016). In the online context, fast heuristics that generate better solutions is crucial for conducting combinatorial auctions (Teich et al., 2004). Further, Hoos and Boutilier (2000) note that resource allocations in large e-commerce combinatorial auctions expect real-time responses for which heuristics that product fast and quality solutions are needed. Appendix B.4 lists the detailed comparisons between best solutions generated by TrACA against results from MA, for each of the 94 instances. For reference, we also provide box plots to show the performance comparisons for some of the instances in Appendix B.7.

[3] When analyzing the heuristic algorithms, prior works (Auger and Doerr, 2011) generally compare median results of the heuristic against a threshold – in our case, the best result from the MA as reported.

In order to establish robustness of TrACA, we analyze quality and range of solutions generated by TrACA for different numbers of ants N. We consider $N = \{100, 200, 300\}$ for analysis. Table 3.4 provides a summary of the results for these robustness checks. From a practitioner's standpoint, these results provide further evidence of TrACA's effectiveness in finding better solutions than MA in comparable timeframes. Note that Column 4 is for 400 ants, same as what is used for the analysis as shown in Table 3.2. Further note that average runtimes for 100 ants is similar to the runtimes reported for MA in Boughaci et al. (2009). This is significant considering MA is considered the best-in-class heuristic in literature currently for solving WDP using the Lau and Goh (2002) instances (Boughaci et al., 2009, 2010; Guo et al., 2006).

Table 3.4.: Summary: Performance of TrACA vs. MA, with No. of Ants = $\{100, 200, 300\}$ across all 94 instances

No. of Ants	100	200	300	400
Median Test	69	77	80	82
ISP	0.72	0.81	0.85	0.86
Z Score	-1.68	-2.4	-3.61	-3.63
Solution Quality	4.6%	5.2%	5.3%	5.67%
Avg. Time TrACA	101.8	177.6	251.6	355.8

3.6 Empirical Hardness Model for TrACA

We use the empirical hardness approach (Leyton-Brown et al., 2009) to build a predictive model of TrACA runtimes. Using this model, we investigate what features of problem instance causes the TrACA solution run-times to vary so substantially across the 94 instances solved. This analysis is useful for the following reasons. First, prediction of time needed to allocate winning bids is required to conduct more rounds in such auctions in a given time-frame (Sheffi, 2004). Run-time variability is therefore critical to practical deployment of WDP algorithms such as TrACA (Leyton-Brown et al., 2009). Second, recall from Table 3.1 that TrACA run-times vary from as low as 162 (in401-430 instances) to 665 seconds (in101-120 instances) for a pre-specified 1500 iterations. What causes the TrACA solution run-times to vary so substantially? Does the run-time variability have anything to do with number of items per bid or is it simply a function of number of items? Further, what does run-time variability say about the difficulty of WDP in such instances?

We use the standard procedure of empirical hardness approach for analyzing TrACA run-times (Leyton-Brown et al., 2002). We estimate a simple linear predictive model of TrACA run-times and characterize what features of the auctions make solving for WDP difficult. Our analysis not only helps in run-time investigation but also helps in demonstrating how TrACA is inherently well suited to solving hard instances of WDP.

3.6.1 Predictive model for TrACA run-times

Recall from Section 3.3.2 that TrACA uses a graphical formulation (directed cyclic graph) of the WDP to search for optimal solutions. Hence, any variability in run-times is a function of the complexity the graphical formulation. We use standard graph centrality measures as predictors to build a linear regression model for predicting the run-times of TrACA, as per the following equation.

$$\text{Run-times} = H_1(\text{directed cyclic graph centrality measures}) + c \tag{3.8}$$

In Equation 3.8, $H_1(.)$ are linear hypotheses of the centrality measures of directed cyclic graphs generated and c is an assumed constant. The linearity in relationship between run-times and graph centrality measures is standard practice in empirical hardness analysis (Leyton-Brown et al., 2002, 2009). Non-linear models may be explored but for simplicity we assume a linear form. For predictor variables we consider network centrality measures, as described in Table 3.5.

Table 3.5.: Predictor Variables for Run-time Prediction

Predictor Variable	Centrality Measure	Variable Symbol
Avg. In-degree	Degree Centrality	AIn_i
Avg. In-degree Closeness	Closeness Centrality	AInC_i
Avg. Out-degree Closeness	Closeness Centrality	AOutC_i
Avg. Betweenness	Betweenness Centrality	ABet_i
Clustering Coefficient (Transitivity)	Transitivity	CC_i
Eigenvalue	Eigenvector Centrality	EV_i
Avg. Eigenvector Centrality Score	Eigenvector Centrality	AEVC_i
Avg. Alpha Centrality	Katz Centrality	AKC_i
Avg. Cluster Size	Community detection in graphs	ACS_i
Standard. Deviation - Cluster Size	Community detection in graphs	SCS_i
Avg. Node Strength	Node Strength Weighted Graphs	ANS_i

Following Leyton-Brown et al. (2009), we divide the dataset into training (45 observations), validation (25 observations) and test set (20 observations). Each set is constructed such that it is a representative sample of the original dataset (Borovicka et al., 2012). The normality assumption on residuals is relaxed and so, estimation of predictor variable coefficients is done using iterated re-weighted least squares (IRLS) regression. The coefficients obtained from IRLS are shown in Table B.7 in Appendix B.6. Since sample size is small, coefficients generated from IRLS step are bootstrapped. Confidence intervals are constructed for each bootstrapped predictor variable coefficient. Finally, we measure the sensitivity of coefficients estimated using bootstrap. Essentially, we measure how each coefficient is affected by the change in the number of observations. This gives an insight about how the impact of a predictor variable may change, if more observations are added to the dataset.

Using the estimated coefficients, we use the validation and test data set to demonstrate the accuracy of the model and discuss implications of what these results mean in terms of empirical hardness of WDP problems, when solved by TrACA.

3.6.2 Bootstrapping Linear Model Coefficients

We bootstrap the IRLS estimated coefficients and obtain the following results for coefficients related to the predictor variables (Table B.8 & Figure 3.2, Appendix B.6). Number of bootstrap replicates is $R = 2000$. From analysis, it is clear that the coefficients of interest are for CC_i and $AEVC_i$. For $CC_i, AEVC_i$, the fitted normal & kernel density estimates are similar. Specifically, the two density estimates overlap over the support (x-axis). In addition, for these two predictors, the confidence interval (Table B.8 Columns 6 & 7) is asymmetric around the observed value suggesting that the inference from the bootstrap is different from the asymptotic theory, and that the estimated coefficients are likely to be more accurate in this small sample. Except $CC_i, AEVC_i$, all other predictor variables have coefficient values (within 95% CI) that vary in nature of impact. Specifically, the upper and lower limits of the confidence intervals have a positive or negative impact on runtime. This variability suggests that the effect of changes in any of these variable values (e.g., increase in AIn_i) can be instrumental in increase or decrease or even no change in TrACA runtime. Prediction of runtime using these variables can be problematic at the very least.

From Figure 3.2 it is clear that for CC_i, defined as Transitivity in directed cyclic graph centrality terms, the CI is on a negative scale. This suggests that run-times can be significantly decreased if more bids tend to cluster together. In other words, if the bid-bundle distribution is such that sets of bundles have few items in common (hence form clusters) then run-times are impacted negatively. Specifically, with an increase in variety and volume of bids submitted for bundles, likelihood of clustering of bundles cannot be ruled out. Such clustering or transitivity leads to shortened runtimes that improves TrACA performance. Specifically, with an increase in velocity of data, clustering helps solve problem of larger variety and volume of auction data.

For $AEVC_i$, defined as Average Eigenvector Centrality, the CI is on a positive scale. This suggests that run-times can increase if there are more ‘important’ bundles (vertices) connected to each other in a network. In other words, if variety of bundles

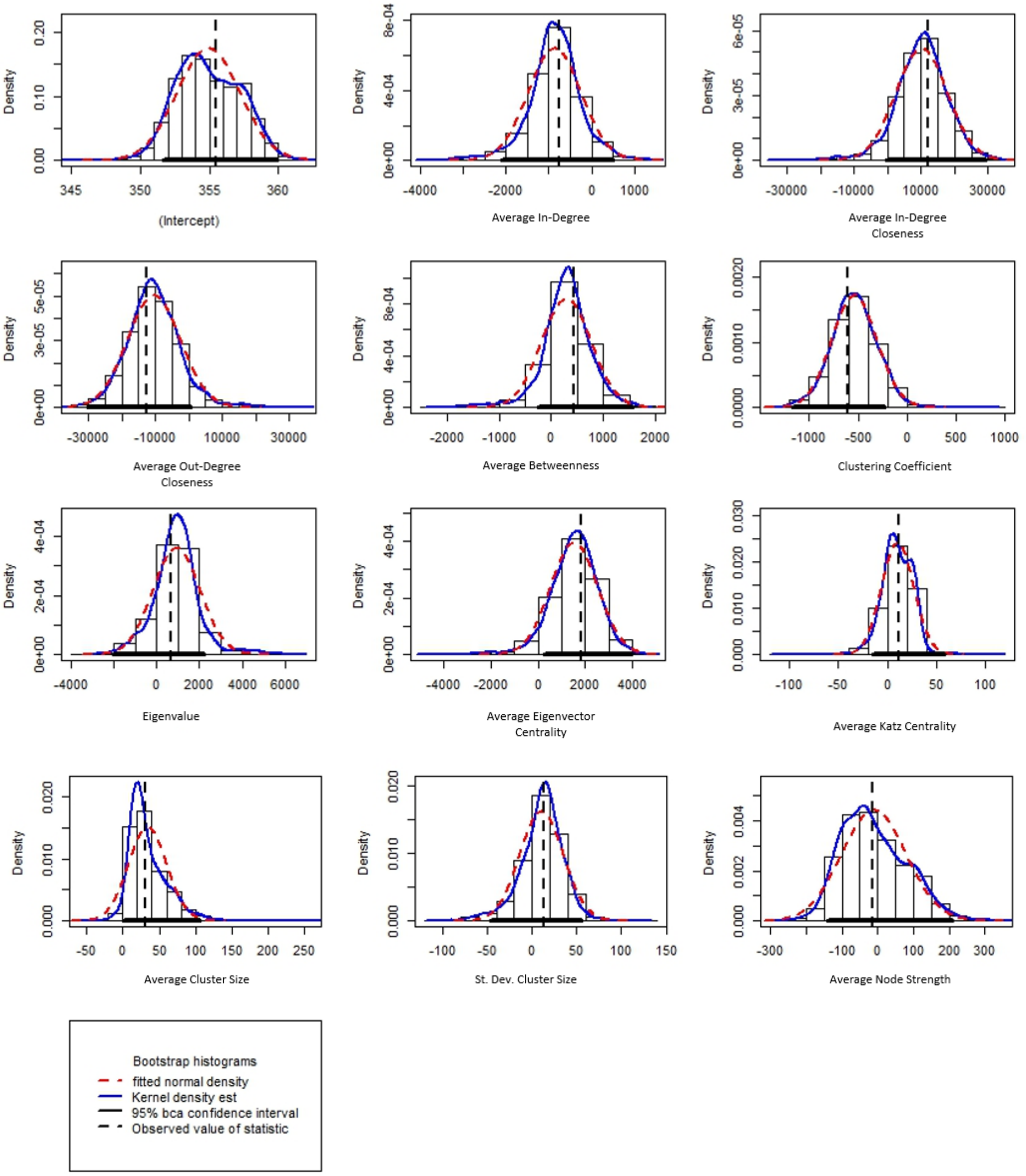

Figure 3.2.: Histogram for observed value vs. bootstrapped coefficient distribution

received is such that there are a few bundles that have less items in common with other bundles then run-times are increased. In contrast to the clustering effect, here individual bundles (vertices) gain prominence (more edges) in the directed cyclic graph. In sum, when $CC_i \& AEVC_i$ are considered together, our approach demonstrates that increase in variety of bundles shouldn't necessarily imply increased runtimes for computing winners.

We now explore the sensitivity of the bootstrapped coefficients and of the percentiles of its bootstrapped distribution to deletion of individual observations[4]. We present test results for specifically the coefficients mentioned previously e.g., AIn_i, SCS_i, CC_i, $AEVC_i$ in Figure B.1, Appendix B.6. The graph's horizontal axis, regarded as the "standardized value of the jackknife," is a reflection of each observation's impact on the coefficient. For each observation the vertical axis is positioned jackknife quantiles, calculated from those samples in bootstrap where there was no particular observation. The standard formula for the estimate is given as $\hat{\theta}_{Jack} = n\hat{\theta} - (n-1)\theta_{(.)}$ where $\hat{\theta}_{(.)}$ is is the average of these "leave-one-out" estimates.

The observation indices corresponding to the points in the graph are shown near the bottom of the plot. The key inference here is that a majority of observations have little to no effect (sensitivity) on Clustering Coefficient (CC_i). However, for $AEVC_i$, most of the observations tend to either have no effect or decrease the coefficient rather than increase it. In the Clustering Coefficient plot for example, observation 14 (Run-time 397.6 seconds) seeks to decrease value of coefficient whereas the same observation can be seen to increase coefficients for AIn_i, $AEVC_i$ and has no effect on coefficient of SCS_i. At the same time, observation 17 (Run-time 584.72 seconds) tends to increase coefficient of $AIn_i, AEVC_i, SCS_i$ and has almost no impact on CC_i. The observations that are outliers in all four plots are those that clearly impact coefficients of all these predictor variables significantly such as observations 7 (Run-time 570.78) , 19 (Run-time 626.16).

[4] using the Jack-Knife test

3.6.3 Run-time Prediction & Problem Analysis

Using the bootstrapped coefficients, we predict run-times in the validation set. Appendix B.8 gives details of predicted vs. actual run-times using Table B.9 & B.10. As evident, the predictions in validation set are approximately accurate with the minimum standard error being 1.264 and maximum being 3.285 seconds. In the final test set, standard errors on predictions marginally increase. This is to be expected since the training set had only 45 observations to use. With more data, the learning of the algorithm can be improved for better predictions.

The overarching conclusion from this analysis points to the structure of bundles and the items they have in common as an important determinant of TrACA runtime. In general, approximation of winner is computationally complex in those cases where more number of items are common among different bundles up for auction. This has been evidenced in exact approaches of solving WDP (Sandholm, 2002a; Sandholm and Suri, 2003; Sandholm et al., 2005). Specifically, exact algorithms (e.g., CPLEX) use a branch-and-bound approach that incorporates a conflict graph (has edges between bundles of items as nodes, if those bundles have items in common) for searching for optimal. Consequently, more the items in common, the denser the graph and denser the graph, more time-consuming the search (Sandholm et al., 2005). However, we show that TrACA run-times improve in such situations, given our graphical formulation. Additionally, there is a higher likelihood of better quality results for auctions that exhibit such property of bundles and items.

3.7 Extension for Multi-Unit Multi-Item CA

In this section, we extend the TrACA approach from the traditional single-unit CA to multi-unit CA. Multi-unit CAs are increasingly becoming the mechanism of choice in two major domains: cloud computing auctions and electricity markets (Bichler et al., 2010; Kwasnica et al., 2005; Sandholm, 2002b). With dynamic pricing of resources getting more common in these domains (Brena et al., 2015; Prasad et al., 2016), winner determination under time constraints and increased participation from interested bidders is poised to become an important problem to solve.

The setting for a multi-unit multi-item auction is as follows. Let $N = \{g_1, g_2, g_3, ..., g_m\}$ be a set of items. Each item $g_i \ \forall \ i \in N$ has $q(g_i)$ units of it available for auction. Consider a set of bids $B = \{b_1, b_2, b_3, ..., b_n\}$. Each bid $b_j \ \forall \ j \in B$ is a pair $(p(b_j), e(b_j))$ where $p(b_j)$ is the price offer for bundle $e(b_j) = (e(b_j)_1, e(b_j)_2, ..., e(b_j)_m)$ that consists of $e(b_j)_i \leq q(g_i)$ units of of item $g_i \ \forall \ i \in N$. An allocation is defined as a subset $S \subseteq B$ where $\sum_{b_j \in S} e(b_j)_i \leq q(g_i) \ \forall \ i \in N$. If $\hat{S}$ denotes the set of all such allocations then the multi-unit WDP is defined as computing an allocation $S \in \hat{S}$ that maximizes auctioneer's revenue $\sum_{b \in S} p(b)$. Using this formulation, TrACA is extended to search for optimal winner determination in multi-unit CA as described in the following sections.

3.7.1 Graph Construction

The graph construction is similar to single-unit CA formulation. It follows all the steps as outlined in Section 3.3.2 and additionally, has the following component that takes care of multi-unit nature of auction data. A directed edge exists between any two vertices $V \setminus \{s, t\}$ such that resource constraints are satisfied. Specifically, $E = \{(v_i, v_j) | e(b_i), e(b_j) \in V \backslash (s, t), \sum_{b_i, b_j} e(b_k)_r \leq q(g_r) \, \forall \, k \in b_i, b_j, r \in N\}$. Consider an auction for 3 items $N = \{A, B, C\}$ with 3 units of each item. The available units of each item are $q(A) = 3, q(B) = 4, q(C) = 2$. Suppose there are 5 bids submitted as follows: $b_1 = (4.2, (1, 2, 1))$, $b_2 = (5, (0, 2, 1))$, $b_3 = (4.5, (2, 3, 2))$, $b_4 = (4, (1, 2, 1))$, $b_5 = (2, (0, 2, 1))$. Using preprocessing, clearly, b_4, b_5 is inferior to b_1, b_2 respectively. Hence, the matrix from preprocessing step consists of price and bundles of three bids $b_1 = \{1A, 2B, 1C\}, b_2 = \{2B, 1C\}, b_3 = \{2A, 3B, 2C\}$. The graph constructed from this shown in Figure 3.3.

Considering availability constraints, the auctioneer is better off selling b_1, b_2 with a total revenue of $4.2 + 5 = 9.2$. The path in the graph denoting this is $s \rightarrow b_1 \rightarrow b_2 \rightarrow t \Leftrightarrow s \rightarrow b_2 \rightarrow b_1 \rightarrow t$.

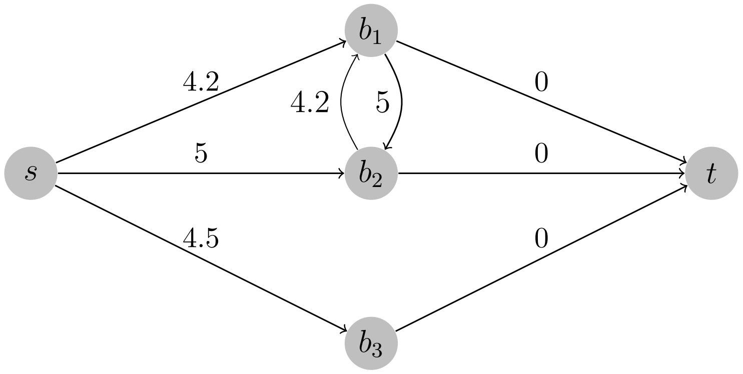

Figure 3.3.: DCG – Edges (b_i, b_j) s.t. $b_i + b_j \leq$ Capacity Constraints

3.7.2 TrACA for Multi-Unit WDP Search

The overall approach is similar to single-unit mutli-item TrACA as described in Algorithm 1 with the only difference being the additional use of capacity constraints in determining node choice. Specifically, when choosing vertex v_j from v_i (where $v_i, v_j \in V \setminus (s,t)$), if sum of units of each item requested by v_j and those in all vertices chosen in the constructed path up to v_i overshoot the capacity limit for any item, then v_j is not chosen.

Since real datasets pertaining to multi-unit CA are unavailable, we test out approach on 20 artificially prepared datasets that follow Leyton-Brown et al. (2000). Each testbed consists of 50 bids on a set of 50 items. Each bid can request anywhere between 0 to 6 copies of each item. Each item capacity varies between 100 (minimum) to 300 (maximum) units. Results from the simulation are in Table B.12 and Figure B.6, Appendix B.10. There are two key takeaways from the results. First, as indicated in Sandholm (2002b), our results show that capacity constraints on units of each item tend to limit the number of winning bids to less than half of total bids submitted. For instance, the average no. of winning bids to total bids ratio across 20 instances tested is 17.6%. Second, convergence pattern for our approach shows the inherent difficulty of solving such problems. Typically, hard multi-unit multi-item auctions have bids that tend to request a small number of units per item, independent of the total number of items (Gonen and Lehmann, 2000; Leyton-Brown et al., 2000). In our example instances, since units per item requested are 0 to 6 (compared to overall capacity of minimum 100 units/item to maximum 300 units/item), the search for optimal is harder as now more bid combinations are explored. The convergence pattern therefore shows spurts in search values that are more frequent than the single-unit multi-item cases (shown in Figure B.5, Appendix B.9). As future work, we plan to develop more realistic instances of larger sizes and add to the increasing body of work in this regard (Leyton-Brown et al., 2000).

3.8 Conclusion, Applications & Future Directions

We develop an ant colony optimization based algorithm to resolve the trade-off of speed vs accuracy for solving challenging instances of the issue of winner determination. Randomized pheromone updating and randomized graph pruning are introduced to increase the speed and quality of the search over existing ACO methods. We check our approach to the problem and compare the results with CPLEX and best-in-class search heuristic for WDP - memetic algorithm and ACLS. Although results are encouraging, we analyze TrACA for empirical hardness results and attempt at understanding the aspects of WDP that make it difficult. We find evidence of ‘tightness’ as demonstrated in multidimensional knapsack problem to be an important factor in determining complexity of WDP. Further, we establish how our graphical formulation can help in demonstrating how the problem of variety and volume can be solve in auction data. Lastly, we use a simple supervised learning model to build a predictive model of TrACA run-times and establish the accuracy of the model by predicting run-times for test set having 20 observations.

Three factors contribute to the rise in use of heuristics for WDP - (1) the increase in size of market participants, (2) in number of items (e.g., shipping route, procurement units) up for auction and (3) in usage of iterative combinatorial auctions for deciding on allocations. All three factors have become more prominent in the age of big data.

Additionally, solving the WDP involves trade-off between optimality and speed. This is where cleverly designed heuristics can provide optimal or close-to optimal solutions within pre-specified time limits (Karaenke et al., 2018). Fundamentally, heuristics facilitate opening up the market for more number of bidders, items and holding more rounds iteratively to rule out inefficient allocations – thereby increasing efficiency.

For future, we would like to direct our research in two primary directions. First, we would like to extend TrACA to solve multi-unit multi-item auctions. We are in process of building a test instances for such auctions, since these are unavailable currently for researchers (Leyton-Brown et al., 2000). Second, we would like to extend TrACA for other NP-complete problem estimations such as multi-unit multi-item CA, Vehicle Routing Problem (VRP) and modern variants of the capacity planning problem that have important applications in industry. In extending our work, our aim would be to not only improve TrACA estimations but also help improve the trade-off between efficiency and speed as much as possible.

4. INCENTIVIZING HONEST MINING IN CRYPTOCURRENCIES: AN AUTOMATED MECHANISM DESIGN APPROACH

4.1 Introduction.

Bitcoin has enjoyed tremendous popularity since 2008, as one of the first fully decentralized cryptocurrencies (Böhme et al., 2015; Nakamoto, 2008; Swan, 2015). This rise in popularity is because Bitcoin uses blockchain (a global and public data structure) to record all historical transactions between Bitcoin clients (Nakamoto, 2008). Blockchain is a way of establishing trust-less[1] transactions (Böhme et al., 2015; Nakamoto, 2008; Narayanan et al., 2016). Security of such trust-less transactions in blockchain is established using cryptographic hash puzzles, solved by a network of agents called miners (Nakamoto, 2008). For miners, solving a tough computational challenge such as a hash puzzle is a way to generate Proof-of-Work (PoW) for reaching global consensus on history of transactions in blockchain(Nakamoto, 2008; Narayanan et al., 2016). PoW demands intensive computations and hence, consumes a lot of energy (Antonopoulos, 2014; Dinh et al., 2018). Each miner incurs a computation cost and competes in a "game" to be the *first* miner to solve the puzzle and mine a block. Winning the game results in the miner getting a block fee & a transaction fee if the mined block is acknowledged by other miners as a valid block (Antonopoulos, 2014; Nakamoto, 2008; Swan, 2015). Adding a valid block to the public chain is therefore incentive-driven and helps maintain historical consensus on transactions and generate trust in the system (Böhme et al., 2015; Lewenberg et al., 2015a; Nakamoto, 2008).

[1] Trust-less is actually a misnomer. Blockchains don't eliminate trust but incentivize actions from agents to maintain trust in the system.

The conventional wisdom at the heart of mining has been that with a large population of miners and sufficiently high aggregate hash power, successful attacks on blockchain integrity (e.g., Sybil, 51 %, etc.) are next to impossible (Antonopoulos, 2014; Nakamoto, 2008). This is because honesty of miner majority is assumed (Eyal and Sirer, 2018; Kroll et al., 2013). However, recent work has shown that this assumption is erroneous. Specifically, Eyal and Sirer (2018); Kiayias et al. (2016); Sapirshtein et al. (2016) have shown that a miner can choose to be selfish while mining instead of conforming to the expected honest mining strategy and reap higher rewards. Further, selfish mining is profitable if the hash power of a miner is larger than approximately 25% of network hash rate (Eyal and Sirer, 2018; Kiayias et al., 2016). Sapirshtein et al. (2016) further show that a more *intelligent* selfish miner can lower this threshold to $\approx$ 23.21% using optimal mining strategies. Hence, even if 51% attacks may be less likely in the short run, incentives in PoW do not rule out selfish behavior from miners.

In this paper, we build on Eyal and Sirer (2018); Kwon et al. (2017); Sapirshtein et al. (2016) and provide insight towards resolving a fundamental question: *how can selfish mining tendencies be reduced in a system intended to reward honest behavior*? Given that miners are agents with private information (e.g., private chains) our approach using mechanism design seeks to prevent miners from withholding blocks and/or forking the public chain in the short run. Attempts at designing such mechanisms have been predominantly focused on improving protocols involving different proofs-of-activity (stake, space, etc.), with Eyal and Sirer (2018); Kroll et al. (2013); Sapirshtein et al. (2016) pointing out that designing consensus mechanisms that prevent selfish mining is critical to the survival of Bitcoin as a decentralized cryptocurrency. The importance of designing incentives that govern such mechanisms, however, is shown in recent studies, (Babaioff et al., 2012; Eyal, 2017; Ray et al., 2018a; Sompolinsky and Zohar, 2018). Further, Chen et al. (2019); Guerraoui and Wang (2018) show how incentives in mining can be unfair when message propagation in a distributed system is not instantaneous. Experimental evidence in

Eyal et al. (2016); Lewenberg et al. (2015b) confirm problem with existing incentives through evidence of disproportionate rewards to dishonest miners. Finally, Dong et al. (2019); Huberman et al. (2019); Jiang and Wu (2019); Kwon et al. (2017); Saad et al. (2019) show how block & transaction free structure in mining rewards in cryptocurrencies can exacerbate selfish mining attacks by introducing possibility of combining forking & block-withholding attacks. Our approach using mechanism design adds to this growing body of work to design better incentive structures for blockchain-based cryptocurrencies. Following are the main contributions of the paper:

1. A method of designing incentives that incentivize honest mining, using non-cooperative game theoretic notions, is developed. Specifically, automated mechanism design (AMD) (Sandholm, 2003) is used to formulate the problem of designing incentives that minimize price of anarchy of the blockchain system. The minimization searches for optimal payoffs that minimizes price of anarchy of mining, subject to individual rationality and incentive compatibility constraints.

2. A supervised learning model is used to study impact of miner actions on discovered optimal payoffs. Specifically, a linear regression model is used to learn the relationship between payoffs and miner actions – structure of reward and punishment – when faced with selfish mining problem.

3. Using notions from the estimated linear model, three generalized incentive schemes are designed that, under appropriate conditions show mining on a public blockchain can be dominant strategy incentive compatible. Essentially, the generalized mechanism measures the amount of inequality or ‘disorder’ a miner introduces to the system by either mining honestly, forking or withholding of blocks. Measuring the disorder informs the design of reward and punishment for incentivizing honest mining. The mechanism achieves equity in mining rewards by minimizing price of anarchy (Leme and Tardos, 2010). From a social choice theory perspective, our mechanism aims to maximize Hammond Equity

(Hammond, 1976) of a set of miners, with conflicting preferences – honest and selfish mining behavior.

The rest of the paper is structured as follows: first, in Section 4.3 we introduce the basic 2-miner model that is used to perform an AMD estimation of payoffs; Section 4.4 provides rationale for incentive structure with rewards & punishment that incentivize/disincentive honest/selfish mining actions and finally, in Section 4.5 we generalize the notions of reward and punishment from a 2-miner model to an N-miner model.

4.2 Literature Review

Decentralized digital currencies are not a new development (Chaum, 1983). In fact, such currencies have been proposed before Bitcoin, starting with Chaum (1983) and subsequently, peer-to-peer currencies have found popularity, e.g. Vishnumurthy et al. (2003); Yang and Garcia-Molina (2003). However, the earlier designs of such decentralized currencies did not have globally maintained ledger (Yang, 2010). Further, numerous cryptocurrencies followed Bitcoin's success (Mukhopadhyay et al., 2016). These cryptocurrencies are maintain a global log of transactions, which relate to the blockchain architecture. Hence, our insights apply to all such systems. To begin with, incentive driven design of currency systems have been addressed in Babaioff et al. (2012). Specifically, miners in such systems prefer to collect the transaction fee themselves to maintain the global ledger/log for transactions. However, the mining incentive mechanism in cryptocurrencies enforces a way in which provision of such incentives are driven by proof of valid miner activity such as proof-of-work, proof-of-stake etc. More formally, disseminating transactions between miners considers the problem of communication between miners and incentivizing better sharing of information. Given our focus, we consider such approaches out-of-scope for us. A recent survey (Barber et al., 2012) has identified incentive-compatibility issues as an important aspect of cryptocurrency mining. Further, Barber et al. (2012) describes possible scenarios where a single entity could control a majority of the mining power. Further, Eyal and Sirer (2018); Sapirshtein et al. (2016) analytically show a vulnerability in the incentive structure of Bitcoin. A widely cited study (Ron and Shamir, 2013) analyzed the Bitcoin transaction graph to show such vulnerabilities. As evidenced, Bitcoin had a fork in March 2013 due to a software bug (Andresen, 2013). This fork got resolved when the two of the largest pools at the time manually abandoned one branch. However, such forks are bug-induced and more generally, the resolution mechanism is fundamentally different from the intentional forks by selfish miners.

Our work is closely related to analyzing current reward mechanisms such as block & transaction fee and questioning its robustness (Babaioff et al., 2012; Chen et al., 2019; Ray et al., 2018a; Sompolinsky and Zohar, 2018). It has been noted in recent studeis that (Eyal, 2017; Tapscott and Tapscott, 2016) that mining rewards need further analysis in order to ensure incentives are aligned with the objective of a decentralized currency system. Using our mechanism, we aim at solving this problem by designing mechanisms that incorporate rewards and punishments (Andreoni et al., 2003; Masclet et al., 2003; Sefton et al., 2007; Walker and Halloran, 2004) for eliciting desired behavior. In particular, our approach relates to using a system of rewards and punishments with incomplete information from participating agents (Dellarocas, 2005; Green and Laffont, 1986; Li et al., 2017a; Liu et al., 2018). Such incomplete information may present moral hazard situations (Dellarocas, 2005) or opportunities for arbitrage (Levy et al., 2017; Liu et al., 2018). In blockchain however, private information in the form of private chains present opportunities to earn more in the short term and have long term consequences on the history of transactions. Our work therefore contributes to this gap in the literature when it comes to analyzing and designing mechanisms for blockchain based mining activities.

4.3 Model

Consider a mining game G_m with two selfish miners M_1, M_2 (with computational power m_1, m_2 respectively, $m_1 \neq m_2$) mining at the head of a public blockchain of length L_p. Following the competing selfish miners model (Eyal and Sirer, 2018; Kiayias et al., 2016; Sapirshtein et al., 2016) assume both miners decide to either follow an *immediate* or a *strategic* release strategy for newly mined blocks. Specifically, each round each miner competes to mine a block and decides to either immediately release the newly mined block to augment the public blockchain (S_l) or strategically release the block – augments private chain with newly mined block to either immediately fork the public chain (S_p) or wait to fork in the future (S_w). Assume that miners private chain lengths of n_1, n_2 respectively is private information and the distribution of private chain lengths is common knowledge. Since there are 4 states of the world corresponding to private chain lengths of each miner – $\xi = \{(n_1, n_1), (n_1, n_2), (n_2, n_1), (n_2, n_2)\}$ assume the following joint prior: $P(n_1, n_1) = \mu_1, P(n_1, n_2) = P(n_2, n_1) = \mu_2, P(n_2, n_2) = \mu_3$ such that $\mu_1 + \mu_3 + 2\mu_2 = 1$.

Definition 4.3.1 *For mining game G_m, the Bayes Nash Equilibria (BNE) are $((S_p, S_p),$ $(S_p, S_p))$ and $((S_w, S_w),$ $(S_w, S_w))$ – Strategic Release Strategy.*

Definition 4.3.2 *For mining game G_m, the optimal outcome is when both miners follow $((S_l, S_l), (S_l, S_l))$ – Immediate Release Strategy.*

Definitions 4.3.1, 4.3.2 are derived from established work on selfish mining games (Eyal and Sirer, 2018; Kiayias et al., 2016; Sapirshtein et al., 2016) and from the protocols such PoW (Proof-of-Work) or PoS (Proof-of-Stake)(Bentov et al., 2014). Specifically, given private information (private chain lengths), miners decide on immediate or strategic release of mined blocks in order to maximize payoff. For instance, forking the public chain gives higher short-term payoff than adding a block to the public chain (Eyal and Sirer, 2018; Kiayias et al., 2016). Miners can withhold blocks and either fork immediately or in the future to reap higher payoffs (Sapirshtein et al., 2016).

4.3.1 Mining Incentive Structure Formulation

For designing payoffs that incentivize immediate and discourage strategic release decisions, assume payoff structure as in Equation 4.1. Expected payoff $E^{n_1,n_2}_{S_1,S_2}$ is a function of computational powers m_1, m_2 and function $V^{\mathrm{s}}(\Delta n, \Delta L)\ \forall\ \mathrm{s} \in \{\mathrm{Win}, \mathrm{Loss}\}$ that takes two inputs: absolute difference in lengths of private chains ($\Delta n = |n_1 - n_2|$) and number of blocks (ΔL_1 or ΔL_2) by which the public blockchain is extended by the winning miner (miner 1 or 2), by beginning next round. Let $\delta_{12} \equiv |n_1 - n_2|$ represent the absolute difference in lengths of private chains when considering payoff for miner 1. Expected payoff for miner 1 is therefore:

$$E^{n_1,n_2}_{S_1,S_2} = \frac{m_1}{m_1 + m_2} V^{\mathrm{win}}(\delta_{12}, \Delta L_1) + \left(1 - \frac{m_1}{m_1 + m_2}\right) V^{\mathrm{loss}}(\delta_{21}, \Delta L_2) \tag{4.1}$$

where $S_1, S_2 \in \{S_p, S_w, S_l\}$.

Equation 4.1 has the following key interpretations. First, it is assumed that miners are rational agents and use expected payoffs for choosing to act honestly or selfishly. In practice, this assumption is due to mining being a highly stochastic endeavor where mining difficulty is adjusted periodically as a function of amount of hashing power deployed by the network of miners (Antonopoulos, 2014; Böhme et al., 2015; Swan, 2015). Moreover, surveys have shown that large mining pools run mining using large scale computational resources and decide course of action based on *probability* of winning, since each round is not a guaranteed win (Bag and Sakurai, 2016; Böhme et al., 2015; Taylor, 2013). Uncertainty of winning coupled with rationality allows use of expected payoff for choosing actions, in our formulation.

Second, the structure of Equation 4.1 assumes a payoffs for winning and losing. In practice, losing miners get nothing but bear the cost of mining (Böhme et al., 2015; Nakamoto, 2008). However, our formulation accounts for the negative externality of selfish mining on losing miners using the V^{loss} function. In doing so, as demonstrated in following sections, Equation 4.1 allows for introducing incentive structures that reward desired and punish undesired behaviors for actions taken by miners (Andreoni et al., 2003; Masclet et al., 2003; Sefton et al., 2007; Walker and Halloran, 2004).

4.3.2 Automated Mechanism Design Formulation

Using the standard AMD approach (Sandholm, 2003), the following aspects of the problem are defined:

- Set of miners M_1, M_2.
- Set of types of miner $\Theta \in \{n_1, n_2\}$.
- Joint Prior: $P(n_1, n_1) = \mu_1, P(n_1, n_2) = P(n_2, n_1) = \mu_2, P(n_2, n_2) = \mu_3$ such that $\mu_1 + \mu_3 + 2\mu_2 = 1$.
- A finite set of outcomes $O \Rightarrow$ change in public blockchain length:

  $$O \in \{0, 1, n_1 + 1, n_2 + 1\}.$$

  Here, 0 corresponds to block-withholding BNE $((S_w, S_w), (S_w, S_w))$, 1 corresponds to honest mining and $\{n_1 + 1,\ n_2 + 1\}$ corresponds to forking BNE $((S_p, S_p), (S_p, S_p))$.
- Ex-post IR constraints.
- Bayesian Nash IC constraints.

For ex-post IR constraints it is assumed that payoffs for either miner 1 or 2 is such that $V^k(\Delta n, \Delta L) \geq 0 \ \forall \ k \in \{\text{win}, \text{loss}\}$. The BN-IC constraints are derived for each BNE and are shown as follows: The Bayes Nash-Incentive Compatibility constraints are shown as follows:

$$\mu_1 \left(E^{n_1,n_1}_{S_p,S_p}\right) + \mu_2 \left(E^{n_1,n_2}_{S_p,S_p}\right) \geq \mu_1 \left(E^{n_2,n_1}_{S_p,S_p}\right) + \mu_2 \left(E^{n_2,n_2}_{S_p,S_p}\right) \tag{4.2}$$

$$\mu_2 \left(E^{n_2,n_1}_{S_p,S_p}\right) + \mu_3 \left(E^{n_2,n_2}_{S_p,S_p}\right) \geq \mu_2 \left(E^{n_1,n_1}_{S_p,S_p}\right) + \mu_3 \left(E^{n_1,n_2}_{S_p,S_p}\right) \tag{4.3}$$

$$\mu_1\left(E^{n_1,n_1}_{S_w,S_w}\right)+\mu_2\left(E^{n_1,n_2}_{S_w,S_w}\right)\geq\mu_1\left(E^{n_2,n_1}_{S_w,S_w}\right)+\mu_2\left(E^{n_2,n_2}_{S_w,S_w}\right) \tag{4.4}$$

$$\mu_2\left(E^{n_2,n_1}_{S_w,S_w}\right)+\mu_3\left(E^{n_2,n_2}_{S_w,S_w}\right)\geq\mu_2\left(E^{n_1,n_1}_{S_w,S_w}\right)+\mu_3\left(E^{n_1,n_2}_{S_w,S_w}\right) \tag{4.5}$$

The BNE Constraints are:

$$\mu_1\left(E^{n_1,n_1}_{S_p,S_p}\right)+\mu_2\left(E^{n_1,n_2}_{S_p,S_p}\right)\geq\mu_1\left(E^{n_1,n_1}_{S_w,S_p}\right)+\mu_2\left(E^{n_1,n_2}_{S_w,S_p}\right) \tag{4.6}$$

$$\mu_1\left(E^{n_1,n_1}_{S_p,S_p}\right)+\mu_2\left(E^{n_1,n_2}_{S_p,S_p}\right)\geq\mu_1\left(E^{n_1,n_1}_{S_l,S_p}\right)+\mu_2\left(E^{n_1,n_2}_{S_l,S_p}\right) \tag{4.7}$$

$$\mu_1\left(E^{n_1,n_1}_{S_w,S_w}\right)+\mu_2\left(E^{n_1,n_2}_{S_w,S_w}\right)\geq\mu_1\left(E^{n_1,n_1}_{S_p,S_w}\right)+\mu_2\left(E^{n_1,n_2}_{S_p,S_w}\right) \tag{4.8}$$

$$\mu_1\left(E^{n_1,n_1}_{S_w,S_w}\right)+\mu_2\left(E^{n_1,n_2}_{S_w,S_w}\right)\geq\mu_1\left(E^{n_1,n_1}_{S_l,S_w}\right)+\mu_2\left(E^{n_1,n_2}_{S_l,S_w}\right) \tag{4.9}$$

Further, Equations 4.6-4.9 show BNE constraints that should for each equilibrium as defined in Definitions 4.3.1 & 4.3.2. Since it is desired that miners have lower tendency to mine on private chains and greater tendency to mine on the public chain, the objective function should essentially compare and incentivize the honest outcome over others. That is, instead of *benevolence* or *self-interested* objectives (Dash et al., 2003; Sandholm, 2003), the designer's objective is to promote one outcome over all others. By construction, the desired equilibria occurs when both miners play S_l. However, the welfare of this equilibria is degraded by selfish mining that occurs when either S_p or S_w is played. Hence, the objective of the mechanism is to minimize the Bayes Nash Price of Anarchy (BN-PoA)[2]. BN-PoA is considered for two cases: when either forking $((S_p,S_p),(S_p,S_p))$ or block-withholding $((S_w,S_w),(S_w,S_w))$ is the worst equilibrium.

$$\Phi_1^{S_p}=\frac{U^1_{n_1,S_p}+U^1_{n_2,S_p}+U^2_{n_1,S_p}+U^2_{n_2,S_p}}{U^1_{n_1,S_l}+U^1_{n_2,S_l}+U^2_{n_1,S_l}+U^2_{n_2,S_l}} \tag{4.10}$$

$$\Phi_1^{S_w}=\frac{U^1_{n_1,S_w}+U^1_{n_2,S_w}+U^2_{n_1,S_w}+U^2_{n_2,S_w}}{U^1_{n_1,S_l}+U^1_{n_2,S_l}+U^2_{n_1,S_l}+U^2_{n_2,S_l}} \tag{4.11}$$

[2] Bayes Nash Price of Anarchy is applicable to designing games where agents have imperfect information(Roughgarden, 2012).

Equations 4.10, 4.11 are BN-PoA expressions when forking and block-withholding are the worst equilibrium, respectively. $U^i_{n_j,S_p}$ is the overall expected utility for miner i, with private chain length n_j in the $((S_p,S_p),(S_p,S_p))$ equilibrium. The AMD problem that searches for optimal payoffs $E^{n_i,n_j}_{S_i,S_j}$ can then be stated as follows, in equations 4.12 & 4.13:

$$\begin{aligned} \underset{E^{n_i,n_j}_{S_i,S_j}}{minimize} \quad & \frac{U^1_{n_1,S_p}+U^1_{n_2,S_p}+U^2_{n_1,S_p}+U^2_{n_2,S_p}}{U^1_{n_1,S_l}+U^1_{n_2,S_l}+U^2_{n_1,S_l}+U^2_{n_2,S_l}} \\ \text{subject to} \quad & \text{BN IC Constraints (4.2-4.5)}, \\ & \text{IR Constraints}, \\ & \text{BNE Constraint}, \\ & E^{n_i,n_j}_{S_i,S_j} \ \forall \ S_i,S_j \in \{S_p,S_w,S_l\},(n_i,n_j) \in \{1,2,3,...\} \end{aligned} \tag{4.12}$$

$$\begin{aligned} \underset{E^{n_i,n_j}_{S_i,S_j}}{minimize} \quad & \frac{U^1_{n_1,S_w}+U^1_{n_2,S_w}+U^2_{n_1,S_w}+U^2_{n_2,S_w}}{U^1_{n_1,S_l}+U^1_{n_2,S_l}+U^2_{n_1,S_l}+U^2_{n_2,S_l}} \\ \text{subject to} \quad & \text{BN IC Constraints (4.2-4.5)}, \\ & \text{IR Constraints}, \\ & \text{BNE Constraint}, \\ & E^{n_i,n_j}_{S_i,S_j} \ \forall \ S_i,S_j \in \{S_p,S_w,S_l\},(n_i,n_j) \in \{1,2,3,...\} \end{aligned} \tag{4.13}$$

Note that $E^{n_i,n_j}_{S_i,S_j}$ are treated as variables for optimization. The optimal payoffs are used to search for functional forms for $V^{\text{win}}, V^{\text{loss}}$. Estimating the functional forms serves two objectives: first it helps in identifying impact of changing private and public chain lengths on $E^{n_i,n_j}_{S_i,S_j}$ and second, it helps in identifying incentives each agent should be given to reduce selfish behavior in the system. Indirectly, reduction in selfish behavior leads to an improvement/minimization in the price of anarchy. Past work in transportation systems deals with similar notions of improving price of anarchy measures through modifying underlying mechanisms or incentives (Cominetti et al., 2009; Youn et al., 2008; Zhang et al., 2018). In our case, since it is unclear how optimal payoffs should incentivize honest increments in $\Delta n, \Delta L$, we bound/minimize the price of anarchy by identifying the optimal payoffs and then searching for the functional form.

4.4 Empirical Estimation of Payoff Function

We use standard R optimization library Rsolnp (Ghalanos and Theussl, 2012) for minimizing $\Phi_1^{S_p}$, $\Phi_1^{S_w}$. Specifically, for 20 variables involved in each of the minimization problems, the optimal values are used for empirically estimating impact of changing private and public chain lengths on designed incentives. Our formulation assumes separate payoff functions for win and loss for miners – $V^{\text{win}}, V^{\text{loss}}$. For simplicity and keeping focus on structural relationships, a linear functional form is assumed as follows.

$$V^{\text{win}} = e_0 + e_1\delta_{12} + e_2\Delta L_1 \tag{4.14}$$

$$V^{\text{loss}} = k_0 + k_1\delta_{21} + k_2\Delta L_2 \tag{4.15}$$

Clearly, assumption of linearity for payoff functions is an approximation. Such approximations may not serve to identify the exact structure of incentives but gives an estimate of how changes in private and public chain impact designing payoffs. Further, in order to estimate payoff functions separately, it is assumed that the expected payoff can be proportionately divided into two parts, given hash powers m_1, m_2. Using this, we separately estimate the win and loss functions and analyze the impact of $\delta_{12}, \delta_{21}, \Delta L_1, \Delta L_2$ on wins or losses incurred. The data is formed from randomly sampling $200,000$ values generated from $200,000$ optimization trials with: random starting points, proportional hash power, private chain lengths, priors on both miners. For ease of convergence of gradient descent, dependent and independent variables are scaled to between $[0, 1]$. Scaling of variables has no limiting consequences and is done to ensure that the choice of arbitrary bounds in optimization does not impact estimation of coefficients.

For the case where $((S_p, S_p), (S_p, S_p))$ is the worst equilibrium, insights are as follows: coefficients for private chain length differences in win and loss – δ_{12}, δ_{21} – as well as public chain additions – ΔL_1, ΔL_2 – are negative ($e_1 = -0.082$ $(p < 0.01), k_1 = -0.181$ $(p < 0.01), e_2 = -0.072$ $(p < 0.01), k_2 = -0.058$ $(p < 0.01)$). Negative coefficients implies punishment for mining activity using private chains. More precisely, our designed incentive penalizes winning miner when increasing public chain length using private chain and prevents free-riding by the losing miner. The winning miner decides between forking, withholding and honest mining by comparing payoffs. With negative coefficients on $\delta_{12}, \Delta L_1$, winning miner suffers the most when forking the chain and the least when mining honestly. Relatedly, the losing miner incurs changes in private chain length depending on action by the winning miner. In order to prevent losing miner from benefiting from selfish actions of the winner, negative $\delta_{21}, \Delta L_2$ coefficients ensure no such *free-riding* happens[3]. Essentially, this incentive design discourages any strategy of forking using private/hidden information by penalizing the amount with which the private information could harm or benefit other miners. From a public goods perspective, using private chains of lengths > 1, for augmenting public chain exerts negative externality on other miner. The penalty on using private chains is therefore a *tax* the selfish miner pays. Further, intercepts e_0, k_0 when estimating $V^{\text{wins}}, V^{\text{loss}}$ are positive ($e_0 = 0.243$ $(p < 0.01), k_0 = 0.155$ $(p < 0.01)$) – indicating fixed positive payoffs (e.g., block payoff) are important to incentivize individually rational mining behavior.

For the case where $((S_w, S_w), (S_w, S_w))$ is the worst equilibrium, insights are as follows: coefficients for private chain length differences in win and loss – δ_{12}, δ_{21} – are negative whereas public chain additions – ΔL_1, ΔL_2 – are positive ($e_1 = -0.047$ $(p < 0.01), k_1 = -0.072$ $(p < 0.01), e_2 = 0.326$ $(p < 0.01), k_2 = 0.139$ $(p < 0.01)$). In other words, withholding blocks is penalized whereas increments in public chain lengths is not. This intuitively follows from: (1) forking is not the worst in terms of miner welfare considering private and public chain length changes and, (2) simply withholding

[3] Free-riding is a common problem in private provisions of public good (Bergstrom et al., 1986). Penalizing gains in private information from public provisions keeps free riding incentives unattractive.

blocks isn't necessarily harmful for other miners, as long as the withheld blocks are not used to augment public chain. Here too, *free-riding* by the losing miner is prevented by penalizing changes in private chain length δ_{21}. Intuitively, our mechanism mirrors notions from VCG or Clarke Tax (Dash et al., 2003; Ephrati and Rosenschein, 1991) for autonomous agents. Considering the public blockchain as a public good, each miner is taxed for the externality (mined blocks to add to the public chain) it introduces when contributing to the chain using selfish or honest behavior. If the externality is worst when forking the public chain, the tax extracts part of payoff from both the winning and losing miners and if the externality is worst when withholding blocks with no impact on public chain, the tax extracts part of payoff for withholding blocks.

Proposition 2 *Consider the two miner scenario and suppose marginal penalty/tax on change in private chain length is made higher than that of change in public chain length, when a miner wins. Then if* $1 \leq n_2 < n_1 \leq 2n_2$, *miner* 1 *with private chain length* n_1 *has* S_l *as the dominant strategy. Further, when* $n_1 = n_2$, (S_l, S_l) *is the dominant strategy equilibrium.*

The intuitive implication from Proposition 2 is that if miners are faced with the prospect of getting penalized for increments on their private chain lengths more than on working on the public chain, then honest mining can be incentivized for those miners who have longer private chains. This builds on the discussion of selfish mining strategy in Eyal and Sirer (2018). Specifically, Eyal and Sirer (2018) shows that selfish miners tend to work on private chains if there is a possibility of controlling the longest chain by adding their private blocks. In doing this, selfish miners always try to keep ahead of number of blocks mined by the honest majority, since maintaining longer private chain provides an opportunity of forking the public chain. By penalizing such selfish behavior, we show that any work on increments on private chains can be disincentivized and public chain mining can be incentivized.

Corollary 2 *Suppose* $1 \leq n_1 < n_2$. *Then augmenting private chain length is the dominant strategy for miner* 1. *However, once* $1 \leq n_2 \leq n_1 \leq 2n_2$, *working on public chain is the dominant strategy.*

This further provides intuition of strategy followed by miner 1 who has shorter private chain length. In such a scenario, even if miner 1 works on a private chain and increments its length, on reaching or exceeding the chain length of other miner 2 then S_l becomes the dominant strategy (following Proposition 2). Hence, private chain lengths do not provide incentive to selfish miners to fork the public chain.

4.5 Generalization of Designed Incentives

In this section, the discovered mechanism/incentive scheme from Section 4.3 is generalized to $N > 2$ miners. A *direct* mechanism is assumed that requires miners to report their private information (private chain lengths)[4]. The mechanism then waits for Proof-of-Work to be generated, following which, depending on action taken by winning miner, payoffs are awarded to the winner along with any to losing miners. Every other parameter for a miner, e.g., computational power, is assumed to be public information. Using the general definition of mechanism design problems (Nisan, 1999), following are the components of the mechanism for N miners with mining powers given by the vector $M = \{m_1, m_2, ..., m_N\}$:

1. Private chain lengths: $X = \{n_1, n_2, n_3, ..., n_N\}$ such that $n_i \in (1, \eta)$ $\forall$ $i \in N$. These are private types for miners. Each miner reports this length to the mechanism each round, irrespective of win or loss.

2. Assume the same game and action space for the miners as in Section 4.3, i.e., $A_i = \{S_p, S_w, S_l\}$. As in Section 4.3, each round miners are trying to mine a single block and on winning the round can either: fork the public chain S_p, or

[4] Using revelation principle (Dasgupta et al., 1979; Green and Laffont, 1977; Myerson, 1979), we restrict our search to mechanisms in which agents report their private information to the mechanism designer.

withhold block and add to private chain S_w or add to public chain to increment public chain length by 1, i.e. honest mining S_l.

3. Set of outcomes O is related to actual observed public chain increments ΔL and is defined as $O \in \{n_i + 1, 0, 1\} \; \forall \; i \in N$ where n_i is the *reported* private chain length of the winning miner i who forks the chain (S_p), 0 is when the winning miner decides to build private chain (S_w) and 1 is honest mining outcome (S_l). Note that by construction, $\Delta L = n_i + 1$ in the case of forking accounts for the *reported* private chain length n_i of the miner along with the newly mined block. Hence, any forking that results in a public chain increment that is actually different from reported n_i length is deemed infeasible by the mechanism[5].

4. Each miner's utility is given by:

$$u_i = \underbrace{g^{\text{win}}(\Delta n_i^{\text{win}}, \Delta L^{\text{win}})}_{\text{Expected Payoff from Win}} + \underbrace{g^{\text{loss}}(\Delta n_i^{\text{loss}}, \Delta L^{\text{loss}})}_{\text{Expected Payoff from Loss}} - \underbrace{c(m_i)}_{\text{Cost of Mining}} \tag{4.16}$$

   where $\Delta L^{\text{win}}, \Delta L^{\text{loss}}$ have the same interpretation as in Section 4.3. However $\Delta n_i^{\text{win}}, \Delta n_i^{\text{loss}}$ needs reinterpretation from $N > 2$ miners perspective. Further, in keeping with all-pay contest theory (Siegel, 2009) and reality of mining in cryptocurrency systems (Antonopoulos, 2014; Swan, 2015), assume that each round all miners incur the convex and non-decreasing cost $c(m_i)$ of mining irrespective of win or loss. Further, similar to Section 4.4 assume that it is individually rational for miners to mine every round, i.e., $g^{win}(\Delta n_i^{\text{win}}, \Delta L^{\text{win}}) + g^{loss}(\Delta n_i^{\text{loss}}) \geq c(m_i)$.

5. Assume existence of a decision rule $d : n_i \rightarrow O$ that takes reported private chain length as inputs from winning miner i (given private chain length n_i) and maps outcome of public chain length increment. As before, the designer considers the desirable outcome as honest mining (S_l) and all other outcomes as

[5] Recent mining attacks such as Stubborn Mining (Nayak et al., 2016; Wang et al., 2019) do analyze cases where selfish miners partially reveal private chains but augment public chain with different length. Our mechanism essentially treats any such action by miners as infeasible.

undesirable (S_p, S_w). In doing so, the designer is assumed to be minimizing N agent Price-of-Anarchy (Leme and Tardos, 2010) or maximizing Hammond Equity (Hammond, 1976) of the system. Hammond Equity captures the notion of reducing inequality by enforcing certain constraints. Generally, the constraints relate to the recipient's utility gain and it is ensure that this utility gain is equal to the donor's utility loss. Similar notions have been used in recent literature (Asheim et al., 2016; De and Mitra, 2017; Mariotti and Veneziani, 2017; Moulin, 2017).

It is clear that computing Δn in a multi-player case needs reformulation. In a two player case, Δn is simply absolute difference between the private chain lengths. However, extending this definition to multiplayer could be done in a variety of ways that preserve decision-making elements from a miner's perspective and also simplify mathematical analysis. In other words, extending definition of Δn to multi-player scenario while ensuring mathematical tractability should ensure that the mechanism makes miners take into account differences between self and other private chain lengths before acting selfishly (forking, block-withholding) or honestly. Hence, two main definitions of Δn are considered: (1) $\Delta n_i^s = |n_i^s - \min(X^s)|, \ \forall \ i \in N, \ s \in \{\text{win}, \text{loss}\}$, (2) $\Delta n_i^s = \left| n_i^s - \tilde{X} \right| \ \forall \ i \in N, \ s \in \{\text{win}, \text{loss}\}$. In words, first definition compares $i's$ private chain length (on win or loss) and minimum of all other miner's private chain lengths; second definition considers $i's$ private chain length (on win or loss) and median of all miner's private chain lengths. Simulation is used to test the efficacy of both definitions of Δn. Theoretical analysis is done only for the first definition. Expanding on the first definition, following is $\Delta n_i^{\text{win}}, \Delta n_i^{\text{loss}}$:

$$\Delta n_i^{\text{win}} = |n_i^{A_i} - \min(X')| \ : \ X' = X \setminus \{n_i\} \tag{4.17}$$

$$\Delta n_i^{\text{loss}} = |n_i - \min(X'')| \ : \ X'' = X \setminus \{n_j\}. \ j \neq i \tag{4.18}$$

where $A_i \in \{S_p, S_w, S_l\}$ and $n_i^{A_i} \in \{0, n_i + 1, n_i\} \ \forall \ A_i \in \{S_p, S_w, S_l\}$. In other words, $n_i^{S_p} = 0$ when miner i wins and forks (S_p), $n_i^{S_w} = n_i + 1$ when miner i wins and builds private chain (S_w) and $n_i^{S_l} = n_i$ when miner i wins and mines honestly (S_l). Note that X', X'' is the set of private chain lengths of all other miners, after miner i suffers a win or loses to miner j respectively. More precisely, if miner i wins then $X' \equiv X \setminus \{n_i\}$ whereas a loss gives $X'' \equiv X \setminus \{n_j\}$ where j is the miner who wins instead of miner i. Since each miner is deciding between selfish and honest behaviors, each possible winner of a mining round chooses between the actions based on the following expected payoffs:

$$u_i^{S_p} = g^{\text{win}}(|\min(X')|, n_i + 1) + g^{\text{loss}}(|n_i - \min(X'')|, \Delta L'') - c(m_i) \tag{4.19}$$

$$u_i^{S_w} = g^{\text{win}}(|n_i + 1 - \min(X')|, 0) + g^{\text{loss}}(|n_i - \min(X'')|, \Delta L'') - c(m_i) \tag{4.20}$$

$$u_i^{S_l} = g^{\text{win}}(|n_i - \min(X')|, 1) + g^{\text{loss}}(|n_i - \min(X'')|, \Delta L'') - c(m_i) \tag{4.21}$$

where $\Delta L''$ is increment in public chain length after miner loses to miner j. In the following subsections, we give structure to the expected payoff functions to formulate incentives that make honest mining a weakly dominant strategy.

4.5.1 Additively Separable Incentives

Without loss of generality, assume an additively separable structure of $g^s(\Delta n_i^s, \Delta L^s)\ \forall\ s \in \{\text{win}, \text{loss}\}$ as $g^{win}(\Delta n_i^{win}, \Delta L^{win}) = h_1(\Delta L^{win}) + h_2(\Delta n_i^{win})$, $g^{loss}(\Delta n_i^{loss}, \Delta L^{loss}) = h_3(\Delta L^{loss}) + h_4(\Delta n_i^{loss})$. Further, assume $h_1(.), h_2(.)$ are concave utility functions on finite outcome sets $K_1 = \{0, n_i + 1, 1\}$, $K_2 = \{|n_i^{S_p} - \min(X')|, |n_i^{S_w} - \min(X')|, |n_i^{s_l} - \min(X')|\}$ respectively, that represent outcomes from chain increments ΔL^{win}, Δn^{win} respectively. In addition, to prevent free-riding, assume payoff from win dominates payoff from loss. Additive separability is a common structure of utility functions, widely used in modeling utility functions of agents in public goods economics (Azevedo et al., 2013; Bergstrom et al., 1986) and finite goods consumption models(Gorman, 1968a,b). Similarity between public goods and blockchain has been noted in Davidson et al. (2016); Glaser (2017); Kewell et al. (2017). First, the public ledger feature and value to all users from rule & history consensus of blockchain, especially in cryptocurrency applications, has been compared to externality of public good consumption (Casey and Vigna, 2018; Tapscott and Tapscott, 2016). Second, miners support provision of public good through private effort/provision(Narayanan et al., 2016). That is, block payoff is private consumption for the miners for winning mining round for providing services to execute transactions through the system.

Assume each miner i is able to preference order payoffs $\succ_i$ based on publicly observable outcome – public chain increment – and private chain increments, from taking actions S_p, S_w, S_l. Further, assume that the preference ordering is complete, transitive and reflexive. Since the mechanism requires miners to report private chain length each round, preference ordering on outcomes assumes miners know that on winning, how each action would change public and private chain lengths. Clearly, the ordering depends on the how $\Delta n^{win}, \Delta L^{win}$ impacts utility of the miner. Extending function insights of V^{win}, V^{loss} from section 4.4 following are defined for $\Delta n^{win}, \Delta n^{loss}$ and functions h_1, h_2:

Definition 4.5.1 ***Zero Minimum Rule****: Δn_i is defined as:*

$$\Delta n_i^{\text{win}} = \begin{cases} 0, & A_i = S_p \\ n_i + 1, & A_i = S_w \\ n_i, & A_i = S_l \end{cases} \tag{4.22}$$

$$\Delta n_i^{\text{loss}} = n_i \ \forall \ A_i \tag{4.23}$$

such that $\min(X') = \min(X'') = 0$.

Zero minimum rule essentially allows the mechanism to compare each miner's reported private chain length to the ideal case: zero private chain length (Gramoli, 2017; Natoli and Gramoli, 2016). In doing so, the mechanism simplifies measurement of differences in private chain length for a winning miner, in any given round. Essentially, the mechanism tracks each individual miner's change in private chain length without involving other miners private chain information.

Definition 4.5.2 ***Public Chain Dominance****: Payoff from unit increment in public chain dominates payoff from unit increment in private chain:* $h_1(1) - h_1(0) \geq h_2(1) - h_2(0)$.

Public chain dominance follows from notions of discovered payoff structure of winning miner, as explained in Section 4.4. Specifically, each round winning miner considers payoff between increments in public or private chain and as shown in 2 miner simulations in Section 4.4, incentivizing public over private chain increments can help incentivize honest mining.

Proposition 3 *Any winning miner with private chain length* $n_i > 0$, S_l *is a weakly dominant strategy under Zero Minimum Rule and Public Chain Dominance. Further, a mechanism with such payoffs is strategy-proof.*

Proposition 3 provides intuition of generalizing the two-miner mechanism in Section 4.4 to N miners. More formally, using concave payoff on discrete and finite outcome sets, it is shown that honest mining is the weakly dominant strategy for any given miner having non-negative reported private chain length. The way the mechanism implements this is using two comparisons: first, by comparing between increments to private chain and second, between increments to public chain. These comparisons enable the mechanism to penalize large increments and reward shorter (honest) increments. Specifically, the mechanism has the highest reward for unit increment to the public chain and zero increment to private chain. In this way, any miner is incentivized to reduce augmenting private chain length and add one block to the public chain on winning a round. Note that by assuming concavity of payoffs, this generalized mechanism improves on the incentives designed in the two-miner case in Section 4.4. Specifically, concavity improves on the linear payoff structure and helps in enabling honest mining be a dominant strategy, irrespective of declared private chain length.

It is also clear from the proposition that miners have no incentive misrepresenting their private information. That is, no miner is better off reporting a higher or lower private chain length or false action. This is a result of the single-peaked nature of payoffs (resulting from concavity of $h_1(.), h_2(.)$) for any miner that wins a round. Even if a miner reports an action $A_i^{'}$ instead of action A_i, taking any action that extends public blockchain by any other length other than 1 is dominated. Hence, the miner is better off taking S_l than S_p, S_w.

4.5.2 Schur-Concave Incentives

In order to address limitations from additive seperability, zero minimum and public chain dominance rule, another incentive design is introduced. Previous rules are relaxed and instead, the following is definition of Δn_i^{win}:

$$\Delta n_i^{\text{win}} = \begin{cases} n_i^{A_i} - \min(X') \ , & \min(X') \leq n_i + 1 \\ n_i^{A_i} \ , & \min(X') > n_i + 1 \end{cases} \tag{4.24}$$

such that $n_i^{A_i} \in \{0, n_i + 1, n_i\}$ when miner takes actions S_p, S_w, S_l respectively. Continuing from the definition of mechanism in Section 4.5, following are defined.

Definition 4.5.3 ***Zero Externality Loss***: $g^{loss}(\Delta n_i^{\text{loss}}, \Delta L^{\text{loss}}) = 0 \ \forall \ (\Delta n_i^{\text{loss}}, \Delta L^{\text{loss}}) \in \mathbb{R}^2$.

Zero externality loss implements payoffs similar to current mining mining protocols where losing miners incur cost of mining only (Antonopoulos, 2014; Böhme et al., 2015; Osborne et al., 2004). Hence, designing mechanisms that incorporate this aspect of mining enables consideration of implementability of proposed mining incentives (Bergemann and Morris, 2005; Green and Laffont, 1986).

Definition 4.5.4 ***Inequality Measurement***: *For a winning miner, pre-order of vectors of private and public chain increment* $\boldsymbol{x} = (\Delta n^{\text{win}}, \Delta L^{\text{win}}) \in \mathbb{R}^2 \setminus (0, 0)$ *can be computed using majorization.*

Inequality Measurement considers measuring differences between public and private chain increments. More precisely, our mechanism looks to evaluate how a winning miner's actions may result in increments to public and private chains that are more *unequal* than desired. The notion of inequality allows our mechanism to show how forking or working only on private chain results in public and private chain increments that are higher, more unequal and therefore undesirable for the system when compared to honest mining. Inequality measurement has been similarly used to measure inequality in parameters related to agent consumption, e.g., income, through the Lorenz Curve or Gini Index (Gastwirth, 1972; Lorenz, 1905).

Definition 4.5.5 ***Ordered Win Payoff****:* $g^{win}(\Delta n^{\text{win}}, \Delta L^{\text{win}})$ *is Schur-Concave and positive valued for* $(\Delta n^{\text{win}}, \Delta L^{\text{win}}) \in \mathbb{R}^2 \setminus (0,0)$ *but* $g^{win}(0,0) = 0$*.*

Definition 4.5.5 basically implies that a miner gets a positive payoff only from a non-zero net input to the system – in terms of ΔL^{win} or Δn^{win}. Using these assumptions and rewriting the sets of payoffs for each action considered by miner i gives the following $\forall\ A_{-i} \in \{S_p, S_w, S_l\}$:

$$u_i^{S_p,A_{-i}} = \begin{cases} g^{win}(-\min(X'), n_i + 1), & \min(X') \leq n_i + 1 \\ g^{win}(0, n_i + 1), & \min(X') > n_i + 1 \end{cases} \tag{4.25}$$

$$u_i^{S_w,A_{-i}} = \begin{cases} g^{win}(n_i + 1 - \min(X'), 0), & \min(X') \leq n_i + 1 \\ g^{win}(n_i + 1, 0), & \min(X') > n_i + 1 \end{cases} \tag{4.26}$$

$$u_i^{S_l,A_{-i}} = \begin{cases} g^{win}(n_i - \min(X'), 1), & \min(X') \leq n_i + 1 \\ g^{win}(n_i, 1), & \min(X') > n_i + 1 \end{cases} \tag{4.27}$$

Proposition 4 *For any miner with private chain length* $n_i > 0$*,* S_l *is a weakly dominant strategy under Zero Externality Loss, Inequality Measurement and Wins Payoff structure. Further, such a direct mechanism is strategy-proof.*

The key takeaway from Proposition 4 is that whenever miner's actions result in disparate increments in public and private chain, payoffs should be low. Forking or block-withholding in any given round results in such disparate increments (when compared to honest mining) and are therefore penalized. In the spirit of Proposition 3, here a miner has no incentive in misreporting chain length because even on doing so, the measurement of inequality between increments enables penalization. Hence, the miner finds no way of *gaming* the system and therefore mines honestly.

In order to substantiate the claims, we present a rigorous numerical example. As before, consider 5 miners and private chains of lengths $X = \{1, 3, 5, 4, 2\}$.

No winning miner has minimum private chain:

Suppose either miner $n_i = 3$ wins or loses to miner with $n_j = 5$. Consider the payoffs noting that $\min(X') = \min(X'') = 1$.

$$u_i^{S_p,S_{-i}} = \left\{ g^{win}(-1,4),\ \forall\ S_{-i} \in \{S_p, S_w, S_l\} \right. \tag{4.28}$$

$$u_i^{S_w,S_{-i}} = \left\{ g^{win}(3,0),\ \forall\ S_{-i} \in \{S_p, S_w, S_l\} \right. \tag{4.29}$$

$$u_i^{S_l,S_{-i}} = \left\{ g^{win}(2,1),\ \forall\ S_{-i} \in \{S_p, S_w, S_l\} \right. \tag{4.30}$$

Compare vectors $\{(1,2), (3,0), (-1,4)\}$. By Schur-concavity, since $(-1,4)$ majorizes $(2,1)$ implies $g^{win}(1,4) \leq g^{win}(2,1)$ and $(3,0)$ majorizes $(2,1)$ implies $g^{win}(3,0) \leq g^{win}(2,1)$.

Miner loses to minimum private chain miner:

Now suppose either miner $n_i = 2$ wins or loses to miner with $n_j = 1$. Consider the payoffs noting that $\min(X') = 1, \min(X'') = 2$.

$$u_i^{S_p,S_{-i}} = \left\{ g^{win}(-1,3),\ \forall\ S_{-i} \in \{S_p, S_w, S_l\} \right. \tag{4.31}$$

$$u_i^{S_w,S_{-i}} = \left\{ g^{win}(2,0),\ \forall\ S_{-i} \in \{S_p, S_w, S_l\} \right. \tag{4.32}$$

$$u_i^{S_l,S_{-i}} = \left\{ g^{win}(1,1),\ \forall\ S_{-i} \in \{S_p, S_w, S_l\} \right. \tag{4.33}$$

Again compare the vectors $\{(1,1), (2,0), (-1,3)\}$. By Schur-concavity, since $(-1,3)$ majorizes $(1,1)$ and $(2,0)$ majorizes $(1,1)$, we have that $g^{win}(1,1) \geq g^{win}(2,0)$ and $g^{win}(1,1) \geq g^{win}(-1,3)$.

Minimum private chain miner wins or loses:

Now suppose either miner $n_i = 1$ wins or loses to miner with $n_j = 2$. Consider the payoffs noting that $\min(X') = 2, \min(X'') = 1$.

$$u_i^{S_p,S_{-i}} = \Big\{ g^{win}(-2,2),\ \forall\ S_{-i} \in \{S_p, S_w, S_l\} \tag{4.34}$$

$$u_i^{S_w,S_{-i}} = \Big\{ g^{win}(0,0),\ \forall\ S_{-i} \in \{S_p, S_w, S_l\} \tag{4.35}$$

$$u_i^{S_l,S_{-i}} = \Big\{ g^{win}(-1,1),\ \forall\ S_{-i} \in \{S_p, S_w, S_l\} \tag{4.36}$$

By definition, since $g^{win}(0,0) = 0$, minimum private chain miner has zero payoff from S_w. In addition, since $(-2,2)$ majorizes $(-1,1)$, by Schur Concavity, $u_i^{S_l} \succ u_i^{S_p}$.

4.5.3 Additive Separability with Concave payoffs

In this section, we propose a mechanism that combines ideas from previous two sections (Sections 4.5.1 & 4.5.2). Specifically, we relax all definitions from Section 4.5.1, maintain definitions from Section 4.5.2. Further, we assume the same additive separable structure of g^{win} as in Section 4.5.1 and that $h_1(\Delta n^{win}), h_2(\Delta L^{win})$ are real valued concave functions $\forall\ (\Delta n^{win}, \Delta L^{win}) \in \mathbb{R}^2 \setminus (0,0)$ such that $\sum_{i=1}^{2} h_i(x_i) > 0\ \forall\ (x_1, x_2) \in \mathbb{R}^2 \setminus (0,0), \sum_{i=1}^{2} h_i(0) = 0$.

Under Zero Externality Loss, Inequality Measurement and Win Payoff assumptions, payoffs can be reformulated as follows:

$$u_i^{S_p,S_{-i}} = \begin{cases} h_1(n_i+1) + h_2(-\min(X')), & \min(X') \le n_i + 1 \\ h_1(n_i+1) + h_2(0), & \min(X') > n_i + 1 \end{cases} \tag{4.37}$$

$$u_i^{S_w,S_{-i}} = \begin{cases} h_1(0) + h_2(n_i + 1 - \min(X')), & \min(X') \le n_i + 1 \\ h_1(0) + h_2(n_i+1), & \min(X') > n_i + 1 \end{cases} \tag{4.38}$$

$$u_i^{S_l} = \begin{cases} h_1(1) + h_2(n_i - \min(X')), & \min(X') \leq n_i + 1 \\ h_1(1) + h_2(n_i), & \min(X') > n_i + 1 \end{cases} \tag{4.39}$$

Proposition 5 *For any miner with private chain length $n_i > 0$, S_l is a weakly dominant strategy under Zero Externality Loss, Inequality Measurement, Win Payoff structure and additively separable concave payoffs. Further, such a direct mechanism is strategy-proof.*

Proposition 5 basically extends the reasoning from Proposition 4 and presents an incentive structure with additive separability. In doing so, the mechanism demonstrates implementability (Ashlagi et al., 2010; Bergemann and Morris, 2005; Green and Laffont, 1986). In other words, separating payoffs from public and private chain increments opens possibilities of designing incentives that are quasilinear or incorporate different context dependent functional structures to public and private chain payoffs. We keep experimental analysis of impact of different structures on miner incentives, for future work.

4.5.4 Myopic Miner

In this section, we directly extend the model in Eyal and Sirer (2018); Sapirshtein et al. (2016) and show how proposed incentive structure makes honest mining a dominant strategy. First, the definition for $\Delta n_i^s \ \forall \ s \in \{\text{win}, \text{loss}\}$ is revised. Instead, as shown in Eyal and Sirer (2018); Sapirshtein et al. (2016) it is assumed that the miner is *myopic* and considers only the difference in increment in its own private chain length to increment in public chain length each round by honest miners. Hence, Δn_i^s is redefined as $\delta_i = n_i - l_h$. Essentially, δ_i is the lead a selfish miner's private chain length n_i has on the increment in public chain l_h by honest miners at the beginning of each round. As shown in Eyal and Sirer (2018), the selfish miner always tries to keep the lead such that $\delta_i \geq 1 \ \Rightarrow n_i \geq l_h + 1$.

Extending definition of payoff function from Section 4.5.2, suppose definitions 4.5.3, 4.5.4 and 4.5.5 hold. Then a myopic miner only considers expected payoffs from forking, withholding and honest mining as per:

$$u_i^{S_p} = g^{\text{win}}(-l_h, n_i + 1), \ \forall \ n_i \geq l_h + 1, n_i \in \{0, 1, 2, ..\} \tag{4.40}$$

$$u_i^{S_w} = g^{\text{win}}(n_i + 1 - l_h, 0), \ \forall \ n_i \geq l_h + 1, n_i \in \{0, 1, 2, ..\} \tag{4.41}$$

$$u_i^{S_l} = g^{\text{win}}(n_i - l_h, 1) \ \forall \ n_i \in \{0, 1, 2, ..\} \tag{4.42}$$

Each action represents the appropriate changes in δ_i and $\Delta L'$. When miner forks the chain, his private chain length is zero and hence $\delta_i = -l_h$; when withholding private chain length is incremented by 1 and hence $\delta_i = n_i + 1 - l_h$ and finally when honest mining, $\delta_i = n_i - l_h$ remains the same.

Proposition 6 *For any myopic miner with $n_i \geq 0$, under Zero Loss Externality, Inequality Measurement and Ordered Win Payoffs, honest mining is a dominant strategy. Further, such a direct mechanism is strategy-proof.*

The idea presented in Proposition 6 is an extension of Proposition 4 with a revised notion of comparing private chain increments with the honest majority. In spirit of Eyal and Sirer (2018); Sapirshtein et al. (2016), private chain increments measured in comparison to honest miner actions keep intact penalization for more unequal private and public chain increments. In addition, Proposition 6 shows that even if miners misreport private chain length, the mechanism makes honest mining dominant by measuring (and penalizing) how much each miner is acting selfishly (keeping a lead on honest miners) or honestly.

4.6 Conclusion

Theoretical analysis of mining incentives help establish the importance of designing the right incentives to encourage desired behavior. The optimal payoffs structure discovered does minimize selfish behavior and incentivize the honest behavior among miners. The key takeaway from analysis is that under either definition of Δn, greater penalty on actions that have negative externality on the system helps to incentivize honest mining. However, following are some limitations of the designed incentives. First, since there is no publicly available time-series data of miner actions for any cryptocurrency, our assumptions of how miners would behave and update their belief about the reward on winning a round under incomplete information may be over-assumed. For instance, we don't consider the case where new miners join or leave the blockchain system in a later round. It can be expected that new miners who join or leave the system may lead to changes in overall network hash rate which would imply changes to miners' action. This is because dynamic miner entry might lead to changes in Δn measurements. However, as shown, if penalty for negative externality to system is high enough, convergence to honest mining is possible. Third, the current miners' decision making strategy does not account for multiple complex incentives other than payoff maximization. For instance, off-platform Bitcoin prices may drive miner decisions on forking or block-withholding (Eyal et al., 2016; Narayanan et al., 2016). However, in spite of the limitations, our attempt at designing incentives for disincentivizing selfish mining points to the larger aim at strengthening the cryptocurrency protocols. Specifically, given that blockchain systems are protocol heavy rather than application heavy (Narayanan et al., 2016; Tapscott and Tapscott, 2016), the need to have robust protocols that maintain decentralization in the system is critical for the survival of cryptocurrencies. Our designed incentives provide a framework for developing further approaches to solving this problem in this area.

REFERENCES

G. Adomavicius and A. Gupta. Toward comprehensive real-time bidder support in iterative combinatorial auctions. Information Systems Research, 16(2):169–185, 2005.

G. Aggarwal, A. Goel, and R. Motwani. Truthful auctions for pricing search keywords. In Proceedings of the 7th ACM conference on Electronic commerce, pages 1–7. ACM, 2006.

S. Alrwais, K. Yuan, E. Alowaisheq, Z. Li, and X. Wang. Understanding the dark side of domain parking. In 23rd {USENIX} Security Symposium ({USENIX} Security 14), pages 207–222, 2014.

E. T. Anderson and J. D. Dana Jr. When is price discrimination profitable? Management Science, 55(6):980–989, 2009.

S. P. Anderson and J. S. Gans. Platform siphoning: Ad-avoidance and media content. American Economic Journal: Microeconomics, 3(4):1–34, 2011.

A. Andersson, M. Tenhunen, and F. Ygge. Integer programming for combinatorial auction winner determination. In MultiAgent Systems, 2000. Proceedings. Fourth International Conference on, pages 39–46. IEEE, 2000.

J. Andreoni, W. Harbaugh, and L. Vesterlund. The carrot or the stick: Rewards, punishments, and cooperation. American Economic Review, 93(3):893–902, 2003.

G. Andresen. March 2013 chain fork post-mortem, 2013.

A. M. Antonopoulos. Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.", New York, NY, USA, 2014.

M. Aseri, M. Dawande, G. Janakiraman, and V. Mookerjee. Ad-blockers: A blessing or a curse? Available at SSRN 3299057, 2018.

G. B. Asheim, T. Mitra, and B. Tungodden. Sustainable recursive social welfare functions. In The Economics of the Global Environment, pages 165–190. Springer, 2016.

I. Ashlagi, M. Braverman, A. Hassidim, and D. Monderer. Monotonicity and implementability. Econometrica, 78(5):1749–1772, 2010.

S. Athey and J. S. Gans. The impact of targeting technology on advertising markets and media competition. American Economic Review, 100(2):608–13, 2010.

A. Auger and B. Doerr. Theory of randomized search heuristics: Foundations and recent developments, volume 1. World Scientific, 2011.

E. M. Azevedo, E. G. Weyl, and A. White. Walrasian equilibrium in large, quasilinear markets. *Theoretical Economics*, 8(2):281–290, 2013.

M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On bitcoin and red balloons. In *Proceedings of the 13th ACM conference on electronic commerce*, pages 56–73. ACM, 2012.

S. Bag and K. Sakurai. Yet another note on block withholding attack on bitcoin mining pools. In *International Conference on Information Security*, pages 167–180. Springer, 2016.

S. Balachander, K. Kannan, and D. G. Schwartz. A theoretical and empirical analysis of alternate auction policies for search advertisements. *Review of Marketing Science*, 7(1), 2009.

T. Barbacovi. Blocking ad blockers. *J. Marshall Rev. Intell. Prop. L.*, 16:i, 2016.

S. Barber, X. Boyen, E. Shi, and E. Uzun. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security*, pages 399–414. Springer, 2012.

I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld. Proof of activity: Extending bitcoin's proof of work via proof of stake. *IACR Cryptology ePrint Archive*, 2014: 452, 2014.

D. Bergemann and S. Morris. Robust mechanism design. *Econometrica*, 73(6): 1771–1813, 2005.

T. Bergstrom, L. Blume, and H. Varian. On the private provision of public goods. *Journal of public economics*, 29(1):25–49, 1986.

M. Bichler. Combinatorial auctions: complexity and algorithms. *Wiley Encyclopedia of Operations Research and Management Science*, 2010.

M. Bichler and J. R. Kalagnanam. Software frameworks for advanced procurement auction markets. *Communications of the ACM*, 49(12):104–108, 2006.

M. Bichler, A. Davenport, G. Hohner, and J. Kalagnanam. Industrial procurement auctions. *Combinatorial auctions*, pages 593–612, 2006.

M. Bichler, P. Shabalin, and A. Pikovsky. A computational analysis of linear price iterative combinatorial auction formats. *Information Systems Research*, 20(1):33–59, 2009.

M. Bichler, A. Gupta, and W. Ketter. Research commentary – designing smart markets. *Information Systems Research*, 21(4):688–699, 2010.

C. Blum and X. Li. Swarm intelligence in optimization. In *Swarm Intelligence*, pages 43–85. Springer, 2008.

C. Blum and A. Roli. Metaheuristics in combinatorial optimization: Overview and conceptual comparison. *ACM computing surveys (CSUR)*, 35(3):268–308, 2003.

R. Böhme, N. Christin, B. Edelman, and T. Moore. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2):213–38, 2015.

T. Borovicka, M. Jirina Jr, P. Kordik, and M. Jirina. Selecting representative data sets. In Advances in data mining knowledge discovery and applications. InTech, 2012.

D. Boughaci, B. Benhamou, and H. Drias. A memetic algorithm for the optimal winner determination problem. Soft Computing-A Fusion of Foundations, Methodologies and Applications, 13(8):905–917, 2009.

D. Boughaci, B. Benhamou, and H. Drias. Local search methods for the optimal winner determination problem in combinatorial auctions. Journal of Mathematical Modelling and Algorithms, 9(2):165–180, 2010.

R. F. Brena, C. W. Handlin, and P. Angulo. A smart grid electricity market with multiagents, smart appliances and combinatorial auctions. In Smart Cities Conference (ISC2), 2015 IEEE First International, pages 1–6. IEEE, 2015.

M. Brinkmann. Adblock plus lost millions of users in the past year. Ghacks Technology News, 2017.

J. K. Brueckner and K. Lee. Economies of scope and multiproduct clubs. Public Finance Quarterly, 19(2):193–208, 1991.

J. M. Buchanan. An economic theory of clubs. Economica, 32(125):1–14, 1965.

A. S. P. Cansizoglu. Solving the Multi-dimensional 0-1 Knapsack Problem using Depth-k Canonical Cuts. North Carolina State University, 2011.

M. J. Casey and P. Vigna. In blockchain we trust. MIT Technology Review, 121(3): 10–16, 2018.

C. P. Chambers and F. Echenique. Supermodularity and preferences. Journal of Economic Theory, 144(3):1004–1014, 2009.

D. Chaum. Blind signatures for untraceable payments. In Advances in cryptology, pages 199–203. Springer, 1983.

X. Chen, C. Papadimitriou, and T. Roughgarden. An axiomatic approach to block rewards. arXiv preprint arXiv:1909.10645, 2019.

Y. Chen and M. H. Riordan. Price-increasing competition. The RAND Journal of Economics, 39(4):1042–1058, 2008.

C.-H. Cho. Why do people avoid advertising on the internet? Journal of Advertising, 33(4):89–97, 2004.

B. Codenotti, G. Manzini, L. Margara, and G. Resta. Perturbation: An efficient technique for the solution of very large instances of the euclidean tsp. INFORMS Journal on Computing, 8(2):125–133, 1996.

N. Cohen. Whiting out the ads, but at what cost? The New York Times, 3, 2012.

R. Cominetti, J. R. Correa, and N. E. Stier-Moses. The impact of oligopolistic competition in networks. Operations Research, 57(6):1421–1437, 2009.

F. T. Commission et al. Ftc report on internet of things urges companies to adopt best practices to address consumer privacy and security risks. available via ftc. accessed january 22, 2016, 2015.

O. Cordón García, F. Herrera Triguero, and T. Stützle. A review on the ant colony optimization metaheuristic: Basis, models and new trends. Mathware & soft computing. 2002 Vol. 9 Núm. 2 [-3], 2002.

S. Cowan and X. Yin. Competition can harm consumers. Australian Economic Papers, 47(3):264–271, 2008.

P. Cramton, Y. Shoham, and R. Steinberg. An overview of combinatorial auctions. ACM SIGecom Exchanges, 7(1):3–14, 2007.

P. Dasgupta, P. Hammond, and E. Maskin. The implementation of social choice rules: Some general results on incentive compatibility. The Review of Economic Studies, 46(2):185–216, 1979.

R. K. Dash, N. R. Jennings, and D. C. Parkes. Computational-mechanism design: A call to arms. IEEE intelligent systems, 18(6):40–47, 2003.

S. Davidson, P. De Filippi, and J. Potts. Economics of blockchain. Available at SSRN 2744751, 2016.

P. De and M. Mitra. Incentives and justice for sequencing problems. Economic Theory, 64(2):239–264, 2017.

A. De Corniere and R. De Nijs. Online advertising and privacy. The RAND Journal of Economics, 47(1):48–72, 2016.

S. De Vries and R. V. Vohra. Combinatorial auctions: A survey. INFORMS Journal on computing, 15(3):284–309, 2003.

C. Dellarocas. Reputation mechanism design in online trading environments with pure moral hazard. Information systems research, 16(2):209–230, 2005.

Digiday. Digiday live: How forbes is fighting ad blocking — and winning. 2016.

T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang. Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 30(7):1366–1385, 2018.

X. Dong, F. Wu, A. Faree, D. Guo, Y. Shen, and J. Ma. Selfholding: A combined attack model using selfish mining with block withholding attack. Computers & Security, page 101584, 2019.

M. Dorigo and M. Birattari. Ant colony optimization. In Encyclopedia of machine learning, pages 36–39. Springer, 2011.

M. Dorigo and G. Di Caro. Ant colony optimization: a new meta-heuristic. In Evolutionary Computation, 1999. CEC 99. Proceedings of the 1999 Congress on, volume 2, pages 1470–1477. IEEE, 1999.

M. Dorigo and T. Stutzle. The ant colony optimization metaheuristic: Algorithms, applications, and advances. International series in operations research and management science, pages 251–286, 2003.

M. Dorigo, V. Maniezzo, A. Colorni, and V. Maniezzo. Positive feedback as a search strategy. Technical Report No. 91-016, Politecnico di Milano, 1991.

M. Dorigo, E. Bonabeau, and G. Theraulaz. Ant algorithms and stigmergy. Future Generation Computer Systems, 16(8):851–871, 2000.

X. Drèze and F.-X. Hussherr. Internet advertising: Is anybody watching? Journal of interactive marketing, 17(4):8–23, 2003.

B. Edelman, M. Ostrovsky, and M. Schwarz. Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. The American economic review, 97(1):242–259, 2007.

B. Ellickson, B. Grodal, S. Scotchmer, and W. R. Zame. Clubs and the market: large finite economies. Journal of Economic Theory, 101(1):40–77, 2001.

M. T. Elliott and P. S. Speck. Consumer perceptions of advertising clutter and its impact across various media. Journal of advertising research, 38(1):29–30, 1998.

W. Elmaghraby and P. Keskinocak. Combinatorial auctions in procurement. In The practice of supply chain management: Where theory and application converge, pages 245–258. Springer, 2004.

E. Ephrati and J. S. Rosenschein. The clarke tax as a consensus mechanism among automated agents. In AAAI, volume 91, pages 173–178, 1991.

D. S. Evans. The online advertising industry: Economics, evolution, and privacy. The journal of economic perspectives, 23(3):37–60, 2009.

I. Eyal. Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. Computer, 50(9):38–49, 2017.

I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7):95–102, 2018.

I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse. Bitcoin-ng: A scalable blockchain protocol. In 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16), pages 45–59, 2016.

Eyeo. Contribute to adblock plus. AdBlock Plus Website, 2013.

R. F.-I. Fedorko. User preferences in the field of online ad-blocking. Perspectives, 10(7):1–11, 2018.

C. Foster. The cost of ad blocking - pagefair and adobe 2016 ad blocking report. 2016.

Y. Fujishima, K. Leyton-Brown, and Y. Shoham. Taming the computational complexity of combinatorial auctions: Optimal and approximate approaches. In IJCAI, volume 99, pages 548–553, 1999.

R. Gan, Q. Guo, H. Chang, and Y. Yi. Ant colony optimization for winner determination in combinatorial auctions. In Natural Computation, 2007. ICNC 2007. Third International Conference on, volume 4, pages 441–445. IEEE, 2007.

K. Garimella, O. Kostakis, and M. Mathioudakis. Ad-blocking: A study on performance, privacy and counter-measures. In Proceedings of the 2017 ACM on Web Science Conference, pages 259–262. ACM, 2017.

J. L. Gastwirth. The estimation of the lorenz curve and gini index. The review of economics and statistics, pages 306–316, 1972.

W. Geng and Z. Chen. Optimal pricing of virtual goods with conspicuous features in a freemium model. International Journal of Electronic Commerce, 23(3):427–449, 2019.

A. Ghalanos and S. Theussl. Rsolnp: general non-linear optimization using augmented lagrange multiplier method. R package version, 1, 2012.

F. Glaser. Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis. In Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.

R. Gonen and D. Lehmann. Optimal solutions for multi-unit combinatorial auctions: Branch and bound heuristics. 2000.

W. Gorman. Conditions for additive separability. Econometrica: Journal of the Econometric Society, pages 605–609, 1968a.

W. M. Gorman. The structure of utility functions. The Review of Economic Studies, 35(4):367–390, 1968b.

V. Gramoli. From blockchain consensus back to byzantine consensus. Future Generation Computer Systems, 2017.

J. Green and J.-J. Laffont. Characterization of satisfactory mechanisms for the revelation of preferences for public goods. Econometrica: Journal of the Econometric Society, pages 427–438, 1977.

J. R. Green and J.-J. Laffont. Partially verifiable information and mechanism design. The Review of Economic Studies, 53(3):447–456, 1986.

J. Greenberg. Ad blockers are making money off ads (and tracking, too). Wired Business, 2016.

R. Guerraoui and J. Wang. On the unfairness of blockchain. In International Conference on Networked Systems, pages 36–50. Springer, 2018.

Y. Guo, A. Lim, B. Rodrigues, and Y. Zhu. Heuristics for a bidding problem. Computers & operations research, 33(8):2179–2188, 2006.

W. J. Gutjahr. A graph-based ant system and its convergence. Future generation computer systems, 16(8):873–888, 2000.

J. Hamari, N. Hanner, and J. Koivisto. Service quality explains why people use freemium services but not if they go premium: An empirical study in free-to-play games. International Journal of Information Management, 37(1):1449–1459, 2017.

P. J. Hammond. Equity, arrow's conditions, and rawls' difference principle. Econometrica: Journal of the Econometric Society, pages 793–804, 1976.

R. W. Helsley and W. C. Strange. Exclusion and the private enforcement of property rights. Journal of Public Economics, 53(2):291–308, 1994.

J. L. Hemmer. Internet advertising battle: Copyright laws use to stop the use of ad-blocking software, the. Temp. J. Sci. Tech. & Envtl. L., 24:479, 2005.

A. Holland and B. O'Sullivan. Robust solutions for combinatorial auctions. In Proceedings of the 6th ACM Conference on Electronic Commerce, pages 183–192. ACM, 2005.

H. H. Hoos and C. Boutilier. Solving combinatorial auctions using stochastic local search. In AAAI/IAAI, pages 22–29, 2000.

J. Huang and W. Cheng. Filtering performance analysis and application study of advertising filtering tools. In 2017 12th International Conference on Intelligent Systems and Knowledge Engineering (ISKE), pages 1–5. IEEE, 2017.

G. Huberman, J. D. Leshno, and C. Moallemi. An economist's perspective on the bitcoin payment system. In AEA Papers and Proceedings, volume 109, pages 93–96, 2019.

M. Ikram and M. A. Kaafar. A first look at mobile ad-blocking apps. In 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), pages 1–8. IEEE, 2017.

U. Iqbal, Z. Shafiq, and Z. Qian. The ad wars: retrospective measurement and analysis of anti-adblock filter lists. In Proceedings of the 2017 Internet Measurement Conference, pages 171–183. ACM, 2017.

G. Iyer, D. Soberman, and J. M. Villas-Boas. The targeting of advertising. Marketing Science, 24(3):461–476, 2005.

S. Jiang and J. Wu. Bitcoin mining with transaction fees: A game on the block size. In Proc. of the 2nd IEEE International Conference on Blockchain (Blockchain 2019), 2019.

J. P. Johnson. Targeted advertising and advertising avoidance. The RAND Journal of Economics, 44(1):128–144, 2013.

Y. Kannai. Remarks concerning concave utility functions on finite sets. Economic Theory, 26(2):333–344, 2005.

P. Karaenke, M. Bichler, and S. Minner. Retail warehouse loading dock coordination by core-selecting package auctions. In ECIS, 2015.

P. Karaenke, M. Bichler, and S. Minner. Coordination is hard: Electronic market mechanisms for increased efficiency in transportation logistics. Management Science, 2018.

A. Karsenty. Ad-blocking and new business models on the internet. DigiWorld Economic Journal, 104(104), 2016.

Z. Katona and M. Sarvary. Eyeo's Adblock Plus: Consumer Movement or Advertising Toll Booth? The Berkeley-Haas Case Series. University of California, Berkeley. Haas ..., 2018.

B. Kewell, R. Adams, and G. Parry. Blockchain for good? Strategic Change, 26(5): 429–437, 2017.

A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis. Blockchain mining games. In Proceedings of the 2016 ACM Conference on Economics and Computation, pages 365–382. ACM, 2016.

V. Krammer. An effective defense against intrusive web advertising. In Privacy, Security and Trust, 2008. PST'08. Sixth Annual Conference on, pages 3–14. IEEE, 2008.

J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In Proceedings of WEIS, volume 2013, page 11, Washington D.C., USA, 2013. WEIS, 2013.

A. M. Kwasnica, J. O. Ledyard, D. Porter, and C. DeMartini. A new and improved design for multiobject iterative auctions. Management science, 51(3):419–434, 2005.

Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim. Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pages 195–209. ACM, 2017.

A. H. Lashkari, A. Seo, G. D. Gil, and A. Ghorbani. Cic-ab: Online ad blocker for browsers. In 2017 International Carnahan Conference on Security Technology (ICCST), pages 1–7. IEEE, 2017.

H. C. Lau and Y. G. Goh. An intelligent brokering system to support multi-agent web-based 4/sup th/-party logistics. In Tools with Artificial Intelligence, 2002.(ICTAI 2002). Proceedings. 14th IEEE International Conference on, pages 154–161. IEEE, 2002.

C.-S. Lee. An analytical framework for evaluating e-commerce business models and strategies. Internet Research, 11(4):349–359, 2001.

K. Lee. Transaction costs and equilibrium pricing of congested public goods with imperfect information. Journal of Public Economics, 45(3):337–362, 1991.

D. Lehmann, R. Müller, and T. Sandholm. The winner determination problem. Combinatorial auctions, pages 297–318, 2006.

R. P. Leme and E. Tardos. Pure and bayes-nash price of anarchy for generalized second price auction. In 2010 IEEE 51st Annual Symposium on Foundations of Computer Science, pages 735–744. IEEE, 2010.

P. Levy, D. Sarne, and I. Rochlin. Contest design with uncertain performance and costly participation. In IJCAI, pages 302–309, 2017.

Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein. Bitcoin mining pools: A cooperative game theoretic analysis. In Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, pages 919–927. International Foundation for Autonomous Agents and Multiagent Systems, 2015a.

Y. Lewenberg, Y. Sompolinsky, and A. Zohar. Inclusive block chain protocols. In International Conference on Financial Cryptography and Data Security, pages 528–547. Springer, 2015b.

K. Leyton-Brown, Y. Shoham, and M. Tennenholtz. An algorithm for multi-unit combinatorial auctions. In AAAI/IAAI, pages 56–61, 2000.

K. Leyton-Brown, E. Nudelman, and Y. Shoham. Learning the empirical hardness of optimization problems: The case of combinatorial auctions. In International Conference on Principles and Practice of Constraint Programming, pages 556–572. Springer, 2002.

K. Leyton-Brown, E. Nudelman, and Y. Shoham. Empirical hardness models: Methodology and a case study on combinatorial auctions. Journal of the ACM (JACM), 56(4):22, 2009.

W. Li, S. Andreina, J.-M. Bohli, and G. Karame. Securing proof-of-stake blockchain protocols. In Data Privacy Management, Cryptocurrencies and Blockchain Technology, pages 297–315. Springer, 2017a.

W. Li, W. Hui, A. Leung, and W. T. Yue. Content restrictions on adblock usage. In PACIS, page 84, 2017b.

B. Liu, J. Lu, R. Wang, and J. Zhang. Optimal prize allocation in contests: The role of negative prizes. Journal of Economic Theory, 175:291–317, 2018.

M. O. Lorenz. Methods of measuring the concentration of wealth. Publications of the American statistical association, 9(70):209–219, 1905.

D. Malandrino, A. Petta, V. Scarano, L. Serra, R. Spinelli, and B. Krishnamurthy. Privacy awareness about information leakage: Who knows what about me? In Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society, pages 279–284. ACM, 2013.

M. Malloy, M. McNamara, A. Cahn, and P. Barford. Ad blockers: Global prevalence and impact. In Proceedings of the 2016 ACM on Internet Measurement Conference, pages 119–125. ACM, 2016.

V. Maniezzo and A. Carbonaro. Ant colony optimization: an overview. In Essays and surveys in metaheuristics, pages 469–492. Springer, 2002.

F. Manjoo. Ad blockers and the nuisance at the heart of the modern web. The New York Times, 2015.

S. Mansfield-Devine. When advertising turns nasty. Network Security, 2015(11): 5–8, 2015.

M. Mariotti and R. Veneziani. Opportunities as chances: maximising the probability that everybody succeeds. The Economic Journal, 128(611):1609–1633, 2017.

D. Martens, M. De Backer, R. Haesen, J. Vanthienen, M. Snoeck, and B. Baesens. Classification with ant colony optimization. IEEE Transactions on Evolutionary Computation, 11(5):651–665, 2007.

D. Masclet, C. Noussair, S. Tucker, and M.-C. Villeval. Monetary and nonmonetary punishment in the voluntary contributions mechanism. American Economic Review, 93(1):366–380, 2003.

F. S. McChesney, M. Reksulak, and W. F. Shughart. Competition policy in public choice perspective. The Oxford Handbook of International Antitrust Economics, 1: 147, 2015.

R. A. Miller. The legal fate of internet ad-blocking. BUJ Sci. & Tech. L., 24:299, 2018.

H. Moulin. One-dimensional mechanism design. Theoretical Economics, 12(2):587–619, 2017.

U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks. A brief survey of cryptocurrency systems. In 2016 14th annual conference on privacy, security and trust (PST), pages 745–752. IEEE, 2016.

S. Muthukrishnan. Ad exchanges: Research issues. In International Workshop on Internet and Network Economics, pages 1–12. Springer, 2009.

R. B. Myerson. Incentive compatibility and the bargaining problem. Econometrica: journal of the Econometric Society, pages 61–73, 1979.

S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Working Paper, 2008.

G. Nan, D. Wu, M. Li, and Y. Tan. Optimal freemium strategy for information goods in the presence of piracy. Journal of the Association for Information Systems, 19(4):3, 2018.

A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.

C. Natoli and V. Gramoli. The blockchain anomaly. In 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), pages 310–317. IEEE, 2016.

K. Nayak, S. Kumar, A. Miller, and E. Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P), pages 305–320. IEEE, 2016.

J. Newman and F. E. Bustamante. The value of first impressions. In International Conference on Passive and Active Network Measurement, pages 273–285. Springer, 2019.

T. Niemand, S. Tischer, T. Fritzsche, and S. Kraus. The freemium effect: Why consumers perceive more value with free than with premium offers. 2015.

N. Nisan. Algorithms for selfish agents. In Annual Symposium on Theoretical Aspects of Computer Science, pages 1–15. Springer, 1999.

R. Nithyanand, S. Khattak, M. Javed, N. Vallina-Rodriguez, M. Falahrastegar, J. E. Powles, E. De Cristofaro, H. Haddadi, and S. J. Murdoch. Adblocking and counter blocking: A slice of the arms race. In FOCI, 2016.

M. J. Osborne et al. An Introduction to Game Theory, volume 3. Oxford University Press, New York, 2004.

W. Palant. Adblock plus user survey results. AdBlock Plus, 2011. URL `https://adblockplus.org/blog/adblock-plus-user-survey-results-part-0`. [Online; posted 10-October-2011].

D. C. Parkes and L. H. Ungar. Iterative combinatorial auctions: Theory and practice. AAAI/IAAI, 7481, 2000.

J. Pfeiffer and F. Rothlauf. Greedy heuristics and weight-coded eas for multidimensional knapsack problems and multi-unit combinatorial auctions. In Operations Research Proceedings 2007, pages 153–158. Springer, 2008.

E. L. Post and C. N. Sekharan. Comparative study and evaluation of online adblockers. In Information Science and Security (ICISS), 2015 2nd International Conference on, pages 1–4. IEEE, 2015.

G. V. Prasad, A. S. Prasad, and S. Rao. A combinatorial auction mechanism for multiple resource procurement in cloud computing. IEEE Transactions on Cloud Computing, 2016.

J. Puchinger, G. R. Raidl, and U. Pferschy. The core concept for the multidimensional knapsack problem. In European Conference on Evolutionary Computation in Combinatorial Optimization, pages 195–208. Springer, 2006.

J. Puchinger, G. R. Raidl, and U. Pferschy. The multidimensional knapsack problem: Structure and algorithms. INFORMS Journal on Computing, 22(2):250–265, 2010.

E. Pujol, O. Hohlfeld, and A. Feldmann. Annoyed users: Ads and ad-block usage in the wild. In Proceedings of the 2015 ACM Conference on Internet Measurement Conference, pages 93–106. ACM, 2015.

A. Ray and M. Ventresca. An ant colony approach for the winner determination problem. In European Conference on Evolutionary Computation in Combinatorial Optimization, pages 174–188. Springer, 2018.

A. Ray, M. Ventresca, and H. Wan. A mechanism design approach to blockchain protocols. In 2018 IEEE International Conference on Blockchain, pages 1603–1608. IEEE, 2018a.

A. Ray, M. Ventresca, and H. Wan. A mechanism design approach to blockchain protocols. In Proceedings of the IEEE 2018 Cybermatics Congress, pages 1603–1608. 2018 IEEE International Conference on Blockchain, 2018b.

M. K. Richter and K.-C. Wong. Concave utility on finite sets. Journal of economic theory, 115(2):341–357, 2004.

D. Ron and A. Shamir. Quantitative analysis of the full bitcoin transaction graph. In International Conference on Financial Cryptography and Data Security, pages 6–24. Springer, 2013.

M. H. Rothkopf, A. Pekeč, and R. M. Harstad. Computationally manageable combinational auctions. Management science, 44(8):1131–1147, 1998.

T. Roughgarden. The price of anarchy in games of incomplete information. In Proceedings of the 13th ACM Conference on Electronic Commerce, pages 862–879. ACM, 2012.

J. Runge, S. Wagner, D. Klapper, and J. Claussen. Freemium pricing: Evidence from a large-scale field experiment. In Academy of Management Proceedings, volume 2017, page 11533. Academy of Management Briarcliff Manor, NY 10510, 2017.

M. Saad, L. Njilla, C. Kamhoua, and A. Mohaisen. Countering selfish mining in blockchains. In 2019 International Conference on Computing, Networking and Communications (ICNC), pages 360–364. IEEE, 2019.

A. Saluke. Ad-blocking software as third-party tortious interference with advertising contracts. Bus. L. Rev., 7:87, 2008.

T. Sandholm. Algorithm for optimal winner determination in combinatorial auctions. Artificial intelligence, 135(1-2):1–54, 2002a.

T. Sandholm. emediator: A next generation electronic commerce server. Computational Intelligence, 18(4):656–676, 2002b.

T. Sandholm. Automated mechanism design: A new application area for search algorithms. In International Conference on Principles and Practice of Constraint Programming, pages 19–36, Berlin, Heidelberg, 2003. Springer.

T. Sandholm and S. Suri. Improved algorithms for optimal winner determination in combinatorial auctions and generalizations. In AAAI/IAAI, pages 90–97, 2000.

T. Sandholm and S. Suri. Bob: Improved winner determination in combinatorial auctions and generalizations. Artificial Intelligence, 145(1-2):33–58, 2003.

T. Sandholm, S. Suri, A. Gilpin, and D. Levine. Winner determination in combinatorial auction generalizations. In Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1, pages 69–76. ACM, 2002.

T. Sandholm, S. Suri, A. Gilpin, and D. Levine. Cabob: A fast optimal algorithm for winner determination in combinatorial auctions. Management Science, 51(3): 374–390, 2005.

T. Sandler. Buchanan clubs. Constitutional political economy, 24(4):265–284, 2013.

T. Sandler and J. Tschirhart. Club theory: Thirty years later. Public choice, 93 (3-4):335–355, 1997.

A. Sapirshtein, Y. Sompolinsky, and A. Zohar. Optimal selfish mining strategies in bitcoin. In International Conference on Financial Cryptography and Data Security, pages 515–532, Berlin, Heidelberg, 2016. Springer.

S. Scotchmer. On price-taking equilibria in club economies with nonanonymous crowding. Journal of Public Economics, 65(1):75–88, 1997.

M. Sefton, R. Shupp, and J. M. Walker. The effect of rewards and sanctions in provision of public goods. Economic inquiry, 45(4):671–690, 2007.

S. Shankland. Millions more people will use brave's ad-blocking browser by year-end, startup predicts. CNET, pages 01–02, 2018.

Y. Sheffi. Combinatorial auctions in the procurement of transportation services. Interfaces, 34(4):245–252, 2004.

B. Shiller, J. Waldfogel, and J. Ryan. Will ad blocking break the internet? Technical report, National Bureau of Economic Research, 2017.

R. Siegel. All-pay contests. Econometrica, 77(1):71–92, 2009.

E. C. Silva and C. M. Kahn. Exclusion and moral hazard: The case of identical demand. Journal of Public Economics, 52(2):217–235, 1993.

Y. Sompolinsky and A. Zohar. Bitcoin's underlying incentives. Communications of the ACM, 61(3):46–53, 2018.

P. S. Speck and M. T. Elliott. Predictors of advertising avoidance in print and broadcast media. Journal of Advertising, 26(3):61–76, 1997.

F. P. Sterbenz and T. Sandler. Sharing among clubs: a club of clubs theory. Oxford Economic Papers, 44(1):1–19, 1992.

B. Stone-Gross, R. Stevens, A. Zarras, R. Kemmerer, C. Kruegel, and G. Vigna. Understanding fraudulent activities in online ad exchanges. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, pages 279–294. ACM, 2011.

T. Stutzle and M. Dorigo. A short convergence proof for a class of ant colony optimization algorithms. IEEE Transactions on evolutionary computation, 6(4): 358–365, 2002.

T. Stützle and H. Hoos. Max-min ant system and local search for the traveling salesman problem. In IEEE International Conference on Evolutionary Computation (ICEC'97). Citeseer, 1997.

M. Sutter, S. Haigner, and M. G. Kocher. Choosing the carrot or the stick? endogenous institutional choice in social dilemma situations. The Review of Economic Studies, 77(4):1540–1566, 2010.

M. Swan. Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.", New York, NY, USA, 2015.

J. Tåg. Paying to remove advertisements. Information Economics and Policy, 21 (4):245–252, 2009.

D. Tapscott and A. Tapscott. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin, 2016.

M. B. Taylor. Bitcoin and the age of bespoke silicon. In 2013 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), pages 1–10. IEEE, 2013.

J. E. Teich, H. Wallenius, J. Wallenius, and O. R. Koppius. Emerging multiple issue e-auctions. European Journal of Operational Research, 159(1):1–16, 2004.

J. Tucker. Ad blockers could be exposing you to hackers with this exploit. Trusted Reviews, 2019.

J. Vallade. Adblock plus and the legal implications of online commercial-skipping. Rutgers L. Rev., 61:823, 2008.

H. R. Varian. Position auctions. international Journal of industrial Organization, 25(6):1163–1178, 2007.

H. R. Varian. Online ad auctions. The American Economic Review, 99(2):430–434, 2009.

H. R. Varian et al. The economics of internet search. Rivista di politica economica, 96(11/12):8, 2006.

A. Vastel, P. Snyder, and B. Livshits. The mounting cost of stale ad blocking rules. Brave Research & Analysis, 2018a.

A. Vastel, P. Snyder, and B. Livshits. Who filters the filters: Understanding the growth, usefulness and efficiency of crowdsourced ad blocking. arXiv preprint arXiv:1810.09160, 2018b.

V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer. Karma: A secure economic framework for peer-to-peer resource sharing. In Workshop on Economics of Peer-to-peer Systems, volume 35, 2003.

N. Vratonjic, M. H. Manshaei, J. Grossklags, and J.-P. Hubaux. Ad-blocking games: Monetizing online content under the threat of ad avoidance. In The Economics of Information Security and Privacy, pages 49–73. Springer, 2013.

T. M. Wagner, A. Benlian, and T. Hess. Converting freemium customers from free to premium—the role of the perceived premium fit in the case of music as a service. Electronic Markets, 24(4):259–268, 2014.

J. L. Walbesser. Blocking advertisement blocking: The war over internet advertising and the effect on intellectual property. Intellectual Property & Technology Law Journal, 23(1):19, 2011.

J. M. Walker and M. A. Halloran. Rewards and sanctions and the provision of public goods in one-shot settings. Experimental Economics, 7(3):235–247, 2004.

R. J. Walls, E. D. Kilmer, N. Lageman, and P. D. McDaniel. Measuring the impact and perception of acceptable advertisements. In Proceedings of the 2015 ACM Conference on Internet Measurement Conference, pages 107–120. ACM, 2015.

W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access, 7:22328–22370, 2019.

J. Wielki and J. Grabara. The impact of ad-blocking on the sustainable development of the digital advertising ecosystem. Sustainability, 10(11):4039, 2018.

C. E. Wills and D. C. Uzunoglu. What ad blockers are (and are not) doing. In Hot Topics in Web Systems and Technologies (HotWeb), 2016 Fourth IEEE Workshop on, pages 72–77. IEEE, 2016.

Q. Wu and J.-K. Hao. A clique-based exact method for optimal winner determination in combinatorial auctions. Information Sciences, 334:103–121, 2016.

M. Xia, G. J. Koehler, and A. B. Whinston. Pricing combinatorial auctions. European Journal of Operational Research, 154(1):251–270, 2004.

B. Yang and H. Garcia-Molina. Ppay: micropayments for peer-to-peer systems. In Proceedings of the 10th ACM conference on Computer and communications security, pages 300–310. ACM, 2003.

X.-S. Yang. Nature-inspired metaheuristic algorithms. Luniver press, 2010.

H. Youn, M. T. Gastner, and H. Jeong. Price of anarchy in transportation networks: efficiency and optimality control. Physical review letters, 101(12):128701, 2008.

S. Zaman and D. Grosu. Combinatorial auction-based allocation of virtual machine instances in clouds. Journal of Parallel and Distributed Computing, 73(4):495–508, 2013.

A. Zambrano and C. Pickard. A defense of ad blocking and consumer inattention. Ethics and Information Technology, 20(3):143–155, 2018.

J. Zhang, S. Pourazarm, C. G. Cassandras, and I. C. Paschalidis. The price of anarchy in transportation networks: Data-driven evaluation and reduction strategies. Proceedings of the IEEE, 106(4):538–553, 2018.

W. Zhou. A simple model of entry that increases price levels and price dispersion. Advances in Economic Analysis & Policy, 6(1), 2006.

A. APPENDIX A

A.1 Proof Lemma 1

Proof Second stage, users choose between

$$u_1 = \alpha(v - t) \tag{A.1}$$

$$u_2 = \alpha(v + z - tm_w) - c(n_2) \tag{A.2}$$

The indifference point is $\alpha_1 = \frac{c}{c+z+t(1-m_w)}$. Mass of free usage members is $n_2 = 1 - \left(\frac{c}{c+z+t(1-m_w)}\right)$. It is easy to see that given parameter range assumptions the max value α_1 assumes is $\frac{1}{1+z}$ $\forall$ $z \in (1, v)$ and minimum value is zero. Hence mass of free members is between $\left(1 - \frac{1}{1+z}, 1\right] \subset [\frac{1}{2}, 1]$. For AB, since mass of free members is always greater than free members, the decision is to charge whitelisters the lower price γ_w^L. ■

A.2 Proof Lemma 2

Proof Second stage, users choose between

$$u_1 = \alpha(v - t) \tag{A.3}$$

$$u_3 = \alpha(v + z) - c(n_3) - p_a \tag{A.4}$$

The indifference point is $\alpha = \frac{c+p_a}{c+t+z}$. Mass of paid usage members us $n_3 = 1 - \left(\frac{c+p_a}{c+t+z}\right)$. First stage, AB solves for premium price for optimizing revenue. Since objective function is trivially concave, $p_a^* = \frac{t+z}{2}$, which implies $\alpha_3 = \frac{2c+t+z}{2(c+t+z)}$. Mass of paid users at equilibrium is $n_3^* = 1 - \frac{2c+t+z}{2(c+t+z)}$. Now, note that $\frac{2c+t+z}{2(c+t+z)}$ can be simplified to $\frac{1}{2} + \frac{c}{2(c+t+z)} \geq \frac{1}{2}$. This implies that $n_3^* \leq \frac{1}{2}$. ■

A.3 Proof Lemma 3

Proof Second stage, users choose between

$$u_1 = \alpha(v - t) \tag{A.5}$$

$$u_2 = \alpha(v + z - tm_w) - c(n_2 + n_3) \tag{A.6}$$

$$u_3 = \alpha(v + z) - c(n_2 + n_3) - p_a \tag{A.7}$$

In the two stage game, Stage 1 – AB sets price for advertisers based on following:

$$p_w = \begin{cases} \gamma_w^L, & n_2 \geq n_3 \\ \gamma_w^H, & n_2 < n_3 \end{cases} \tag{A.8}$$

where $\gamma_w^H > \gamma_w^L; \gamma_w^H, \gamma_w^L \in (0, 1)$, and price for premium membership p_a. For freemium, n_2 denotes mass of free members while n_1 is mass of non-members. As derived from stage 2, mass of free members is $n_2 = \frac{p_a}{tm_w} - \frac{c}{c+z+t(1-m_w)}$ and of premium members is $n_3 = 1 - \frac{p_a}{tm_w}$ such that $\alpha_1 = \frac{c}{c+z+t(1-m_w)}$ and $\alpha_2 = \frac{p_a}{tm_w}$. So the AB basically has to solve the following problem, and choose between two revenue choices:

$$\begin{aligned} \max_{p_a} \quad & \gamma_w^L m_w + p_a n_3 \\ \text{s.t.} \quad & p_a - tm_w \leq 0 \\ & 1 + \frac{c}{c + z + t(1 - m_w)} - \frac{2p_a}{tm_w} \leq 0 \end{aligned} \tag{A.9}$$

and

$$\begin{aligned} \max_{p_a} \quad & \gamma_w^H m_w + p_a n_3 \\ \text{s.t.} \quad & p_a - tm_w \leq 0 \\ & \frac{2p_a}{tm_w} - \frac{c}{c + z + t(1 - m_w)} - 1 < 0 \end{aligned} \tag{A.10}$$

Solving first problem, Equation A.9, we have the following Lagrangean

$$\mathfrak{L} = \gamma_w^L m_w + p_a \left(1 - \frac{p_a}{tm_w}\right) - \lambda_1 \left(p_a - tm_w\right) - \lambda_2 \left(1 + \frac{c}{c+z+t(1-m_w)} - \frac{2p_a}{tm_w}\right)$$

The FOC is

$$FOC : 1 - \frac{2p_a}{tm_w} - \lambda_1 + \frac{2\lambda_2}{tm_w}$$

Following are the complementary slackness conditions to analyze:

- **Case 1** $\lambda_1 = 0, \lambda_2 = 0$: $p_a^* = \frac{tm_w}{2}$. This is clearly not valid since $\frac{c}{c+z+t(1-m_w)} < 0$ doesn't hold.
- **Case 2** $\lambda_1 = 0, \lambda_2 > 0$: This implies second constraint holds with equality. Hence solving $\frac{2p_a}{tm_w} = 1 + \frac{c}{c+z+t(1-m_w)}$, we have that $p_a^* = \frac{tm_w}{2}\left(1 + \frac{c}{c+z+t(1-m_w)}\right) < tm_w \ \forall \ \frac{c}{c+z+t(1-m_w)} \in (0, \frac{1}{2})$.
- **Case 3** $\lambda_1 > 0, \lambda_2 = 0$: This implies first constraint holds with equality such that $p_a^* = tm_w$, and second holds with inequality since $-1 + \frac{c}{c+z+t(1-m_w)} < 0$. However, in FOC, $\lambda_1 = -1 < 0$ hence this solution doesn't hold.
- **Case 4** $\lambda_1 > 0, \lambda_2 > 0$: This implies both constraints holds with equality. But this is impossible since on solving, we get different values of p_a^*.

Hence, AB has mass of premium members is $n_3 = \frac{1}{2} - \frac{c}{2(c+z+t(1-m_w))}$ while mass of free members is $n_2 = \frac{1}{2} - \frac{c}{2(c+z+t(1-m_w))}$. Revenue from this is

$$\pi_{AB}^* = \frac{tm_w}{2}\left(1 + \frac{c}{c+z+t(1-m_w)}\right)\left(\frac{1}{2} - \frac{c}{2(c+z+t(1-m_w))}\right) + \gamma_w^L m_w.$$

Solving second problem, following is the Lagrangean:

$$\mathfrak{L} = \gamma_w^H m_w + p_a \left(1 - \frac{p_a}{tm_w}\right) - \lambda_1 \left(p_a - tm_w\right) - \lambda_2 \left(\frac{2p_a}{tm_w} - \frac{c}{c+z+t(1-m_w)} - 1\right)$$

The FOC is the same and is

$$FOC : 1 - \frac{2p_a}{tm_w} - \lambda_1 - \frac{\lambda_2}{tm_w}$$

Following are the complementary slackness conditions to analyze:

- **Case 1** $\lambda_1 = 0, \lambda_2 = 0$: $p_a^* = \frac{tm_w}{2}$. This is a valid solution in this case.
- **Case 2** $\lambda_1 = 0, \lambda_2 > 0$: This implies second constraint holds with equality. This is not possible in this scenario and hence, this case is neglected.
- **Case 3** $\lambda_1 > 0, \lambda_2 = 0$: This implies first constraint holds with equality such that $p_a^* = tm_w$, and second is violated since $1 - \frac{c}{c+z+t(1-m_w)} > 0 \ \forall \ \sigma \in (1 - \frac{c}{c+z+t(1-m_w)}, 1)$. Further, in FOC, $\lambda_1 = -1 < 0$ hence this solution doesn't hold.
- **Case 4** $\lambda_1 > 0, \lambda_2 > 0$: This implies both constraints holds with equality. But this is impossible since on solving, we get different values of p_a^*.

So analyzing revenues from all three cases we have that AB revenue from this is

$$\pi_{AB}^* = \frac{tm_w}{4} + \gamma_w^H m_w.$$

Comparison of revenue from these two scenarios help establish mass of whitelisted advertisers for which AB charges higher or lower. In doing so, note that the following holds true $\forall \ \sigma \in [\frac{1}{2}, 1), c, t, m_w \in (0, 1)$:

$$\frac{1}{2}\left(1 + \frac{c}{c+z+t(1-m_w)}\right)\left(\frac{1}{2} - \left(\frac{c}{c+z+t(1-m_w)}\right)\right) < \frac{1}{4}$$

This is because the following simplifies to,

$$\Rightarrow \frac{1}{2}\left(1 + \frac{c}{c+z+t(1-m_w)}\right)\left(\frac{1}{2} - \left(\frac{c}{c+z+t(1-m_w)}\right)\right) - \frac{1}{4}$$
$$\Rightarrow -\frac{1}{4}\left(\left(\frac{c}{c+z+t(1-m_w)}\right) + 2\left(\frac{c}{c+z+t(1-m_w)}\right)^2\right) < 0$$

Therefore, since $\gamma_w^H > \gamma_w^L$ and $\frac{1}{2}\left(1+\frac{c}{c+z+t(1-m_w)}\right)\left(\frac{1}{2}-\left(\frac{c}{c+z+t(1-m_w)}\right)\right) < \frac{1}{4}$, AB always chooses $p_a^* = \frac{tm_w}{2}$ such that revenue is

$$\boxed{\pi_{AB}^* = \frac{tm_w}{4} + \gamma_w^H m_w}$$

$\blacksquare$

A.4 Proof Proposition 1

Proof Comparison - Ad-Exchange vs. Paid

This is a proof by deduction using properties of functions on compact sets. Specifically, all 8 extreme cases corresponding to the set $I : (c, t, m_w) \in \{(0,1)\times(0,1)\times(0,1)\}$ are listed out, and under each case, a function defined as difference between area under the graphs under ad-exchange and paid models is analyzed. For each case it shown that difference in ad-exchange vs. paid welfare is non-negative and finally, it is shown that since the difference in welfare is nowhere negative or zero, the only scenario is that the difference is positive over the domain I.

Case	c	t	m_w	Indifference Point - Ad-Ex	Indifference Point - Paid
1	1	1	1	$\frac{1}{1+z}$	$\frac{3+z}{2(2+z)}$
2	1	1	0	$\frac{1}{2+z}$	$\frac{3+z}{2(2+z)}$
3	1	0	1	$\frac{1}{1+z}$	$\frac{2+z}{2(1+z)}$
4	1	0	0	$\frac{1}{1+z}$	$\frac{2+z}{2(1+z)}$
5	0	1	1	0	$\frac{1}{2}$
6	0	1	0	0	$\frac{1}{2}$
7	0	0	1	0	$\frac{1}{2}$
8	0	0	0	0	$\frac{1}{2}$

Recall that user welfare under these two models is,

$$V_1^{\text{ad-ex}} = (v + z - tm_w)\left(\frac{1-\alpha_1^2}{2}\right) - c(1-\alpha_1)^2$$
$$V_1^{\text{paid}} = (v+z)\left(\frac{1-\alpha_3^2}{2}\right) - c(1-\alpha_3)^2 - \frac{t+z}{2}(1-\alpha_3)$$

Case 1: Area under the graph considering ad-exchange is

$$(v+z-1)\left(\frac{1-\left(\frac{1}{1+z}\right)^2}{2}\right) - \left(1-\frac{1}{1+z}\right)^2$$

and considering paid is

$$(v+z)\left(\frac{1-\left(\frac{3+z}{2(2+z)}\right)^2}{2}\right) - \left(1-\frac{3+z}{2(2+z)}\right)^2 - \frac{1+z}{2}\left(1-\frac{3+z}{2(2+z)}\right)$$

Subtracting paid welfare from ad-exchange welfare and collecting terms for $v + z$, we have

$$\Rightarrow \frac{(v+z)}{2}\left(\left(\frac{3+z}{2(2+z)}\right)^2 - \frac{1}{(1+z)^2}\right) > 0 \;\forall\; v > 2,\; z \in (1, v)$$

Collecting rest of the terms

$$\Rightarrow -\frac{1}{2}\left(1-\left(\frac{1}{1+z}\right)^2\right) - \left(\frac{z}{1+z}\right)^2 + \left(1-\frac{3+z}{2(2+z)}\right)^2 + \frac{1+z}{2}\left(1-\frac{3+z}{2(2+z)}\right)$$
$$\Rightarrow -\frac{1}{2}\left(1-\left(\frac{1}{1+z}\right)^2\right) - \left(\frac{z}{1+z}\right)^2 + \left(1-\frac{3+z}{2(2+z)}\right)\left(\left(1-\frac{3+z}{2(2+z)}\right) + \frac{1+z}{2}\right)$$
$$\Rightarrow -\frac{1}{2}\left(1-\left(\frac{1}{1+z}\right)^2\right) - \left(\frac{z}{1+z}\right)^2 + \left(\frac{1+z}{2(2+z)}\right)\left(\left(\frac{1+z}{2(2+z)}\right) + \frac{1+z}{2}\right)$$
$$\Rightarrow \frac{(3+z)(1+z)^2}{4(2+z)^2} - \frac{(2z+3z^2)}{2(1+z)^2}$$

Adding to previous term, we have that

$$\frac{(v+z)}{2}\left(\left(\frac{3+z}{2(2+z)}\right)^2-\frac{1}{(1+z)^2}\right)+\frac{(3+z)(1+z)^2}{4(2+z)^2}-\frac{(2z+3z^2)}{2(1+z)^2}>0\ \forall\ z\in(1,v),v>2$$

So summation of both terms is >0 such that, ad-exchange is better than paid model.

Case 2: Area under the graph considering ad-exchange is

$$(v+z-1)\left(\frac{1-\left(\frac{1}{2+z}\right)^2}{2}\right)-\left(1-\frac{1}{2+z}\right)^2$$

and considering paid is

$$(v+z)\left(\frac{1-\left(\frac{3+z}{2(2+z)}\right)^2}{2}\right)-\left(1-\frac{3+z}{2(2+z)}\right)^2-\frac{1+z}{2}\left(1-\frac{3+z}{2(2+z)}\right)$$

Subtracting paid welfare from ad-exchange welfare and collecting terms for $v+z$, we have

$$\Rightarrow\frac{(v+z)}{2}\left(\left(\frac{3+z}{2(2+z)}\right)^2-\frac{1}{(2+z)^2}\right)>0\ \forall\ v>2,\ z\in(1,v)$$

Collecting rest of the terms,

$$\Rightarrow-\frac{1}{2}\left(1-\left(\frac{1}{2+z}\right)^2\right)-\left(\frac{1+z}{2+z}\right)^2+\left(1-\frac{3+z}{2(2+z)}\right)^2+\frac{1+z}{2}\left(1-\frac{3+z}{2(2+z)}\right)$$
$$\Rightarrow-\frac{1}{2}\left(1-\left(\frac{1}{2+z}\right)^2\right)-\left(\frac{1+z}{2+z}\right)^2+\left(1-\frac{3+z}{2(2+z)}\right)\left(\left(1-\frac{3+z}{2(2+z)}\right)+\frac{1+z}{2}\right)$$
$$\Rightarrow-\frac{1}{2}\left(1-\left(\frac{1}{2+z}\right)^2\right)-\left(\frac{1+z}{2+z}\right)^2+\left(\frac{1+z}{2(2+z)}\right)\left(\left(\frac{1+z}{2(2+z)}\right)+\frac{1+z}{2}\right)$$
$$\Rightarrow\frac{z^3-z^2-9z-7}{4(2+z)^2}$$

Again, summation of both terms gives,

$$\Rightarrow \frac{z^3 - z^2 - 9z - 7}{4(2+z)^2} + \frac{(v+z)}{2}\left(\left(\frac{3+z}{2(2+z)}\right)^2 - \frac{1}{(2+z)^2}\right) > 0 \;\forall\; v > 2,\; z \in (1, v)$$

proves that ad-exchange is better than paid.

Case 3: Area under the graph considering ad-exchange is

$$(v+z)\left(\frac{1 - \left(\frac{1}{1+z}\right)^2}{2}\right) - \left(1 - \frac{1}{1+z}\right)^2$$

and considering paid is

$$(v+z)\left(\frac{1 - \left(\frac{2+z}{2(1+z)}\right)^2}{2}\right) - \left(1 - \frac{2+z}{2(1+z)}\right)^2 - \frac{z}{2}\left(1 - \frac{2+z}{2(1+z)}\right)$$

Subtracting paid welfare from ad-exchange welfare and collecting terms for $v + z$, we have

$$\Rightarrow \frac{(v+z)}{2}\left(\left(\frac{2+z}{2(1+z)}\right)^2 - \frac{1}{(1+z)^2}\right) > 0 \;\forall\; z \in (1, v),\; v > 2$$

Collecting rest of the terms we have

$$\begin{aligned}
& -\left(1 - \frac{1}{1+z}\right)^2 + \left(1 - \left(\frac{2+z}{2(1+z)}\right)\right)\left(\left(1 - \left(\frac{2+z}{2(1+z)}\right)\right) + \frac{z}{2}\right) \\
& \Rightarrow -\left(\frac{z}{1+z}\right)^2 + \left(\frac{z}{2(1+z)}\right)\left(\frac{z}{2(1+z)} + \frac{z}{2}\right) \\
& \Rightarrow -\left(\frac{z}{1+z}\right)^2 + \frac{1}{4}\left(\frac{z}{(1+z)}\right)^2 + \frac{z^2}{4(1+z)} \\
& \Rightarrow -\frac{3}{4}\left(\frac{z}{1+z}\right)^2 + \frac{z^2}{4(1+z)} \\
& \Rightarrow \frac{z^2}{4}\left(\frac{1}{1+z} - \frac{3}{(1+z)^2}\right) \\
& \Rightarrow \frac{z^2(z-2)}{4(1+z)^2}
\end{aligned}$$

Adding this to the previous terms we have

$$\frac{(v+z)}{2}\left(\left(\frac{2+z}{2(1+z)}\right)^2-\frac{1}{(1+z)^2}\right)+\frac{z^2(z-2)}{4(1+z)^2}>0\ \forall\ z\in(1,v),v>2$$

Note that proof for Case 3 covers for Case 4. Further, for Case 5, user welfare is higher under ad-exchange than paid since

$$\Rightarrow (v+z-1)\frac{1}{2}-(v+z)\frac{3}{8}+\frac{z+1}{4} \tag{A.11}$$

$$\Rightarrow (v+z)\frac{1}{8}+\frac{z-1}{4}>0\ \forall\ z\in(1,v)\ v>2 \tag{A.12}$$

For Case 6-8, following holds

$$\Rightarrow (v+z)\frac{1}{2}-(v+z)\frac{3}{8}+\frac{z+1}{4} \tag{A.13}$$

$$\Rightarrow (v+z)\frac{1}{8}+\frac{z+1}{4}>0 \tag{A.14}$$

Having analyzed the end points of c, t, m_w interval, more generally consider the following function, defined as difference between ad-exchange and paid user welfares:

$$g(c,t,m_w)=\frac{1}{2}\left((\alpha_3-\alpha_1)\left((v+z)(\alpha_3+\alpha_1)-2c(2-\alpha_1-\alpha_3)\right)+(t+z)(1-\alpha_3)-tm_w(1-\alpha_1^2)\right) \tag{A.15}$$

Using a proof by contradiction strategy, we show that since $g(c,t,m_w)$ is defined on a closed interval $I:(c,t,m_w)\in\{(0,1)\times(0,1)\times(0,1)\}$, if the function takes non-negative value at end points of this interval then for $g(c,t,m_w)$ to take a negative value, at some point on the interior of the interval, $\exists\ (c,t,m_w)$ s.t. $g(c,t,m_w)=0$. This is a direct rephrasing of the Bolzano Theorem – a generalization of the

Intermediate Value Theorem[1]. Hence, suppose $\exists\ (c, t, m_w)$, s.t. $g(.) = 0$. Equating equation A.15 to zero, we have that

$$(\alpha_3 - \alpha_1)\left((v+z)(\alpha_3 + \alpha_1) - 2c(2 - \alpha_1 - \alpha_3)\right) + (t+z)(1-\alpha_3) - tm_w(1-\alpha_1^2) = 0$$

It is clear that since $\alpha_3 > \alpha_1\ \forall\ c, t, m_w \in (0,1)$ the only values for which the above expression equals zero is when

$$\left(\frac{tm_w(1-\alpha_1^2) - (t+z)(1-\alpha_3)}{\alpha_3 - \alpha_1}\right) = (v+z)(\alpha_3+\alpha_1) - 2c(2-\alpha_1-\alpha_3)$$

This is clearly not possible since the LHS of equation is negative because $(t+z)(1-\alpha_3) > tm_w(1-\alpha_1^2)\ \forall\ c, t, m_w \in (0,1),\ z \in (1, v)$ and $\alpha_3 - \alpha_1 > 0$, while the RHS is clearly positive $\forall\ c, t, m_w \in (0,1),\ z \in (1, v)\ v > 2$. Therefore there do not exist any $(c, t, m_w) \in I$ where $g(c, t, m_w) = 0$, which is a contradiction. More generally, using Intermediate Value Theorem, consider a multivariate continuous function $g(c, t, m_w)$, defined as the difference between ad-exchange user welfare and paid user welfare, on the connected interval $I : (c, t, m_w) \in \{(0,1) \times (0,1) \times (0,1)\}$ that takes values $g(0,0,0) > 0$ and $g(1,1,1) > 0$ on the interval end points. Since value on the endpoints are positive, and the function does not equal zero on any intermediate point vector $(c, t, m_w) \in I$, the function takes positive values in the range $g(c, t, m_w) \in (g(0,0,0), g(1,1,1))$. Therefore, ad-exchange has higher welfare for users than paid revenue model.

Comparison - Ad-Exchange vs. Freemium

This is a proof by deduction. Specifically, comparing user welfare, following expression is analyzed. $V_1^{\text{ad-ex}} - V_1^{\text{frm}}$:

$$(v + z - tm_w)\left(\frac{1-\alpha_1^2}{2}\right) - c(1-\alpha_1)^2 - \left(\left(\frac{\alpha_2^2 - \alpha_1^2}{2}\right)(v + z - tm_w)\right.$$
$$\left. - c(\alpha_2 - \alpha_1)(1-\alpha_1) + \frac{1-\alpha_2^2}{2}(v+z) - c(1-\alpha_2)(1-\alpha_1) - (1-\alpha_2)\left(\frac{tm_w}{2}\right)\right)$$

[1] IVT: Let $I = [a, b]$ be a closed interval in $\mathbb{R}$, and let f be a continuous real-valued function on I. Then f assumes every value between $f(a)$ and $f(b)$.

Collecting terms with same coefficients, consider $v + z - tm_w$.

$$\begin{aligned}
&\left(\frac{1-\alpha_1^2}{2}\right) - \left(\frac{\alpha_2^2-\alpha_1^2}{2}\right) \\
&\Rightarrow \frac{1-\alpha_2^2}{2}
\end{aligned}$$

Similarly, for c, we have

$$\begin{aligned}
&(\alpha_2-\alpha_1)(1-\alpha_1) + (1-\alpha_2)(1-\alpha_1) - (1-\alpha_1)^2 \\
&\Rightarrow (1-\alpha_1)(\alpha_2-\alpha_1-1+\alpha_1+1-\alpha_2) \\
&\Rightarrow 0
\end{aligned}$$

Collecting simplified terms and other terms we get

$$\begin{aligned}
&(v+z-tm_w)\left(\frac{1-\alpha_2^2}{2}\right) - \frac{(1-\alpha_2^2)}{2}(v+z) + (1-\alpha_2)\left(\frac{tm_w}{2}\right) \\
&\Rightarrow -\frac{(1-\alpha_2^2)}{2}(tm_w) + (1-\alpha_2)\left(\frac{tm_w}{2}\right) \\
&\Rightarrow -\frac{tm_w}{2}(1-\alpha_2)(2+\alpha_2) < 0
\end{aligned}$$

Clearly, Freemium better than Ad-Exchange Model for User welfare. By transitivity, it can concluded that

$$\boxed{\text{Freemium} \succ \text{Ad-Exchange} \succ \text{Paid}} \tag{A.16}$$

■

A.5 Proof Lemma 4

Proof Considering CP, recall that CP payoffs under ad-exchange and paid is as follows:

$$\begin{aligned}
\pi_{CP}^{\text{ad-ex}} &= \frac{(1-k)m_w}{2}\left(1-\alpha_1^2\right)+\frac{\alpha_1^2}{2} \\
\pi_{CP}^{\text{paid}} &= \frac{1}{2}\left(\alpha_3\right)^2
\end{aligned}$$

Subtracting π_{CP}^{paid} from $\pi_{CP}^{\text{ad-ex}}$ we get,

$$\frac{(1-k)m_w}{2}(1-\alpha_1^2)+\frac{\alpha_1^2-\alpha_3^2}{2}$$

In order to determine the scenarios where CP earns more or less from ad-exchange, than paid, define the following as threshold revenue sharing fraction

$$k_{\tau}^{ap} = 1-\frac{\alpha_3^2-\alpha_1^2}{m_w(1-\alpha_1^2)} \tag{A.17}$$

where $\alpha_3 = \frac{2c+t+z}{2(c+t+z)}, \alpha_1 = \frac{c}{c+z+t(1-m_w)}$. It is important to note that since $k \in (0,1)$ it must be true that

$$\begin{aligned}
& 0 \leq k_{\tau}^{ap} \leq 1 \\
& \Rightarrow 0 \leq 1-\frac{\alpha_3^2-\alpha_1^2}{m_w(1-\alpha_1^2)} \leq 1 \\
& \Rightarrow \frac{\alpha_3^2-\alpha_1^2}{m_w(1-\alpha_1^2)} \leq 1 \cap \frac{\alpha_3^2-\alpha_1^2}{m_w(1-\alpha_1^2)} \geq 0
\end{aligned}$$

Substituting expressions for α_1, α_3 we get for $\frac{\alpha_3^2-\alpha_1^2}{m_w(1-\alpha_1^2)} \leq 1$,

$$\begin{aligned}
m_w &\geq \frac{\left(\frac{2c+t+z}{2(c+t+z)}\right)^2 - \left(\frac{c}{c+z+t(1-m_w)}\right)^2}{1-\left(\frac{c}{c+z+t(1-m_w)}\right)^2} \\
&\Rightarrow m_w - m_w\left(\frac{c}{c+z+t(1-m_w)}\right)^2 \geq \left(\frac{2c+t+z}{2(c+t+z)}\right)^2 - \left(\frac{c}{c+z+t(1-m_w)}\right)^2 \\
&\Rightarrow m_w + \left(\frac{c}{c+z+t(1-m_w)}\right)^2(1-m_w) \geq \left(\frac{2c+t+z}{2(c+t+z)}\right)^2 \\
&\Rightarrow 1-(1-m_w) + \left(\frac{c}{c+z+t(1-m_w)}\right)^2(1-m_w) \geq \left(\frac{2c+t+z}{2(c+t+z)}\right)^2 \\
&\Rightarrow 1-M+M\left(\frac{c}{c+z+tM}\right)^2 \geq \left(\frac{2c+t+z}{2(c+t+z)}\right)^2
\end{aligned}$$

where $M = 1-m_w$. Simplifying the above expression we get a cubic polynomial in M as follows:

$$-M^3t^2+2tM^2\left(\frac{1-\alpha_3}{2}-(c+z)\right)+\left(2t(c+z)(1-\alpha_3)-2cz-z^2\right)M+(c+z)^2(1-\alpha_3) \geq 0 \tag{A.18}$$

Suppose the LHS cubic polynomial is denoted P_M. Given that P_M can never always be increasing or decreasing, it is sufficient to establish that the polynomial has at least one root of $M \in (0,1)$ such that the polynomial is increasing or decreasing greater or less than that root. For that, suppose P_M has three roots m_1, m_2, m_3. Then it must be true that

$$\begin{aligned}
m_1m_2m_3 &= \frac{(c+z)^2(1-\alpha_3)}{t^2} > 0 \\
\sum_{i,j} m_im_j &= -\frac{2t(c+z)(1-\alpha_3)-2cz-z^2}{t^2}, i \neq j,\ i,j = \{1,2,3\} \\
m_1+m_2+m_3 &= \frac{(1-\alpha_3)-2(c+z)}{t} < 0
\end{aligned}$$

By construction, $M \in (0,1)$. So, product of all roots being positive implies either all are positive or only one is positive, other two being negative. Further, summation of all roots being negative implies that all roots cannot be positive. Hence only one possibility remains that $\exists\ m_i > 0 \in (0,1),\ i \in \{1,2,3\}$, while $m_j, m_k < 0,\ i \neq j, i \neq k,\ i,j,k \in \{1,2,3\}$. This can also be verified by the Intermediate value theorem where substituting $M = 0$ in cubic equation, we have

$$\begin{aligned} M = 0 &\Rightarrow P_M \equiv (c+z)^2(1-\alpha_3) > 0 \\ M = 1 &\Rightarrow P_M \equiv c^2 - \alpha_3(c+z+t)^2 < 0 \end{aligned}$$

So, $P_M(M = 0) > 0$ and $P_M(M = 1) < 0$ implying there must be at least one $M \in (0,1)$ such that $P_M(M) = 0$. So for a given $k_\tau^{ap} \in (0,1)$, for Ad-exchange to be a better model than Paid, $\exists\ \hat{m_w}$ such that $P_M \geq 0,\ m_w \in (\hat{m_w}, 1)$ such that any revenue sharing $k \in (0, k_\tau^{ap})$ is valid for CP to enjoy better returns from Ad-exchange than from Paid.

Conversely, solving the inequality

$$\begin{aligned} &k \leq 1 - \frac{\alpha_3^2 - \alpha_1^2}{m_w(1-\alpha_1^2)} \\ &\Rightarrow k m_w(1-\alpha_1^2) \leq m_w(1-\alpha_1^2) - (\alpha_3^2 - \alpha_1^2) \\ &\Rightarrow m_w(1-\alpha_1^2)(k-1) + (\alpha_3^2 - \alpha_1^2) \leq 0 \\ &\Rightarrow (1-M)(1-\alpha_1^2)(k-1) + (\alpha_3^2 - \alpha_1^2) \leq 0 \\ &\Rightarrow (1-M)(1 - \frac{c^2}{(c+z+tM)^2})(k-1) + (\alpha_3^2 - \frac{c^2}{(c+z+tM)^2}) \leq 0 \\ &\Rightarrow (1-M)((c+z+tM)^2 - c^2)(k-1) + \alpha_3^2(c+z+tM)^2 - c^2 \leq 0 \end{aligned}$$

we have a cubic polynomial P_M in M. For this polynomial to have at least one real root in $(0,1)$, it must be true that $P_M(M = 0)$ and $P_M(M = 1)$ should be of opposite sign. In fact, $P_M(M = 1) > 0$ and for $P_M(M = 0) < 0$, following must hold:

$k < 1 - \alpha_3^2$. Therefore the following can be said about CP: For $k \in (0, 1 - \alpha_3^2)$ & $m_w \in (\widehat{m_w}, 1)$ where $\widehat{m_w}$ satisfies:

$$m_w + (1 - m_w)\left(\frac{c}{c + z + t(1 - m_w)}\right)^2 \geq \left(\frac{2c + t + z}{2(c + t + z)}\right)^2$$

$$m_w((c + z + t(1 - m_w))^2 - c^2)(k - 1) + \left(\frac{2c + t + z}{2(c + t + z)}\right)^2 (c + z + t(1 - m_w))^2 - c^2 \leq 0$$

CP is better off under Ad-Exchange than under Paid model. ■

A.6 Proof Lemma 5

Proof Comparing CP Welfare/payoff, $\pi_{CP}^{\text{ad-ex}} - \pi_{CP}^{\text{frm}}$:

$$\frac{(1 - k)m_w}{2}\left(1 - \alpha_1^2\right) + \frac{\alpha_1^2}{2} - \frac{m_w}{2}\left(\alpha_2^2 - \alpha_1^2\right) - \frac{1}{2}\left(\alpha_1\right)^2$$

Threshold for k to be defined here is

$$k \leq 1 - \frac{\frac{1}{4} - \alpha_1^2}{1 - \alpha_1^2} \tag{A.19}$$

such that $k \in (0, 1 - \frac{\frac{1}{4} - \alpha_1^2}{1 - \alpha_1^2})$ for Ad-Exchange to be a better model than Freemium. Again, substituting α_1 we have,

$$\begin{aligned}
& k \leq 1 - \frac{\frac{1}{4} - \left(\frac{c}{c+z+t(1-m_w)}\right)^2}{1 - \left(\frac{c}{c+z+t(1-m_w)}\right)^2} \\
& \Rightarrow \frac{\frac{1}{4} - \left(\frac{c}{c+z+t(1-m_w)}\right)^2}{1 - \left(\frac{c}{c+z+t(1-m_w)}\right)^2} \leq 1 - k \\
& \Rightarrow \frac{(c + z + t(1 - m_w))^2 - 4c^2}{4\left((c + z + t(1 - m_w))^2 - c^2\right)} \leq 1 - k \\
& \Rightarrow (c + z + tM)^2 - 4c^2 \leq 4(c + z + tM)^2 - 4c^2 - k(4(c + z + tM)^2 - 4c^2)
\end{aligned}$$

This is a quadratic expression in M denoted Q_M, the discriminant of the quadratic expression should be non-negative for there to exist at least one root $M \in (0, 1)$. Therefore, collecting terms for coefficients of M, M^2 and constant term, we have that since $Q_M(M = 0)$ and $Q_M(M = 1)$ take negative values for $k < \frac{3}{4}$, the CP is better off with Ad-Exchange for $m_w \in (0, m_1) \cup (m_2, 1)$ and $k < \frac{3}{4}$. Otherwise, Freemium is better.

A.7 Proof Proposition 2

For CP welfare comparison,

$$\pi_{CP}^{\text{frm}} = \frac{m_w}{2}\left(\frac{1}{4} - \left(\frac{c}{c + z + t(1 - m_w)}\right)^2\right) + \frac{1}{2}\left(\frac{c}{c + z + t(1 - m_w)}\right)^2 - \frac{1}{2}\left(\frac{2c + t + z}{2(c + t + z)}\right)^2$$

which simplifies for sake of comparison,

$$m_w\left(\frac{1}{4} - \alpha_1^2\right) + \left(\alpha_1^2 - \alpha_3^2\right)$$

Analyzing expression, we have that for Freemium to be better than paid, m_w should be such that $m_w \in (0, 1)$ and

$$m_w \geq \frac{\alpha_3^2 - \alpha_1^2}{\frac{1}{4} - \alpha_1^2}$$

The RHS of inequality should obey

$$0 \leq \frac{\alpha_3^2 - \alpha_1^2}{\frac{1}{4} - \alpha_1^2} \leq 1$$
$$\Rightarrow \frac{\alpha_3^2 - \alpha_1^2}{\frac{1}{4} - \alpha_1^2} \geq 0 \cup \frac{\alpha_3^2 - \alpha_1^2}{\frac{1}{4} - \alpha_1^2} \leq 1$$

The expression is trivially non-negative, given α_1, α_3. However, since $\alpha_3 > \frac{1}{2}$, it must be true that $\alpha_3^2 > \frac{1}{4} \Rightarrow \alpha_3^2 - \alpha_1^2 > \frac{1}{4} - \alpha_1^2$. More specifically,

$$\frac{\alpha_3^2 - \alpha_1^2}{\frac{1}{4} - \alpha_1^2} > 1$$

This implies that $m_w \geq \frac{\alpha_3^2 - \alpha_1^2}{\frac{1}{4} - \alpha_1^2} > 1$ does not hold and so, Freemium cannot be better than paid. So, there doesn't exist $m_w \in (0,1)$ such that Freemium is better than Paid. Hence for CP, Paid is always better than Freemium.

A.8 Proof Lemma 6

Considering AB, comparing the two revenue models,

$$\frac{km_w}{2}\left(1-\alpha_1^2\right) + \gamma_w^L m_w - \left(\frac{t+z}{2}\right)(1-\alpha_3)$$

Checking for ranges where Ad-Exchange is better than paid, it is clear that

$$\begin{aligned}
&\frac{km_w}{2}\left(1-\alpha_1^2\right) + \gamma_w^L m_w \geq \left(\frac{t+z}{2}\right)(1-\alpha_3) \\
&\Rightarrow km_w\left(1-\alpha_1^2\right) \geq (t+z)(1-\alpha_3) - 2\gamma_w^L m_w \\
&\Rightarrow k \geq \frac{(t+z)(1-\alpha_3)}{m_w\left(1-\alpha_1^2\right)} - \frac{2\gamma_w^L}{\left(1-\alpha_1^2\right)}
\end{aligned}$$

It must be true that:

$$\begin{aligned}
&0 \leq \frac{(t+z)(1-\alpha_3)}{m_w\left(1-\alpha_1^2\right)} - \frac{2\gamma_w^L}{\left(1-\alpha_1^2\right)} \leq 1 \\
&\Rightarrow \frac{(t+z)(1-\alpha_3)}{m_w\left(1-\alpha_1^2\right)} \geq \frac{2\gamma_w^L}{\left(1-\alpha_1^2\right)} \cap \frac{(t+z)(1-\alpha_3)}{m_w\left(1-\alpha_1^2\right)} \leq 1 + \frac{2\gamma_w^L}{\left(1-\alpha_1^2\right)}
\end{aligned}$$

From the first inequality, we have that $m_w \leq \frac{(t+z)(1-\alpha_3)}{2\gamma_w^L}$ and from second, it is true for all $m_w \in (\underline{m_w}, 1)$. Solving the original inequality we have that for $m_w \in (0,1)$ for at least one value, we must have that $k > (1-\alpha_3)(z+t) - 2\gamma_w^L$. Hence, for Ad-Exchange to be better model for AB, $k \in ((1-\alpha_3)(z+t) - 2\gamma_w^L, 1)$ and $m_w \in (\underline{m_w}, \frac{(t+z)(1-\alpha_3)}{2\gamma_w^L})$ where $\underline{m_w}$ satisfies:

$$\frac{(t+z)(1-\alpha_3)}{m_w\,(1-\alpha_1^2)} \leq 1 + \frac{2\gamma_w^L}{(1-\alpha_1^2)}$$

■

A.9 Proof Proposition 3

Proof Comparing AB models for Ad-Exchange & Freemium,

$$\begin{aligned}
&\frac{km_w}{2}\left(1-\alpha_1^2\right) + p_w m_w - \left(p_w m_w + \frac{tm_w}{4}\right)\\
&\Rightarrow \frac{km_w}{2}\left(1-\alpha_1^2\right) - \frac{tm_w}{4}
\end{aligned}$$

Substituting value for $\alpha_1 = \frac{c}{c+z+t(1-m_w)}$ we have that for Ad-Exchange to better than Freemium following should hold

$$\begin{aligned}
&\frac{km_w}{2}\left(1-\alpha_1^2\right) - \frac{tm_w}{4} \geq 0\\
&\Rightarrow k \geq \frac{t}{2(1-\alpha_1^2)}\\
&\Rightarrow k \geq \frac{t}{2(1-\left(\frac{c}{c+z+t(1-m_w)}\right)^2)}\\
&\Rightarrow 2k - \frac{2kc^2}{(c+z+t(1-m_w))^2} - t \geq 0\\
&\Rightarrow 2k(c+z+t(1-m_w))^2 - 2kc^2 - t(c+z+t(1-m_w))^2 \geq 0
\end{aligned}$$

This is a quadratic expression in $M = 1 - m_w$ with discriminant as $8c^2kt^2(2k-t)$ and values at the domain extremes $M = 0$ and $M = 1$ as positive, given $c, t \in (0,1)$ and $z \in (1, v)$. Therefore for there to exist roots in interior of domain it must be true that $8c^2kt^2(2k-t) > 0 \Rightarrow k > \frac{t}{2}$. Hence, it is clear from the quadratic equation that for $k > \frac{t}{2}$ and $m_w \in (m_1, m_2)$, Ad-Exchange is better than Freemium. Otherwise Freemium is better. Comparing Freemium and Paid business models for AB we have

$$\gamma_w^H m_w + \frac{tm_w}{4} - \left(\frac{t+z}{2}\right)(1-\alpha_3)$$

Solving for m_w it is clear that,

$$\begin{aligned} m_w\left(\frac{t}{4}+\gamma_w^H\right) &\geq \left(\frac{t+z}{2}\right)(1-\alpha_3) \\ \Rightarrow m_w &\geq \left(\frac{t+z}{(\frac{t}{2}+2\gamma_w^H)}\right)(1-\alpha_3) \end{aligned}$$

Hence, for values of $m_w \in \left(\left(\frac{t+z}{(\frac{t}{2}+2\gamma_w^H)}\right)(1-\alpha_3), 1\right)$ Freemium is better than Paid. ■

A.10 Proof Lemma 7

Proof Consider Ad-Ex vs. Ad-Ex. Following are true for benefits z_i:

$$\begin{aligned} \frac{\partial \pi^*_{AB1}}{\partial z_1} &= \frac{m_1}{c_1+c_2+2k_f} > 0 \\ \frac{\partial \pi^*_{AB1}}{\partial z_2} &= -\frac{m_1}{c_1+c_2+2k_f} < 0 \\ \frac{\partial \pi^*_{AB2}}{\partial z_1} &= -\frac{m_2}{c_1+c_2+2k_f} < 0 \\ \frac{\partial \pi^*_{AB2}}{\partial z_2} &= \frac{m_2}{c_1+c_2+2k_f} > 0 \end{aligned}$$

So both AB's benefit from own increase in club benefits but are hurt by other's increase in benefits. Finally,

$$\begin{aligned}
\frac{\partial \pi^*_{AB1}}{\partial c_1} &= -m_1 \left(\frac{c_2 + k_f + z_1 - z_2 + t(m_2 - m_1)}{(c_1 + c_2 + 2k_f)^2} \right) < 0 \\
\frac{\partial \pi^*_{AB1}}{\partial c_2} &= m_1 \left(\frac{c_1 + k_f + z_2 - z_1 + t(m_1 - m_2)}{(c_1 + c_2 + 2k_f)^2} \right) > 0 \\
\frac{\partial \pi^*_{AB2}}{\partial c_2} &= -m_2 \left(\frac{c_1 + k_f + z_2 - z_1 + t(m_1 - m_2)}{(c_1 + c_2 + 2k_f)^2} \right) < 0 \\
\frac{\partial \pi^*_{AB2}}{\partial c_1} &= m_2 \left(\frac{c_2 + k_f + z_1 - z_2 + t(m_2 - m_1)}{(c_1 + c_2 + 2k_f)^2} \right) > 0
\end{aligned}$$

Congestion costs also have opposite effect on profits as benefits.

Now consider Ad-ex vs. Paid. For increase in z_1, z_2,

$$\begin{aligned}
\frac{\partial \pi^*_{AB1}}{\partial z_1} &= \frac{m_1}{2(c_1 + c_2 + k_f + k_p)} > 0 \\
\frac{\partial \pi^*_{AB2}}{\partial z_1} &= -\frac{c_1 + tm_1 + k_f + z_2 - z_1}{2(c_1 + c_2 + k_f + k_p)} < 0 \\
\frac{\partial \pi^*_{AB2}}{\partial z_2} &= \frac{c_1 + tm_1 + k_f + z_2 - z_1}{2(c_1 + c_2 + k_f + k_p)} > 0 \\
\frac{\partial \pi^*_{AB1}}{\partial z_2} &= -\frac{m_1}{2(c_1 + c_2 + k_f + k_p)} < 0
\end{aligned}$$

and for increase in congestion costs,

$$\begin{aligned}
\frac{\partial \pi^*_{AB1}}{\partial c_1} &= -m_1 \left(\frac{c_2 + k_p + z_1 - z_2 - tm_1}{2(c_1 + c_2 + k_f + k_p)^2} \right) < 0 \\
\frac{\partial \pi^*_{AB1}}{\partial c_2} &= m_1 \left(\frac{c_1 + k_f + z_2 - z_1 + tm_1}{2(c_1 + c_2 + k_f + k_p)^2} \right) > 0 \\
\frac{\partial \pi^*_{AB2}}{\partial c_2} &= -\frac{(c_1 + tm_1 + k_f + z_2 - z_1)^2}{4(c_1 + c_2 + k_f + k_p)^2} < 0 \\
\frac{\partial \pi^*_{AB2}}{\partial c_1} &= \frac{(c_1 + 2c_2 + k_f + 2k_p + z_1 - z_2 - tm_1)(c_1 + tm_1 + k_f + z_2 - z_1)}{4(c_1 + c_2 + k_f + k_p)^2} > 0
\end{aligned}$$

Now consider Ad-ex vs. Freemium. Suppose AB1 is Freemium and AB2 is Ad-Ex. It is clear that since in Freemium, AB doesn't earn from free members but from price of whitelisting, at equilibrium

$$p_1^* = \frac{tm_1}{2}$$

Hence $\pi^*_{AB1} = m_1\gamma_1 + \frac{t^2m_1^2}{4(k_p-k_f)}$. It is clear from the expression that this is a concave function in m_1 which does not depend on c_1. Hence $\frac{\partial\pi^*_{AB1}}{\partial c_1} = \frac{\partial\pi^*_{AB1}}{\partial c_2} = 0$. Further, $\frac{\partial\pi^*_{AB2}}{\partial c_1} = m_1\left(\frac{c_2+k_f+z_1-z_2+t(m_1-m_2)}{2(c_1+c_2+2k_f)^2}\right) > 0$ and $\frac{\partial\pi^*_{AB2}}{\partial c_2} = -m_2\frac{(c_1+k_f+z_2-z_1+t(m_1-m_2))}{2(c_1+c_2+2k_f)^2} < 0$ still hold. For all other Freemium competition models, this holds true since each case, differentiation expressions are one of the earlier derived ones. ■

A.11 Proof Proposition 4

Proof Consider Ad-Exchange vs. Ad-Exchange. Users choose from two Free ABs essentially. Solving for indifferent user at $x \in (0,1)$ we have that

$$x = \frac{z_1 - z_2 + k_f + c_2n_2 - c_1n_1 + t(m_2 - m_1)}{2k_f}$$

Solving for member masses, we have in Stage 2,

$$n_1 = 1 - \frac{c_1 + k_f - (z_1 - z_2 + t(m_2 - m_1))}{c_1 + c_2 + 2k_f}$$
$$n_2 = 1 - \frac{c_2 + k_f - (z_2 - z_1 + t(m_1 - m_2))}{c_1 + c_2 + 2k_f}$$

Hence user participation is a function of m_i, z_i, c_i. Each of these parameters is exogenous but can change with change in AB technology. Substituting user masses in first stage equations for AB we have

$$\pi_{AB1} = m_1\left(1 - \frac{c_1 + k_f - (z_1 - z_2 + t(m_2 - m_1))}{c_1 + c_2 + 2k_f}\right)$$
$$\pi_{AB2} = m_2\left(1 - \frac{c_2 + k_f - (z_2 - z_1 + t(m_1 - m_2))}{c_1 + c_2 + 2k_f}\right)$$

It is clear to see that:

$$\frac{\partial \pi^*_{AB1}}{\partial m_1} = \left(1 - \frac{c_1 + k_f - (z_1 - z_2 + t(m_2 - m_1))}{c_1 + c_2 + 2k_f}\right) + m_1\left(-\frac{t}{c_1 + c_2 + 2k_f}\right)$$
$$\Rightarrow \left(1 - \frac{c_1 + k_f - (z_1 - z_2 + t(m_2 - m_1))}{c_1 + c_2 + 2k_f}\right) - m_1\left(\frac{t}{c_1 + c_2 + 2k_f}\right)$$
$$\Rightarrow \frac{c_2 + k_f + t(m_2 - 2m_1) + z_1 - z_2}{c_1 + c_2 + 2k_f} > 0$$

given parameter ranges and boundary condition while,

$$\frac{\partial \pi^*_{AB2}}{\partial m_2} = \frac{c_1 + k_f + t(m_1 - 2m_2) + z_2 - z_1}{c_1 + c_2 + 2k_f} > 0$$

is also true. More specifically, the points at which both the expressions equal zero are for values of m_1, m_2 that are clearly greater than one. Hence, both expressions are positive in the domain $m_w \in (0, 1)$. Further, it is also true that

$$\frac{\partial \pi^*_{AB1}}{\partial m_2} = \frac{tm_1}{c_1 + c_2 + 2k_f} > 0$$
$$\frac{\partial \pi^*_{AB1}}{\partial m_2} = \frac{tm_2}{c_1 + c_2 + 2k_f} > 0$$

So both ad-blockers benefit from increase in mass of whitelisters at either AB.

Consider the Ad-Ex vs. Paid duopoly. Assume AB1 is Ad-Exchange and AB2 is Paid. Solving for indifferent user we have,

$$x = \frac{z_1 - z_2 + p_2 + k_p + c_2 n_2 - c_1 n_1 - t m_1}{k_f + k_p}$$

Solving for member masses, we have in Stage 2,

$$\begin{aligned} n_1 &= 1 - \frac{c_1 + k_f + t m_1 - p_2 - (z_1 - z_2)}{c_1 + c_2 + k_f + k_p} \\ n_2 &= 1 - \frac{c_2 + k_p + z_1 - z_2 + p_2 - t m_1}{c_1 + c_2 + k_f + k_p} \end{aligned}$$

Solving for optimal price in Stage 1, we have $p_2^* = \frac{c_1 + t m_1 + k_f + z_2 - z_1}{2}$. Substituting in expressions we have equilibrium masses as,

$$\begin{aligned} n_1^* &= \frac{1}{2}\left(\frac{c_1 + 2c_2 + k_f + 2k_p + z_1 - z_2 - t m_1}{c_1 + c_2 + k_f + k_p}\right) \\ n_2^* &= \frac{1}{2}\left(\frac{c_1 + k_f + z_2 - z_1 + t m_1}{c_1 + c_2 + k_f + k_p}\right) \end{aligned}$$

and therefore equilibrium profits are:

$$\begin{aligned} \pi_{AB1}^* &= \frac{m_1}{2}\left(\frac{c_1 + 2c_2 + k_f + 2k_p + z_1 - z_2 - t m_1}{c_1 + c_2 + k_f + k_p}\right) \\ \pi_{AB2}^* &= \frac{(c_1 + t m_1 + k_f + z_2 - z_1)^2}{4(c_1 + c_2 + k_f + k_p)} \end{aligned}$$

Hence user participation is a function of same three variables. First note that p_2^* is increasing in m_1, c_1, z_2 and decreasing in z_1. Further, for m_1 increase:

$$\begin{aligned} \frac{\partial \pi_{AB1}^*}{\partial m_1} &= \frac{c_1 + 2c_2 + k_f + 2k_p + z_1 - z_2 - 2t m_1}{c_1 + c_2 + k_f + k_p} > 0 \\ \frac{\partial \pi_{AB2}^*}{\partial m_1} &= \frac{t(c_1 + t m_1 + k_f + z_2 - z_1)}{4(c_1 + c_2 + k_f + k_p)} > 0 \end{aligned}$$

both AB's benefit from it.

Now consider Freemium vs. Ad-Ex. There are two indifference points here – one for a free vs. paid user for freemium AB and the other, free vs. ad-exchange user for the other AB. Assume AB1 is freemium and AB2 is Ad-Exchange. Accordingly, the two indifference users are:

$$x_1 = \frac{tm_1 - p_1}{k_p - k_f}, \quad \text{Freemium Indifferent User}$$
$$x_2 = \frac{z_1 - z_2 + k_f + c_2 n_2 - c_1 n_1 + t(m_2 - m_1)}{2k_f}, \quad \text{Ad-Exchange Indifferent User}$$

Solving for Stage 2 masses, we have same result as Ad-Exchange competition:

$$n_1 = 1 - \frac{c_1 + k_f - (z_1 - z_2 + t(m_2 - m_1))}{c_1 + c_2 + 2k_f}$$
$$n_2 = 1 - \frac{c_2 + k_f - (z_2 - z_1 + t(m_1 - m_2))}{c_1 + c_2 + 2k_f}$$

The first stage AB1 problem is $\max_{p_1} \gamma_1 m_1 + p_1 \left(1 - \frac{tm_1 - p_1}{k_p - k_f}\right)$, concave in p_1. Hence, price at equilibrium is $p_1^* = \frac{m_1 t}{2}$. So, premium membership is $x_1^* = \frac{tm_1}{2(k_p - k_f)}$. Using boundary conditions this can be shown to be less than x_2^*, and greater than zero. Further, effect of increase in m_1, m_2 is the same where

$$\frac{\partial \pi^*_{AB1}}{\partial m_1} = \gamma_1 + \frac{t^2 m_1}{2(k_p - k_f)} > 0$$
$$\frac{\partial \pi^*_{AB1}}{\partial m_2} = 0$$
$$\frac{\partial \pi^*_{AB2}}{\partial m_1} = \frac{tm_2}{c_1 + c_2 + 2k_f} > 0$$
$$\frac{\partial \pi^*_{AB2}}{\partial m_2} = \frac{c_1 + k_f + z_2 - z_1 + t(m_1 - 2m_2)}{c_1 + c_2 + 2k_f} > 0$$

In the case of Freemium vs. Paid, there are two indifferent user points – one for a free vs. paid user for freemium AB and the other, free vs. paid user for the other

AB. Assume AB1 is freemium and AB2 is Paid. Accordingly, the two indifference users are:

$$\begin{aligned} x_1 &= \frac{tm_1 - p_1}{k_p - k_f}, \quad \text{Freemium Indifferent User} \\ x_2 &= \frac{z_1 - z_2 + k_p + c_2 n_2 - c_1 n_1 - tm_1}{k_p + k_f}, \quad \text{Paid Indifferent User} \end{aligned}$$

Solving for Stage 2 masses, we have same result as Ad-Exchange competition:

$$\begin{aligned} n_1 &= 1 - \frac{c_1 + k_f + tm_1 - p_2 - (z_1 - z_2)}{c_1 + c_2 + k_f + k_p} \\ n_2 &= 1 - \frac{c_2 + k_p + z_1 - z_2 + p_2 - tm_1}{c_1 + c_2 + k_f + k_p} \end{aligned}$$

Solving for equilibrium prices in Stage 1, we have

$$\begin{aligned} p_1^* &= \frac{tm_1}{2} \\ p_2^* &= \frac{c_1 + tm_1 + k_f + z_2 - z_1}{2} \end{aligned}$$

Substituting and simplifying, the equilibrium masses for both ABs are:

$$\begin{aligned} n_1^* &= \frac{1}{2}\left(\frac{c_1 + 2c_2 + k_f + 2k_p + z_1 - z_2 - tm_1}{c_1 + c_2 + k_f + k_p}\right) \\ n_2^* &= \frac{1}{2}\left(\frac{c_1 + k_f + z_2 - z_1 + tm_1}{c_1 + c_2 + k_f + k_p}\right) \end{aligned}$$

where premium members are $n_1^{*p} = \frac{tm_1}{2(k_p - k_f)}$. Similar to Ad-Exchange vs. Freemium,

$$\begin{aligned} \frac{\partial \pi_{AB1}^*}{\partial m_1} &= \gamma_1 + \frac{t^2 m_1}{2(k_p - k_f)} > 0 \\ \frac{\partial \pi_{AB1}^*}{\partial m_2} &= 0 \\ \frac{\partial \pi_{AB2}^*}{\partial m_1} &= \frac{t(tm_1 + c_1 + k_f + z_2 - z_1)}{2(c_1 + c_2 + k_f + k_p)} > 0 \\ \frac{\partial \pi_{AB2}^*}{\partial m_2} &= 0 \end{aligned}$$

Hence, insights are same too.

Finally, in the case of Freemium vs. Freemium, participating masses in Stage 2 is similar to Ad-Exchange vs. Ad-Exchange. That is, in Stage 2,

$$n_1 = 1 - \frac{c_1 + k_f - (z_1 - z_2 + t(m_2 - m_1))}{c_1 + c_2 + 2k_f}$$
$$n_2 = 1 - \frac{c_2 + k_f - (z_2 - z_1 + t(m_1 - m_2))}{c_1 + c_2 + 2k_f}$$

are the total participating masses in two Freemium ABs in Stage 2. Solving for premium member masses in Stage 2 we have

$$x_1 = \frac{tm_1 - p_1}{k_p - k_f}, \quad \text{Freemium Indifferent User for AB1}$$
$$x_2 = 1 - \frac{tm_1 - p_2}{k_p - k_f}, \quad \text{Freemium Indifferent User for AB2}$$

Stage 1 Equilibrium prices are:

$$p_1^* = \frac{tm_1}{2}$$
$$p_2^* = \frac{tm_2}{2}$$

Equilibrium masses for premium members are:

$$n_1^{*p} = \frac{tm_1}{2(k_p - k_f)}$$
$$n_2^{*p} = \frac{tm_2}{2(k_p - k_f)}$$

while free members are

$$n_1^{*f} = \frac{c_2 + k_f + t(m_2 - m_1) + z_1 - z_2}{c_1 + c_2 + 2k_f} - \frac{tm_1}{2(k_p - k_f)}$$
$$n_2^{*f} = \frac{tm_2}{2(k_p - k_f)} - \frac{c_2 + k_f + t(m_2 - m_1) + z_1 - z_2}{c_1 + c_2 + 2k_f}$$

Effect of increase in m_1, m_2,

$$\begin{aligned}
\frac{\partial \pi^*_{AB1}}{\partial m_1} &= \gamma_1 + \frac{t^2 m_1}{2(k_p - k_f)} > 0 \\
\frac{\partial \pi^*_{AB1}}{\partial m_2} &= 0 \\
\frac{\partial \pi^*_{AB2}}{\partial m_1} &= 0 \\
\frac{\partial \pi^*_{AB2}}{\partial m_2} &= \gamma_2 + \frac{t^2 m_2}{2(k_p - k_f)} > 0
\end{aligned}$$

Hence, increase in whitelisting never hurts but benefits ABs. ■

A.12 Proof Proposition 5

Proof For the Paid vs. Paid case, we have that Stage 2 masses are:

$$\begin{aligned}
n_1 &= 1 - \frac{(p_1 - p_2) + z_2 - z_1 + c_1 + k_p}{c_1 + c_2 + 2k_p} \\
n_2 &= 1 - \frac{(p_2 - p_1) + z_1 - z_2 + c_2 + k_p}{c_1 + c_2 + 2k_p}
\end{aligned}$$

Solving for optimal prices in Stage 1, we have that:

$$\begin{aligned}
p_1^* &= \frac{c_1 + 2c_2 + 3k_p + z_1 - z_2}{3} \\
p_2^* &= \frac{c_2 + 2c_1 + 3k_p + z_2 - z_1}{3}
\end{aligned}$$

Note that optimal prices are increasing in both congestion costs. Further, prices are increasing in self benefits but decreasing in others benefits. Solving for equilibrium masses we have:

$$n_1^* = \frac{c_1 + 2c_2 + 3k_p + z_1 - z_2}{3(c_1 + c_2 + 2k_p)}$$
$$n_2^* = \frac{c_2 + 2c_1 + 3k_p + z_2 - z_1}{3(c_1 + c_2 + 2k_p)}$$

So at equilibrium, the profits are increasing in congestion costs:

$$\frac{\partial \pi_{AB1}^*}{\partial c_1} = \frac{(c_1 + 2c_2 + 3k_p + z_1 - z_2)(c_1 + k_p + z_2 - z_1)}{9(c_1 + c_2 + 2k_p)^2} > 0$$
$$\frac{\partial \pi_{AB1}^*}{\partial c_2} = \frac{(c_1 + 2c_2 + 3k_p + z_1 - z_2)(3c_1 + 2c_2 + 5k_p + z_2 - z_1)}{9(c_1 + c_2 + 2k_p)^2} > 0$$

and

$$\frac{\partial \pi_{AB2}^*}{\partial c_1} = \frac{(c_2 + 2c_1 + 3k_p + z_2 - z_1)(2c_1 + 3c_2 + 5k_p + z_1 - z_2)}{9(c_1 + c_2 + 2k_p)^2} > 0$$
$$\frac{\partial \pi_{AB2}^*}{\partial c_2} = \frac{(c_2 + 2c_1 + 3k_p + z_2 - z_1)(c_2 + k_p + z_1 - z_2)}{9(c_1 + c_2 + 2k_p)^2} > 0$$

while profits are increasing in self benefits and decreasing in others benefits. ■

A.13 Proof Proposition 6

Consider the user problem – selection between u_i, u_k, u_j where u_i, u_j are for paid AB users. Hence there are two indifference points, where on one indifference point x_1 user is indifferent between joining AB1 and not joining at all while on x_2, user is indifferent between joining AB2 and not joining at all.

Solving for stage 2 masses we have:

$$n_1 = \frac{z_1 + t - p_1}{c_1 + k_p}$$
$$n_2 = \frac{z_2 + t - p_2}{c_2 + k_p}$$

In the first stage, AB1 & 2 solve for optimal prices given these masses. Trivially concave, the optimal prices are:

$$p_1^* = \frac{t + z_1}{2}$$
$$p_2^* = \frac{t + z_2}{2}$$

Substituting back in stage 2 expressions, it is easy to see that

$$n_1^* = \frac{t + z_1}{2(c_1 + k_p)}$$
$$n_2^* = \frac{t + z_2}{2(c_2 + k_p)}$$

From here, it is clear that profits at equilibrium are $\pi^*_{AB1} = \frac{(t+z_1)^2}{4(c_1+k_p)}$ and $\pi^*_{AB2} = \frac{(t+z_2)^2}{4(c_2+k_p)}$. These are clearly decreasing in c_1, c_2 respectively and increasing in t, z_1 and t, z_2, respectively.

B. APPENDIX B

B.1 Proof Proposition 1 - Part 1

Proof This is a proof by contradiction. The basic strategy is to show that if there does exist a path that is not feasible, then by construction that path cannot represent a solution to the WDP-IP problem.

Suppose an infeasible path exists. By Definition 1, it is clear that since edges exist only between disjoint bundles, any infeasible path cannot be between nodes having items in common. Then the infeasible path will be such that it has at least one node that has more than one visits. A visit to a node implies allocation of the bundle by construction. By WDP-IP constraint equation (2), since each item up for auction can be allocated at most once, more than one visit implies that the bundles visited more than once have items that have been allocated more than once. But this is violates equation (2) of WDP-IP. Therefore, an infeasible path cannot represent a feasible solution to the WDP-IP problem. ■

B.2 Proof of Proposition 1 - Part 2

Proof This is a proof by contradiction. The basic strategy is to show that if there does exist a feasible path that does not have maximum weight then that cannot be equivalent to the optimal solution, as defined by WDP-IP.

Suppose there exists a feasible path $P^* \equiv \{s, v_z, v_{z+1}, ..., v_{z+p}, t\}$, such that it is the optimal solution to the problem but for contradiction does not have the maximum weight. From the WDP-IP and Proposition 1-Part 1, we know that any feasible path of the graph represents a feasible solution to WDP-IP. Hence, P^* is represented as an allocation with revenue $\sum_{j \in P^*} x_j q_j$ with $x_z = 1, x_{z+1} = 1, ..., x_{z+p} = 1$, all other

$x_j = 0 \; \forall \; j = \{1, 2, 3...l\} \setminus \{z, z+1, z+2, ...z+p\}$ bids such that $\sum\limits_{j=1}^{l} A_{ij}x_j \leq 1 \;\; \forall \;\; i \in \{1, 2, 3, 4...., k\}$ is satisfied. Since weights on edges are strictly positive, there must exist at least one node $v_j \in \{1, .., l\} \setminus \{z, .., z+p\}$ such that adding the node(s) to the path results in increasing the revenue from P^* (if not, then P^* has the maximum revenue, represents optimal solution and we are done). By feasibility, these nodes can only be added to the path such that bundles on the path are disjoint in nature. Hence, there must be at least one node that can be removed and replaced with other unselected nodes in the graph such that a new feasible path $P^{'}$ can be constructed that has $\sum_{j \in P^{'}} x_j q_j \geq \sum_{j \in P^*} x_j q_j$. But this implies that the existing feasible path is not optimal, which is a contradiction. Hence, a feasible path of maximum weight is an optimal solution to the WDP-IP problem. ■

B.3 Proof of Proposition 2

Proof This is a proof by induction. The basic idea is to show that as the number of ants $N \to \infty$, for positive values of $\tau_{min}, \alpha, \beta$ the probability that the ant system converges onto M_{opt} converges to 1. Suppose the probability of at least one ant traversing the optimal path is given by P_{opt}. For any ant at any node v_i, the probability of selecting the next node v_j in its neighborhood $(N(i))$ is given by $p_{ij} = \frac{\tau_{ij}^{\alpha}[w_{ij}]^{\beta}}{\sum_{j \in N(i)} \tau_{ij}^{\alpha}[w_{ij}]^{\beta}}$. Since pheromones are bounded by RPU $[\tau_{min}, \tau_{max}]$, $p_{ij} \geq p_{ij}^{\min} = \frac{\tau_{min}^{\alpha}[w_{ij}]^{\beta}}{\sum_{j \in N(i) \setminus q} \tau_{max}^{\alpha} w_{ij}^{\beta} + \tau_{min}^{\alpha} w_{iq}^{\beta}}$. The $p_{ij}^{\min}$ considers all edges from node v_i except those that have been randomly pruned by RGP. Further, $p_{ij}^{\min}$ considers all edges from v_i except one $(q \subset N(i))$ as having τ_{max} and that one edge q as having τ_{min} such that it has not been pruned.

Since each vertex is chosen stochastically given the current vertex an ant is on, the probability $\bar{p}$ of an ant traversing the optimal path M_{opt} of cardinality $|L|$ is such that $\bar{p} \geq (p_{ij}^{\min})^{|L|}$. Therefore, if N ants are used for solution construction, the probability that no ant traverses the optimal path is $(1 - \bar{p})^N$. Using this, we can express P_{opt} as

$$P_{opt} = 1 - (1 - \bar{p})^N \geq 1 - (1 - (p_{ij}^{\min})^{|L|})^N$$

Hence, $P_{opt} \geq 1-(1-(p_{ij}^{\min})^{|L|})^N$. Substituting expression for $p_{ij}^{\min} = \frac{\tau_{min}^{\alpha}[w_{ij}]^{\beta}}{\sum_{j\in N(i)\backslash q} \tau_{max}^{\alpha} w_{ij}^{\beta} + \tau_{min}^{\alpha} w_{iq}^{\beta}}$. we have that

$$P_{opt} \geq 1 - \left(1 - \left(\frac{\tau_{min}^{\alpha}[w_{ij}]^{\beta}}{\sum_{j\in N(i)\backslash q} \tau_{max}^{\alpha} w_{ij}^{\beta} + \tau_{min}^{\alpha} w_{iq}^{\beta}}\right)^{|L|}\right)^{N}$$

The expression within parenthesis can be made arbitrarily small using either larger N, and/or values of $\tau_{min}, \alpha, \beta$ s.t. $1-(p_{ij}^{\min})^{|L|}$ decreases. Hence, for values of $\tau_{min}, \alpha, \beta$ the probability P_{opt} can be made arbitrarily close to one. ■

B.4 TrACA Comparison

The experiments were run on an Intel i5-Core 3.5 GHz computer, Windows OS with 16GB RAM. The source code for preprocessing was written in R and for the ant colony system was written in MATLAB.

Table B.1.: Experimental Run Results - Test Instances 101-410

Instance	CPLEX	MA	ACLS	ACO Best	ACO Median	%Diff ACO Best vs. CPLEX	% Diff ACO Best vs. MA	% Diff ACO Best vs. ACLS
*in*101	67, 101.940	67, 101.930	69, 840.070	72, 724.620	69, 505.350	8.379	8.379	4.130
*in*102	72, 518	67, 797.610	70, 897.460	72, 391.300	70, 816.550	−0.175	6.776	2.107
*in*103	69, 791	66, 350.990	69, 791.250	70, 263.900	68, 500.380	0.678	5.897	0.677
*in*104	70, 951	64, 618.510	67, 268.710	72, 709.650	72, 709.650	2.479	12.521	8.088
*in*105	71, 852	66, 376.830	69, 834.280	74, 710.870	69, 655.450	3.979	12.556	6.983
*in*106	66, 621	65, 481.640	66, 436.080	70, 109.670	65, 481.070	5.237	7.068	5.530
*in*107	69, 182	66, 245.700	69, 182.250	69, 398.190	68, 556.220	0.312	4.759	0.312
*in*108	75, 147	74, 588.510	74, 588.510	75, 776.730	73, 403.750	0.838	1.593	1.593
*in*109	66, 439	62, 492.660	66, 239.280	68, 652.180	65, 638.600	3.331	9.856	3.643
*in*110	65, 215	65, 171.190	67, 395.070	68, 154.710	66, 103.890	4.508	4.578	1.127
*in*111	68, 411.910	72, 969.160	NA	74, 498.480	72, 711.300	8.897	2.096	NA
*in*112	71, 203.710	66, 671.670	NA	71, 342.480	70, 649.440	0.195	7.006	NA
*in*113	70, 960.220	68, 901.960	NA	72, 440.320	72, 440.320	2.086	5.135	NA
*in*114	66, 222.390	64, 190.630	NA	68, 239.570	67, 749.260	3.046	6.308	NA
*in*115	69, 312.600	62, 052.250	NA	69, 908.300	67, 582.560	0.859	12.660	NA
*in*116	65, 811.620	64, 849.850	NA	69, 093.730	68, 973.010	4.987	6.544	NA
*in*117	69, 354.130	66, 466.390	NA	69, 982.830	67, 505.990	0.907	5.291	NA
*in*118	68, 569.090	69, 239.960	NA	71, 385.200	67, 132.890	4.107	3.098	NA
*in*119	67, 038.420	63, 968.320	NA	66, 153.540	64, 083.190	−1.320	3.416	NA
*in*120	74, 660.720	68, 587.410	NA	74, 648.330	72, 865.390	−0.017	8.837	NA
*in*201	78, 114	77, 499.820	81, 557.740	81, 557.740	81, 557.740	4.409	5.236	0
*in*202	90, 708.120	90, 464.190	90, 464.190	90, 708.130	90, 333.850	0.00001	0.270	0.270
*in*203	86, 239.210	86, 239.210	86, 239.210	86, 239.210	86, 239.210	0	0	0
*in*204	84, 709.310	81, 969.050	87, 075.420	87, 075.430	85, 480.420	2.793	6.230	0.00001
*in*205	82, 464.150	82, 469.190	82, 469.190	86, 515.950	84, 840.310	4.913	4.907	4.907
*in*206	88, 478.770	86, 881.420	86, 881.420	91, 518.960	87, 755.490	3.436	5.338	5.338
*in*207	93, 129.240	91, 033.510	91, 033.510	93, 129.250	91, 247.660	0.00001	2.302	2.302
*in*208	94, 904.680	83, 667.760	91, 782.200	94, 904.680	91, 782.040	0	13.430	3.402
*in*209	83, 027.590	81, 966.650	81, 966.650	87, 268.960	86, 356.430	5.108	6.469	6.469
*in*210	86, 940.490	85, 079.980	87, 569.190	89, 962.400	86, 878.260	3.476	5.739	2.733
*in*211	83, 250.210	79, 746.140	NA	84, 913.680	83, 618.950	1.998	6.480	NA
*in*212	90, 778.200	81, 061.380	NA	90, 778.210	88, 124.010	0.00001	11.987	NA
*in*213	84, 487.620	83, 549.210	NA	85, 369.180	84, 169.240	1.043	2.178	NA
*in*214	85, 181.610	81, 935.320	NA	85, 181.610	84, 823.260	0	3.962	NA
*in*215	90, 538.840	83, 663.140	NA	91, 531.690	88, 879.960	1.097	9.405	NA
*in*216	88, 869.740	83, 286.630	NA	91, 580.930	91, 580.930	3.051	9.959	NA
*in*217	85, 267.590	83, 125.250	NA	86, 962.930	86, 895.060	1.988	4.617	NA
*in*218	89, 914.390	86, 936.780	NA	94, 965.190	90, 151.270	5.617	9.235	NA
*in*219	87, 883.450	88, 054.210	NA	90, 309.730	89, 760.600	2.761	2.562	NA
*in*220	87, 883.450	86, 937.850	NA	89, 792.910	88, 255.520	2.173	3.284	NA
*in*401	77, 417.480	72, 948.070	77, 417.480	77, 417.480	77, 417.480	0	6.127	0
*in*402	76, 273.330	71, 454.780	74, 469.070	76, 273.340	76, 273.340	0.00001	6.744	2.423
*in*403	74, 843.950	74, 843.960	74, 843.960	74, 843.960	74, 843.960	0.00001	0	0
*in*404	78, 761.690	78, 761.680	78, 761.680	78, 761.690	78, 761.690	0	0.00001	0.00001
*in*405	75, 915.900	72, 674.250	74, 899.120	75, 915.900	75, 336.860	0	4.461	1.358
*in*406	72, 863.320	71, 791.030	71, 791.030	72, 863.320	72, 863.320	0.00001	1.494	1.494
*in*407	76, 365.720	73, 935.280	73, 935.280	76, 365.720	76, 365.720	0	3.287	3.287
*in*408	77, 018.830	72, 580.040	77, 018.730	77, 018.830	77, 018.830	0	6.116	0.0001
*in*409	73, 188.620	68, 724.530	73, 188.620	73, 188.620	73, 188.620	0	6.496	0
*in*410	73, 791.650	71, 791.570	73, 791.660	73, 791.660	73, 710.070	0.00001	2.786	0

Table B.2.: Experimental Run Results - Test Instances 411-620

Instance	CPLEX	MA	ACLS	ACO Best	ACO Median	%Diff ACO Best vs. CPLEX	% Diff ACO Best vs. MA	% Diff ACO Best vs. ACLS
*in*411	73,935.400	71,200.550	NA	73,935.410	73,898.990	0.00001	3.841	NA
*in*412	75,292.630	75,292.630	NA	75,292.630	75,292.630	0	0	NA
*in*413	74,434.900	73,350.870	NA	74,434.990	74,434.990	0.0001	1.478	NA
*in*414	77,146.370	77,146.360	NA	77,146.370	76,749.550	0	0.00001	NA
*in*415	73,519.130	71,926.730	NA	73,519.130	73,519.130	0	2.214	NA
*in*416	73,487.010	72,520.660	NA	73,487.020	73,487.020	0.00001	1.333	NA
*in*417	74,981.350	74,680.990	NA	74,981.350	74,981.350	0	0.402	NA
*in*418	71,404.840	71,404.840	NA	71,404.840	71,404.840	0	0	NA
*in*419	72,505.210	70,472.840	NA	72,505.210	72,505.210	0	2.884	NA
*in*420	75,510.680	71,381.020	NA	75,510.680	75,510.680	0.00001	5.785	NA
*in*421	75,694.940	75,694.940	NA	75,694.950	74,729.600	0.00001	0.00001	NA
*in*422	77,443.910	72,850.900	NA	77,443.910	77,443.910	0	6.305	NA
*in*423	68,134.350	68,134.350	NA	68,134.350	68,134.350	0.00001	0.00001	NA
*in*424	77,352.760	73,196.150	NA	77,352.760	76,385.110	0	5.679	NA
*in*425	77,333.910	73,258.590	NA	77,333.910	77,333.910	0	5.563	NA
*in*426	76,430.180	74,524.800	NA	76,430.180	76,430.180	0	2.557	NA
*in*427	76,387.570	73,147.950	NA	76,387.570	76,387.570	0	4.429	NA
*in*428	77,384.940	76,554.580	NA	77,384.940	76,609.980	0	1.085	NA
*in*429	75,540.960	75,540.960	NA	75,540.960	75,540.960	0	0.00001	NA
*in*430	79,038.750	76,264.920	NA	79,038.750	79,038.750	0	3.637	NA
*in*501	88656.950	79,132.030	84,165.230	88,656.960	86,780.240	0.00001	12.037	5.337
*in*502	83757.540	80,340.760	83,163.660	86,236.910	84,915.890	2.87	7.339	3.695
*in*503	86318.170	83,277.710	83,277.710	86,318.180	85,106.870	0.00001	3.651	3.651
*in*504	84220.220	81,903.020	83,947.130	85,600.000	83,947.140	1.6	4.514	1.969
*in*601	106,817.500	99,044.320	105,286.700	108,800.400	105,058.500	1.856	9.850	3.337
*in*602	98,579.420	98,164.230	101,150.900	105,611.500	102,360.800	7.133	7.587	4.410
*in*603	98,953.480	94,126.960	96,628.980	105,121.000	99,171.900	6.233	11.680	8.788
*in*604	100,005.800	103,568.900	106,127.200	107,733.800	105,838.900	7.728	4.021	1.514
*in*605	105,105.200	102,404.800	106,273.500	109,841.000	105,925.800	4.506	7.262	3.357
*in*606	107,113.100	104,346.100	105,218.200	107,113.100	105,218.200	0.00001	2.652	1.801
*in*607	102,119.100	105,869.400	105,869.400	113,180.300	105,869.400	10.832	6.906	6.906
*in*608	101,044.800	95,671.770	99,541.750	105,266.100	104,285.700	4.178	10.028	5.751
*in*609	109,472.300	98,566.940	104,602.400	109,472.300	104,084.700	0	11.064	4.656
*in*610	106,453.600	102,468.600	109,008.400	113,717.000	111,487.900	6.823	10.977	4.319
*in*611	100,666.300	98,974.640	NA	106,666.300	101,902.400	5.960	7.771	NA
*in*612	109,796.700	106,056.100	NA	109,796.700	106,056.100	0	3.527	NA
*in*613	98,009.040	93,289.850	NA	107,980.200	105,559.100	10.174	15.747	NA
*in*614	102,002.600	97,510.720	NA	108,364.600	106,152.600	6.237	11.131	NA
*in*615	103,149.500	101,770.700	NA	110,508.800	108,615.900	7.135	8.586	NA
*in*616	105,412.700	100,169.500	NA	109,740.500	105,441.800	4.106	9.555	NA
*in*617	103,864.700	100,653.900	NA	113,302.400	106,931.500	9.087	12.566	NA
*in*618	101,855.300	102,378.300	NA	111,385.100	108,048.500	9.356	8.798	NA
*in*619	99,021.430	97,306.300	NA	107,571.600	105,627.100	8.635	10.549	NA
*in*620	102,111.700	102,951.700	NA	110,938.000	107,924.700	8.644	7.757	NA

B.5 Comparison with Best Exact Algorithm - Max W Clique

Table B.3.: Comparison with Optimal using Max W Clique

Instance	MaxWClique	ACO Best	ACO Median	%Diff ACO Best vs. MaxWClique	% Of Optimal Solution
*in*101	72,724.610	72,724.620	69,505.350	0.00001	**100**
*in*102	72,518.220	72,391.300	70,816.550	−0.175	99.825
*in*103	72,129.500	70,263.900	68,500.380	−2.586	97.414
*in*104	72,709.640	72,709.650	72,709.650	0.00001	**100**
*in*105	75,646.120	74,710.870	69,655.450	−1.236	98.764
*in*106	71,258.610	70,109.670	65,481.070	−1.612	98.388
*in*107	69,713.400	69,398.190	68,556.220	−0.452	99.548
*in*108	75,813.200	75,776.730	73,403.750	−0.048	99.952
*in*109	69,475.890	68,652.180	65,638.600	−1.186	98.814
*in*110	68,295.280	68,154.710	66,103.890	−0.206	99.794
*in*111	75,133.290	74,498.480	72,711.300	−0.845	99.155
*in*112	71,342.480	71,342.480	70,649.440	0.00000	**100**
*in*113	73,365.870	72,440.320	72,440.320	−1.262	98.738
*in*114	69,224.750	68,239.570	67,749.260	−1.423	98.577
*in*115	70,221.560	69,908.300	67,582.560	−0.446	99.554
*in*116	70,032.430	69,093.730	68,973.010	−1.340	98.660
*in*117	69,982.830	69,982.830	67,505.990	0.00000	**100**
*in*118	72,160.980	71,385.200	67,132.890	−1.075	98.925
*in*119	67,038.420	66,153.540	64,083.190	−1.320	98.680
*in*120	75,514.930	74,648.330	72,865.390	−1.148	98.852
*in*201	81,557.740	81,557.740	81,557.740	0.00000	**100**
*in*202	90,708.120	90,708.130	90,333.850	0.00001	**100**
*in*203	86,239.210	86,239.210	86,239.210	0.00000	**100**
*in*204	87,075.420	87,075.430	85,480.420	0.00001	**100**
*in*205	86,515.950	86,515.950	84,840.310	0.00000	**100**
*in*206	91,518.960	91,518.960	87,755.490	0.00000	**100**
*in*207	93,129.240	93,129.250	91,247.660	0.00001	**100**
*in*208	94,904.670	94,904.680	91,782.040	0.00001	**100**
*in*209	87,268.960	87,268.960	86,356.430	0.00001	**100**
*in*210	89,962.390	89,962.400	86,878.260	0.00001	**100**
*in*211	84,913.680	84,913.680	83,618.950	0.00000	**100**
*in*212	90,778.200	90,778.210	88,124.010	0.00001	**100**
*in*213	85,369.180	85,369.180	84,169.240	0.00001	**100**
*in*214	85,181.600	85,181.610	84,823.260	0.00001	**100**
*in*215	91,531.690	91,531.690	88,879.960	0.00000	**100**
*in*216	91,580.930	91,580.930	91,580.930	0.00000	**100**
*in*217	86,962.920	86,962.930	86,895.060	0.00001	**100**
*in*218	94,965.190	94,965.190	90,151.270	0	**100**
*in*219	93,586.430	90,309.730	89,760.600	−3.501	96.499
*in*220	89,792.900	89,792.910	88,255.520	0.00001	**100**

Table B.4.: Comparison with Optimal using Max W Clique

Instance	MaxWClique	ACO Best	ACO Median	%Diff ACO Best vs. MaxWClique	% Of Optimal Solution
*in*401	77,417.480	77,417.480	77,417.480	0.00000	**100**
*in*402	76,273.330	76,273.340	76,273.340	0.00001	**100**
*in*403	74,843.950	74,843.960	74,843.960	0.00001	**100**
*in*404	78,761.690	78,761.690	78,761.690	0	**100**
*in*405	75,915.900	75,915.900	75,336.860	0	**100**
*in*406	72,863.320	72,863.320	72,863.320	0.00001	**100**
*in*407	76,365.720	76,365.720	76,365.720	0	**100**
*in*408	77,018.830	77,018.830	77,018.830	0.00000	**100**
*in*409	73,188.620	73,188.620	73,188.620	0	**100**
*in*410	73,791.650	73,791.660	73,710.070	0.00001	**100**
*in*411	73,935.400	73,935.410	73,898.990	0.00001	**100**
*in*412	75,292.630	75,292.630	75,292.630	0	**100**
*in*413	74,434.900	74,434.990	74,434.990	0.0001	**100**
*in*414	77,146.370	77,146.370	76,749.550	0.00000	**100**
*in*415	73,519.130	73,519.130	73,519.130	0	**100**
*in*416	73,487.010	73,487.020	73,487.020	0.00001	**100**
*in*417	74,981.350	74,981.350	74,981.350	0.00000	**100**
*in*418	71,404.840	71,404.840	71,404.840	0.00000	**100**
*in*419	72,505.210	72,505.210	72,505.210	0.00000	**100**
*in*420	75,510.680	75,510.680	75,510.680	0.00001	**100**
*in*421	75,694.940	75,694.950	74,729.600	0.00001	**100**
*in*422	77,443.910	77,443.910	77,443.910	0	**100**
*in*423	68,134.350	68,134.350	68,134.350	0.00001	**100**
*in*424	77,352.760	77,352.760	76,385.110	0	**100**
*in*425	77,333.910	77,333.910	77,333.910	0	**100**
*in*426	76,430.180	76,430.180	76,430.180	0	**100**
*in*427	76,387.570	76,387.570	76,387.570	0	**100**
*in*428	77,384.940	77,384.940	76,609.980	0	**100**
*in*429	75,540.960	75,540.960	75,540.960	0	**100**
*in*430	79,038.750	79,038.750	79,038.750	0	**100**
*in*501	88,656.950	88,656.960	86,780.240	0.00001	**100**
*in*502	86,236.910	86,236.910	84,915.890	0.00000	**100**
*in*503	87,812.370	86,318.180	85,106.870	−1.702	98.298
*in*504	85,600	85,600.000	83,947.140	0.00000	**100**
*in*601	108,800.400	108,800.400	105,058.500	0.00000	**100**
*in*602	105,611.500	105,611.500	102,360.800	0.00001	**100**
*in*603	105,121.000	105,121.000	99,171.900	0.00000	**100**
*in*604	107,733.800	107,733.800	105,838.900	0.00000	**100**
*in*605	109,841.000	109,841.000	105,925.800	0.00000	**100**
*in*606	107,113.100	107,113.100	105,218.200	0.00001	**100**
*in*607	113,180.300	113,180.300	105,869.400	0.00000	**100**
*in*608	105,266.100	105,266.100	104,285.700	0.00001	**100**
*in*609	109,472.300	109,472.300	104,084.700	0.00000	**100**
*in*610	113,717.000	113,717.000	111,487.900	0.00000	**100**

Table B.5.: Comparison with Optimal using Max W Clique

Instance	MaxWClique	ACO Best	ACO Median	%Diff ACO Best vs. MaxWClique	% Of Optimal Solution
*in*611	106,666.300	106,666.300	101,902.400	0.00000	**100**
*in*612	109,796.700	109,796.700	106,056.100	0.00000	**100**
*in*613	107,980.100	107,980.200	105,559.100	0.00001	**100**
*in*614	108,364.600	108,364.600	106,152.600	0.00001	**100**
*in*615	110,508.800	110,508.800	108,615.900	0.00000	**100**
*in*616	109,740.500	109,740.500	105,441.800	0	**100**
*in*617	113,302.400	113,302.400	106,931.500	0.00000	**100**
*in*618	111,385.100	111,385.100	108,048.500	0.00000	**100**
*in*619	107,571.600	107,571.600	105,627.100	0.00000	**100**
*in*620	110,938.000	110,938.000	107,924.700	0.00000	**100**

Table B.6.: Summary: TrACA vs MaxWClique (Wu and Hao, 2016). Max time taken by TrACA ≈ 625 sec.

Test Instance	OSP 100	OSP 200	OSP 300	OSP 400
Lau and Goh (2002)				
in101-in120	0.02	0.03	0.041	0.033
in201-in220	0.053	0.095	0.13	0.17
in401-in430	0.5	0.61	0.69	0.73
in501-in504	0.008	0	0.025	0
in601-in620	0.033	0.083	0.143	0.18

B.6 Regression & Bootstrap Results

Table B.7.: IRLS Estimated Coefficients

	Dependent variable:
	Run times
Avg. In-Degree	−1,178.420***
	(254.233)
Avg. In-Degree Closeness	2,577.499
	(3,300.123)
Avg. Out-Degree Closeness	−2,595.040
	(3,376.119)
Avg. Betweenness	−20.704
	(182.043)
Clustering Coefficient (Transitivity)	−471.619***
	(101.655)
Eigenvalue	1,598.136***
	(397.583)
Avg. Eigenvector Centrality	838.843**
	(374.180)
Avg. Katz Centrality	6.140
	(7.080)
Avg. Cluster Size	−1.901
	(9.670)
Std. Dev. Cluster Size	2.859
	(8.530)
Avg. Node Strength	−99.030***
	(28.199)
Constant	355.341***
	(0.811)
Observations	90
Residual Std. Error	5.742 (df = 78)
Note:	*p<0.1; **p<0.05; ***p<0.01

Table B.8.: Original sample value for each component of the bootstrapped statistics (*Original*), Bootstrap estimates of bias (*bootBias*), standard error (*bootSE*) and median value of statistic (*bootMed*).

	R	Original	bootBias	bootSE	bootMed	2.5%	97.5%
(Intercept)	2,000	355.462	−0.534	2.285	354.708	351.517	360.473
AIn_i	2,000	−759.771	−101.692	623.776	−839.495	−1,880.657	564.500
$AInC_i$	2,000	12,206.130	−1,985.034	7,713.555	10,535.710	−927.121	29,309.460
$AOutC_i$	2,000	−12,399.840	2,057.958	7,939.376	−10,644.690	−30,018.690	1,103.094
$ABet_i$	2,000	428.228	−134.332	476.376	312.259	−371.120	1,496.240
CC_i	2,000	−608.652	71.821	231.755	−539.720	−1,134.705	−226.241
EV_i	2,000	664.107	267.714	1,107.816	931.728	−1,774.887	2,567.673
$AEVC_i$	2,000	1,853.234	−316.067	1,009.278	1,596.848	191.152	4,147.449
AKC_i	2,000	12.180	−1.472	16.555	10.276	−18.797	46.099
ACS_i	2,000	30.161	3.958	26.498	27.012	−25.731	78.138
SCS_i	2,000	13.731	−3.036	24.536	12.977	−31.323	64.855
ANS_i	2,000	−13.840	3.369	90.286	−23.567	−194.166	159.748

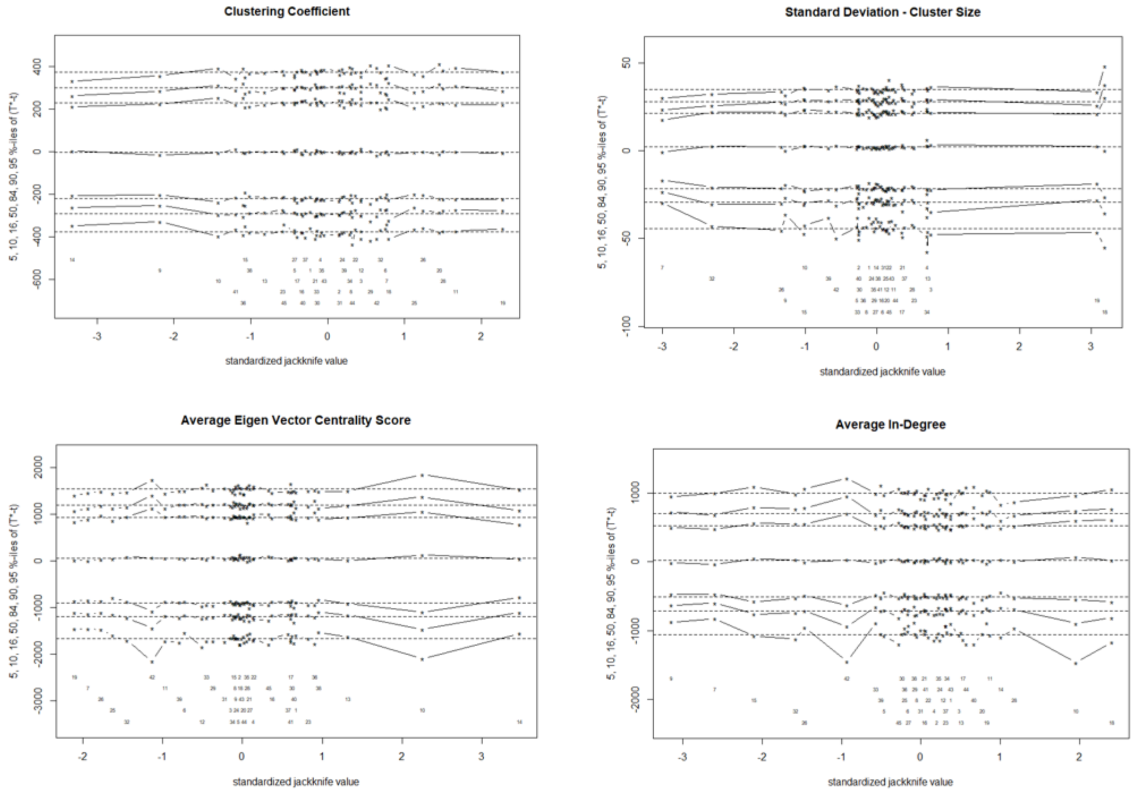

Figure B.1.: Sensitivity analysis of bootstrapped coefficients for $AIn_i, SCS_i, CC_i, AEVC_i$

B.7 Sample Box-Plots

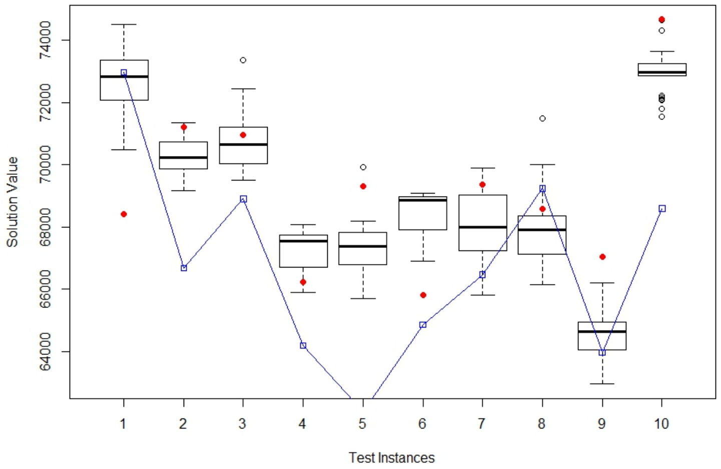

Figure B.2.: TrACA results for instances 111-120. Red dots are CPLEX values. Blue squares joined by lines are Memetic Algorithm values.

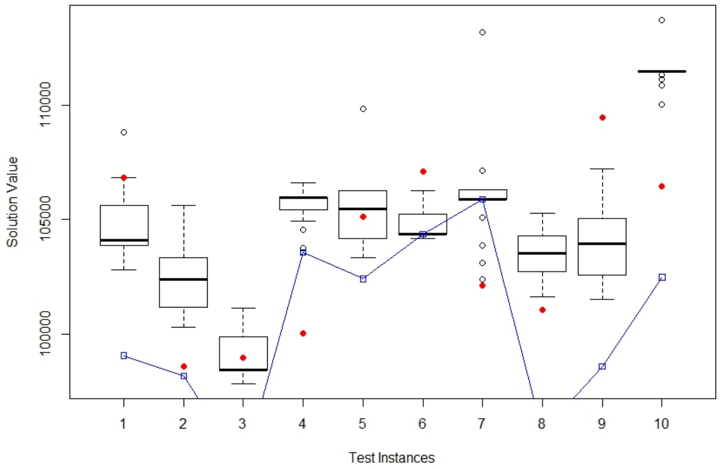

Figure B.3.: TrACA results for instances 601-610. Red dots are CPLEX values. Blue squares joined by lines are Memetic Algorithm values.

B.8 Run-time Predictions

Predicted Run-times using Supervised learning model. Run-times are dependent on problem complexity. Our findings regarding complexity of WDP are similar to evidence from closely related problem - multidimensional knapsack (MKP) (Puchinger et al., 2006, 2010; Xia et al., 2004). MKP involves choosing a subset of items to maximize profit, such that resource constraints are not violated. One of the constraints is defined as tightness. Tightness is defined as the inverse of total quantity of each item requested by each set. For instance, lower value of tightness for item j implies more sets have requested the j^{th} item. Lower value of tightness makes solving MKP harder (Puchinger et al., 2010). In terms of WDP, tightness is equivalent to inverse of number of bundles that request an item (Cansizoglu, 2011; Pfeiffer and Rothlauf, 2008). TrACA clearly demonstrates that using its graphical formulation for solving WDP, it is well suited to solve large auctions that have higher likelihood for low tightness for items.

Table B.9.: Predicted run-times vs. Actual run-times - Validation Set

Observations	TrACA Predicted Run-time	Actual Run-time	S.E. (Standard Error)
1	157.650	161.400	1.264
2	602.024	597.021	1.649
3	420.383	407.664	1.723
4	608.360	593.151	2.582
5	319.853	323.599	3.195
6	154.447	153.699	1.369
7	149.958	148.188	1.786
8	409.204	421.463	2.433
9	169.720	169.964	2.574
10	350.948	357.696	1.984
11	407.331	403.494	2.826
12	570.320	557.922	1.875
13	380.794	384.180	2.003
14	134.977	135.436	3.285
15	382.159	383.195	2.343
16	581.560	589.612	1.705
17	152.093	155.853	2.048
18	150.444	152.520	1.425
19	394.143	398.866	2.920
20	401.712	408.108	3.361
21	159.113	160.895	2.156
22	155.660	157.628	1.514
23	587.256	613.290	2.669
24	415.602	417.553	1.719
25	600.414	619.785	1.927

Table B.10.: Predicted run-times vs. Actual run-times - Test Set

Observations	TrACA Predicted runtimes	Actual runtimes	S.E. (Standard Error)
1	444.908	446.255	3.639
2	406.306	409.015	1.815
3	395.892	389.741	2.911
4	160.151	160.354	2.064
5	610.949	611.307	1.856
6	354.300	348.166	2.174
7	397.482	389.191	2.057
8	150.983	149.777	1.522
9	428.136	420.688	1.819
10	161.534	155.064	2.619
11	567.663	543.512	1.862
12	576.123	569.499	1.967
13	437.300	436.220	3.009
14	616.808	666.477	2.193
15	143.267	145.932	1.746
16	387.443	391.939	2.133
17	342.538	346.308	2.317
18	354.844	335.790	2.499
19	380.367	382.820	2.445
20	572.779	563.744	1.769

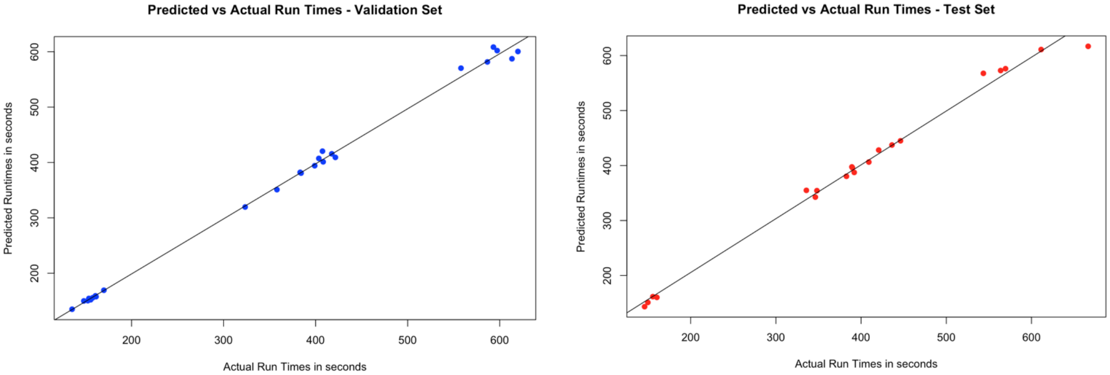

Figure B.4.: Predicted Values from Bootstrapped IRLS Model for Validation & Test Set

B.9 CPLEX vs TrACA

Table B.11.: Summary: TrACA vs CPLEX. For Median Test we use Wilcoxon Rank Sum test.

Test Instance Lau and Goh (2002)	Median Test	ISP	Z Score	Solution Quality
in101-in120	4	0.32	0.44	2.5%
in201-in220	8	0.53	-0.45	2.55%
in401-in430	10	0.81	0.44	0%
in601-in620	13	0.75	-1.98	5.2%

We outline here the comparison of CPLEX & TrACA. Usually, many prior literature do not compare CPLEX with their meta-heuristic algorithms. CPLEX aims to generate the optimal solution even though it may take a considerable amount of time. Recall that, to keep the comparison consistent, we allow the CPLEX solver run for the same duration as the maximum time TrACA takes to solve for each set of instances (Table 3.1, Column 6). Table B.11 shows the results for comparison between CPLEX and TrACA. When choosing between CPLEX and TrACA, the choice is between a deterministic algorithm and a heuristic. Hence the choice depends on how TrACA's solution distribution generated in repeated trials, within specified time, compares with CPLEX results. Although the results from Median Test and ISP (Table B.11 Columns 2, 3) point to better solution from CPLEX, values in Z score and Solution Quality (Column 4, 5), point to value from using TrACA for repeated solving of WDP. Further, we consider TrACA's speed of convergence to optimal as another parameter for comparison with CPLEX. As shown in Figure B.5, for instances in101 and in104, TrACA converges to a better solution in the 800th and 650th iteration respectively. For the most difficult instances in601-in620 in terms of size (1500 bids of 1500 items), TrACA converges to better solution during the first 600 iterations for 10 out of 20 instances and before 1200 iterations for the rest 8 instances. In terms of time, this translates to better results in as low as 4.5 minutes. Hence, the value from using TrACA is in applications that need fast and repeated approximation within a specified duration. For industrial applications, Bichler and Kalagnanam (2006) notes that the private procurement auctions exhibit trends of repeated winner determination. In these auctions, the range of items can be 10 to nearly 100,000 with number of bidders ranging from only a few up to several hundreds. With such variability in number of items and bids, iterative combinatorial auctions are being used to improve efficiency of allocation (Cramton et al., 2007).

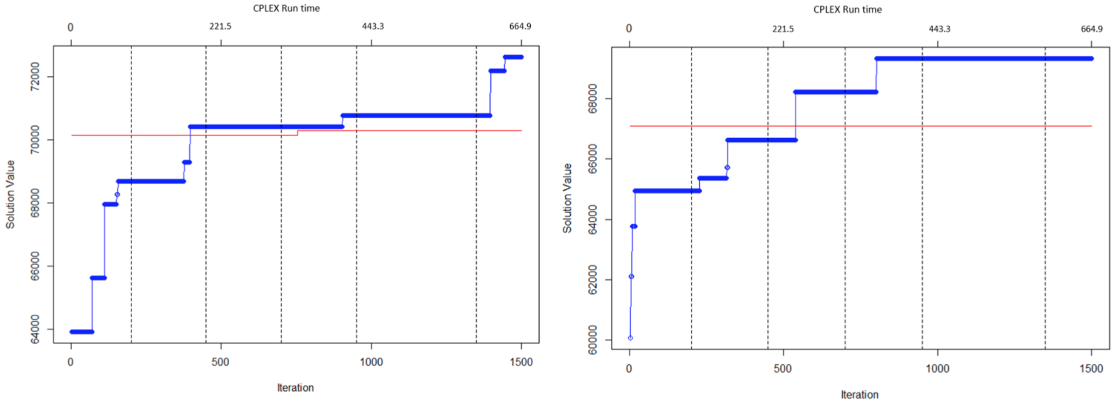

Figure B.5.: Typical convergence pattern for 400 ant simulation run for 1500 iterations and Randomized graph pruning happening at $t_c = \{200, 450, 700, 950, 1350\}$. The graph shows CPLEX solution constructions in the 601 sec it takes TrACA to construct solution for in101, in104 instances.

B.10 Multi-Unit Multi-Item Simulations

Table B.12.: Results for Multi-Unit, Multi-Item Auction Simulations

Test Instance	Maximum Revenue	Time Taken (sec.)	No. of Winning Bids
1	12,666.190	6.240	10
2	13,337.560	5.470	7
3	15,050.360	6.870	8
4	11,686.960	6.980	7
5	12,903.910	5.980	8
6	13,973.420	5.670	9
7	10,927.230	6.390	10
8	13,824.450	5.500	9
9	13,147.860	5.080	10
10	12,810.790	6.290	10
11	11,972.500	6.200	8
12	12,256.950	6.180	9
13	13,996.160	5.360	9
14	13,016.230	6.940	8
15	9,785.222	6.440	10
16	13,339.720	6.570	9
17	14,605.560	6.490	8
18	12,613.410	5.080	10
19	15,071.530	5.390	8
20	12,233.180	5.530	9

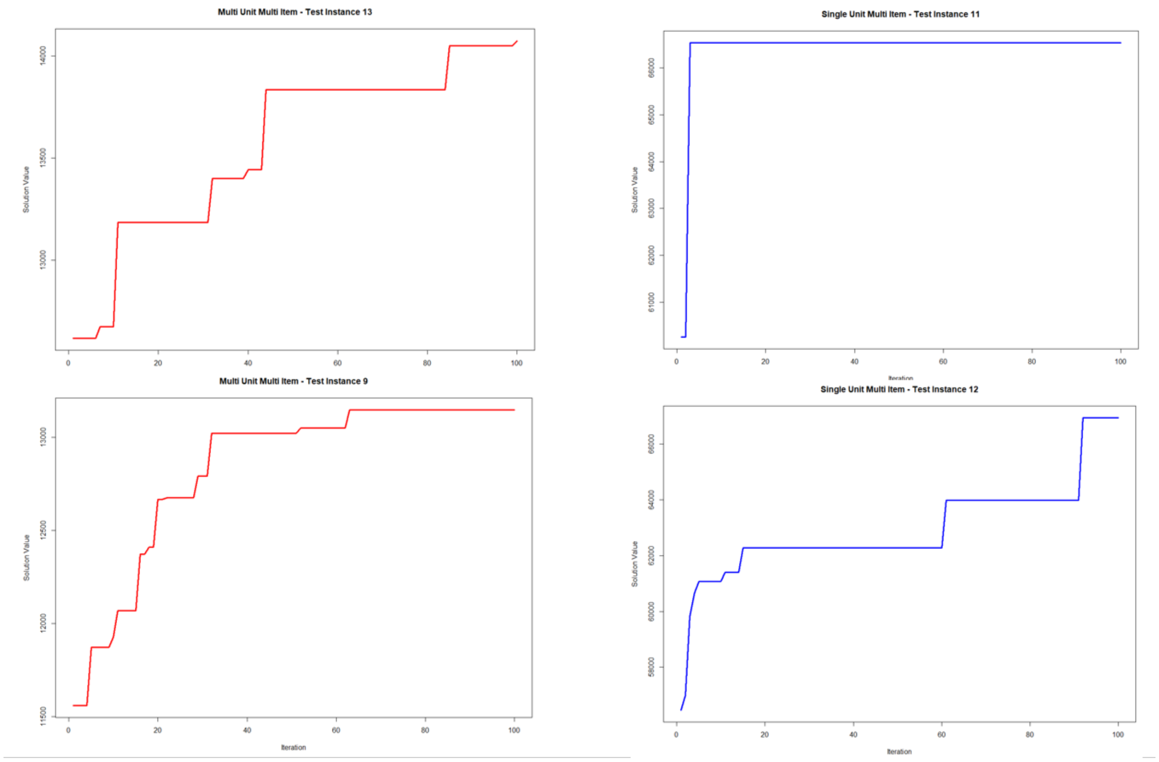

Figure B.6.: Comparison of search: Single Unit Multi Item vs Multi Unit Multi Item. Convergence trend shown for first 100 iterations.

C. APPENDIX C

C.1 Proof Proposition 1

The proof uses the basic definition of dominant strategies that states a strategy $s_i \in S_i$ is a dominant strategy for player i if $\forall\ \hat{s}_i \neq s_i$ and all $s_{-i} \in S_{-i}$, $u_i(s_i, s_{-i}) \geq u_i(\hat{s}_i, s_{-i})$, and for at least one choice of s_{-i} the inequality is strict. Consider the same action space for miners $A = \{S_p, S_w, S_l\}$. Combining $V^{\text{win}}, V^{\text{loss}}$, suppose that the expected payoff for miner 1, from any action is given by $E^{n_1,n_2}_{S_1,S_2} = \gamma_0 - \gamma_1\delta_{12} - \gamma_2\delta_{21} - \gamma_3\Delta L_1 - \gamma_4\Delta L_2$, with $\gamma_1 > \gamma_3$. For $n_2 \leq n_1 \leq 2n_2$, miner 1's payoffs for all actions of miner 2 are as follows:

$$E^{n_1,n_2}_{S_p,S_p} = \gamma_0 - \gamma_1 n_2 - \gamma_2 n_1 - \gamma_3 n_1 - \gamma_4 n_2 \tag{C.1}$$

$$E^{n_1,n_2}_{S_p,S_w} = \gamma_0 - \gamma_1 n_2 - \gamma_2(n_1 - n_2 - 1) - \gamma_3 n_1 \tag{C.2}$$

$$E^{n_1,n_2}_{S_p,S_l} = \gamma_0 - \gamma_1 n_2 - \gamma_2(n_1 - n_2) - \gamma_3 n_1 - \gamma_4 \tag{C.3}$$

$$E^{n_1,n_2}_{S_w,S_p} = \gamma_0 - \gamma_1(n_1 + 1 - n_2) - \gamma_2 n_1 - \gamma_4 n_2 \tag{C.4}$$

$$E^{n_1,n_2}_{S_w,S_w} = \gamma_0 - \gamma_1(n_1 + 1 - n_2) - \gamma_2(n_1 - n_2 - 1) \tag{C.5}$$

$$E^{n_1,n_2}_{S_w,S_l} = \gamma_0 - \gamma_1(n_1 + 1 - n_2) - \gamma_2(n_1 - n_2) - \gamma_4 \tag{C.6}$$

$$E^{n_1,n_2}_{S_l,S_p} = \gamma_0 - \gamma_1(n_1 - n_2) - \gamma_2 n_1 - \gamma_3 - \gamma_4 n_2 \tag{C.7}$$

$$E^{n_1,n_2}_{S_l,S_w} = \gamma_0 - \gamma_1(n_1 - n_2) - \gamma_2(n_1 - n_2 - 1) - \gamma_3 \tag{C.8}$$

$$E^{n_1,n_2}_{S_l,S_l} = \gamma_0 - \gamma_1(n_1 - n_2) - \gamma_2(n_1 - n_2) - \gamma_3 - \gamma_4 \tag{C.9}$$

Comparing payoffs for miner 1 actions S_l and S_w (i.e., equations C.4, C.5, C.6, C.7, C.8, C.9), for all actions of miner 2, S_l dominates S_w for miner 1. This is because, $E^{n_1,n_2}_{S_l,S_{-i}} - E^{n_1,n_2}_{S_w,S_{-i}} > 0\ \forall\ S_{-i} \in \{S_p, S_w, S_l\}$ since $\gamma_1 > \gamma_3$. Further, comparing miner 1 payoffs for actions S_l and S_p, $E^{n_1,n_2}_{S_l,S_{-i}} - E^{n_1,n_2}_{S_p,S_{-i}} = 2\gamma_1(n_2 - n_1) + \gamma_3(n_1 - 1) \geq 0\ \forall\ S_{-i} \in \{S_p, S_w, S_l\}$ since $n_2 < n_1 \leq 2n_2$. Hence, S_l is a dominant strategy for miner 1. By symmetry, similar analysis can be done for $n_1 < n_2 \leq 2n_1$.

Now, consider the case where $n_1 = n_2$. Then it is clear that same arguments hold for miner 1 and by symmetry for miner 2. Using the equations C.1 - C.9, clearly S_l strictly dominates S_w and dominates S_p. Hence, using elimination of dominated strategies, (S_l, S_l) is the dominant strategy equilibrium.

C.2 Proof Corollary 1

This is straightforward from equations C.1-C.9 and w.l.o.g consider miner 1 having the shorter private chain length. Then, since $\gamma_1 + \gamma_3 > 0$ and $\gamma_1(n_1 + 1) + \gamma_3 n_1 > 0$, S_w dominates S_l and S_p.

Consider the case where miner 1 successfully mines on a private chain and shortens the difference in chain lengths with the longer miner 2. Subsequently, when miner 1 gains in chain length to miner 2, following the previous proposition, S_l becomes the dominant strategy for miner 1.

C.3 Proof Proposition 2

The basic strategy of the proof is to show that a miner i's preference ordering is unanimous in ranking payoff from action S_l as weakly the best. Therefore, given weakly dominant strategies, no miner is better off with any other action.

Using definition of $\Delta n_i^{win}, \Delta n_i^{loss}$ following are the payoffs miner i with private chain $n_i > 0$ faces when competing with any other miner $j \neq i$ to mine a block:

$$u_i^{S_p,S_p} = h_1(n_i + 1) + h_2(0) + h_3(n_j + 1) + h_4(n_i) \tag{C.10}$$
$$u_i^{S_p,S_w} = h_1(n_i + 1) + h_2(0) + h_3(0) + h_4(n_i) \tag{C.11}$$
$$u_i^{S_p,S_l} = h_1(n_i + 1) + h_2(0) + h_3(1) + h_4(n_i) \tag{C.12}$$

$$u_i^{S_w,S_p} = h_1(0) + h_2(n_i + 1) + h_3(n_j + 1) + h_4(n_i) \tag{C.13}$$
$$u_i^{S_w,S_w} = h_1(0) + h_2(n_i + 1) + h_3(0) + h_4(n_i) \tag{C.14}$$
$$u_i^{S_w,S_l} = h_1(0) + h_2(n_i + 1) + h_3(1) + h_4(n_i) \tag{C.15}$$

$$u_i^{S_l,S_p} = h_1(1) + h_2(n_i) + h_3(n_j + 1) + h_4(n_i) \tag{C.16}$$
$$u_i^{S_l,S_w} = h_1(1) + h_2(n_i) + h_3(0) + h_4(n_i) \tag{C.17}$$
$$u_i^{S_l,S_l} = h_1(1) + h_2(n_i) + h_3(1) + h_4(n_i) \tag{C.18}$$

Since h_1, h_2 are assumed concave utility functions on finite sets $K_1 = \{0, n_i + 1, 1\}$ and $K_2 = \{0, n_i + 1, n_i\}$ respectively, by the theorem of concave utility functions on finite sets (Chambers and Echenique, 2009; Kannai, 2005; Richter and Wong, 2004), it is clear that:

- For K_1, since $\exists\ \alpha_1 > 0, \alpha_2 > 0$ such that $\alpha_1 + \alpha_2 = 1$ and $\alpha_1\,(n_i + 1) + \alpha_2(0) = 1$, outcomes $1 \succeq 0$ and $1 \succeq n_i + 1$. Hence, $h_1(1) \geq h_1(0)$ and $h_1(1) \geq h_1(n_i + 1)$.
- For K_2, since $\exists\ \beta_1 > 0, \beta_2 > 0$ such that $\beta_1 + \beta_2 = 1$ and $\beta_1\,(n_i + 1) + \beta_2(0) = n_i$, outcomes $n_i \succeq 0$ and $n_i \succeq n_i + 1$. Hence, $h_2(n_i) \geq h_2(0)$ and $h_2(n_i) \geq h_2(n_i + 1)$.

Using these inequalities, comparing dominance solvability when $A_{-i} = S_l$, we have:

$$h_1(1) \geq h_1(0),\ h_2(n_i) \geq h_2(n_i+1) \tag{C.19}$$

$$\Rightarrow h_1(1) + h_2(n_i) \geq h_1(0) + h_2(n_i+1) \tag{C.20}$$

$$h_1(1) \geq h_1(n_i+1),\ h_2(n_i) \geq h_2(0) \tag{C.21}$$

$$\Rightarrow h_1(1) + h_2(n_i) \geq h_1(n_i+1) + h_2(0) \tag{C.22}$$

which trivially implies $u_i^{S_l,S_l} \geq u_i^{S_w,S_l}$ and $u_i^{S_l,S_l} \geq u_i^{S_p,S_l}$. Using equations C.20, C.22, similar comparisons with $A_{-i} = S_w$ and $A_{-i} = S_p$ yield $u_i^{S_l,S_w} \geq u_i^{S_w,S_w}$ and $u_i^{S_l,S_w} \geq u_i^{S_p,S_w}$; $u_i^{S_l,S_p} \geq u_i^{S_w,S_p}$ and $u_i^{S_l,S_p} \geq u_i^{S_p,S_p}$. Hence, S_l is weakly dominant strategy.

Now misreporting private chain length by any other positive length does not change the outcome since any misreporting of length simply changes $\alpha_1, \alpha_2, \beta_1, \beta_2$. Further, if the miner misreports chain length as 0, then $K_1 = \{0, 1, 1\}$ and $K_2 = \{0, 1, 0\}$. Notice that on substituting these values in all payoff equations, miner is indifferent between S_p & S_l while on comparing S_l & S_w, since public chain dominant assumption applies, we have that $S_l \geq S_w$ and the outcome still is honest mining. Hence, the mechanism is strategy-proof.

C.4 Proof Proposition 3

The basic strategy of the proof is similar to previous proposition. Essentially, this is a proof by case where four cases are analyzed – each case, a miner i is compared with another miner j as a possible winner and it is shown that under no circumstances can action S_l be worse than action S_p, S_w.

- If $\min(X') = 0$, among $(0, n_i{+}1), (n_i{+}1, 0), (n_i, 1)$ it is clear that by majorization $(0, n_i + 1) \succ (n_i, 1)$. So, by Schur-Concavity for majorization $g^{win}(n_i, 1) \geq g^{win}(0, n_i + 1)$, $g^{win}(n_i, 1) \geq g^{win}(n_i + 1, 0)$.
- If $\min(X') = k \geq 1$ such that $n_i - k \geq 1$, among $(-k, n_i + 1), (n_i + 1 - k, 0), (n_i - k, 1)$ it is clear that if $n_i - k > 1$ then since $n_i + 1 > n_i + 1 - k > n_i - k$, $(-k, n_i + 1) \succ (n_i - k, 1)$, $(n_i + 1 - k, 0) \succ (n_i - k, 1)$. Hence, again by Schur-Concavity, $g^{win}(n_i - k, 1) \geq g^{win}(-k, n_i + 1)$, $g^{win}(n_i, 1) \geq g^{win}(n_i + 1 - k, 0)$. It is even simpler when $n_i - k = 1$ because then, the vectors become $(-k, n_i + 1), (2, 0), (1, 1)$. Since $(-k, n_i + 1) \succ (1, 1)$ and $(2, 0) \succ (1, 1)$ we have $g^{win}(n_i - k, 1) \geq g^{win}(-k, n_i + 1)$, $g^{win}(n_i - k, 1) \geq g^{win}(n_i + 1 - k, 0)$.
- Now, if $\min(X') = n_i{+}1 \ \forall\, n_i \in \{0, 1, 2, ..\}$, among $(-n_i{-}1, n_i{+}1), (0, 0), (-1, 1)$, it is clear that $(-n_i - 1, n_i + 1) \succ (-1, 1)$ and $(0, 0)$ is dominated. Hence, $g^{win}(-1, 1) \geq g^{win}(-n_i - 1, n_i + 1)$, $g^{win}(-1, 1) \geq g^{win}(0, 0)$.
- Finally, if $\min(X') > n_i{+}1 \ \forall\, n_i \in \{1, 2, ..\}$, then by definition $\Delta n_i^{\text{win}} = n_i^{A_i} \ \forall\, S_i \in \{S_p, S_w, S_l\}$. Hence, among $(0, n_i{+}1), (n_i{+}1, 0), (n_i, 1)$ it is clear that $(0, n_i{+}1) \succ$

$(n_i, 1)$ and $(n_i+1, 0) \succ (n_i, 1)$. So, $g^{win}(n_i, 1) \geq g^{win}(0, n_i+1)$, $g^{win}(n_i, 1) \geq g^{win}(n_i+1, 0)$.

Consider a miner misreporting private chain length: $n_i = \{0, 1, n_i - k\}$. For the first case, if $\min(X') = 0$ then S_l payoffs are equal to S_p and S_w and miner is indifferent. If $\min(X') = 1$, S_l and S_p have equal payoffs with S_w having zero payoffs – again miner indifferent. Finally $\min(X') > 1$ then S_l payoffs are equal to S_p and S_w and miner is indifferent. Now consider reporting $n_i = 1$ – if $\min(X') = 0$ then S_l again dominate S_p and S_w – because vectors $(2,0), (0,2)$ majorize $(1,1)$. If $\min(X') = 1$ then S_l dominates S_p and is equal to S_w – because vectors $(-1,2), (1,0)$ weakly majorize $(0,1)$. Finally, when $\min(X') > 1$, then if $\min(X') = 2$, S_l dominates S_p ($(-2,2) \succ (-1,1)$) and payoff from $S_w = 0$ ($g^{win}(0,0) = 0$). Otherwise, for any other value of $\min(X') > 1$, then S_l payoffs are equal to S_p and S_w and miner is indifferent and same argument from before follows. Now consider reporting $n_i - k$. As shown, if $\min(X') = n_j < n_i - k$, then by same arguments as before $(-n_j, n_i - k + 1) \succ (n_i - k - n_j, 1)$ and $(n_i - k + 1 - n_j, 0) \succ (n_i - k - n_j, 1)$. Since misrepresenting private chain lengths does not impact payoffs, using Revelation Principle for Dominant Strategies then a direct mechanism is DSIC (dominant strategy incentive compatible).

Note that we do not consider cases where the miner misreports private chain length as $n_i^{'} > n_i$ since, by definition the outcomes of the mechanism would have to be $\{0, 1, n_i^{'} + 1\}$ where, clearly, $n_i^{'} + 1 \neq n_i + 1$, the actual increment by which the public chain is forked. Hence, this case is deemed infeasible by the mechanism and therefore ignored.

C.5 Proof Proposition 4

Consider the vectors $(-\min(X'), n_i + 1), (n_i + 1 - \min(X'), 0), (n_i - \min(X'), 1)$. For $n_i \geq 1$, it is clear that:

- If $\min(X') = 0$, among $(0, n_i+1), (n_i+1, 0), (n_i, 1)$ it is clear that by majorization $(0, n_i+1) \succ (n_i, 1)$. So, by Karamata Inequality for majorization $h_1(n_i+1) + h_2(0) \leq h_1(1) + h_2(n_i)$.
- If $\min(X') = k \geq 1$ such that $n_i - k \geq 1$, among $(-k, n_i+1), (n_i+1-k, 0), (n_i - k, 1)$ it is clear that if $n_i - k > 1$ then since $n_i + 1 > n_i + 1 - k > n_i - k$ and $n_i + 1 + k > n_i + 1 - k$, $(k, n_i+1) \succ (n_i - k, 1)$, $(n_i + 1 - k, 0) \succ (n_i - k, 1)$. Hence, again by Karamata Inequality, $h_1(n_i+1) + h_2(-k) \leq h_1(1) + h_2(n_i - k)$ and $h_1(n_i + 1 - k) + h_2(0) \leq h_1(1) + h_2(n_i - k)$. It is even simpler when $n_i - k = 1$ because then, the vectors become $(-k, n_i+1), (2,0), (1,1)$. Since $(-k, n_i+1) \succ (1,1)$ and $(2,0) \succ (1,1)$ we have $h_1(n_i+1) + h_2(-k) \leq h_1(1) + h_2(1)$ and $h_1(0) + h_2(2) \leq h_1(1) + h_2(1)$.
- Now, if $\min(X') = n_i + 1 \; \forall \, n_i \in \{0, 1, 2, ..\}$, among $(-n_i - 1, n_i + 1), (0,0), (-1,1)$, it is clear that $(-n_i - 1, n_i + 1) \succ (-1, 1)$ and $(0,0)$ is dominated. Hence, $h_1(1) + h_2(-1) \geq h_2(-n_i - 1) + h_1(n_i + 1)$, $h_1(1) + h_2(-1) \geq h_1(0) + h_2(0)$.

- Finally, if $\min(X') > n_i+1 \; \forall \, n_i \in \{1,2,..\}$, then by definition $\Delta n_i^{\text{win}} = n_i^{A_i} \; \forall \, S_i \in \{S_p, S_w, S_l\}$. Hence, among $(0, n_i+1), (n_i+1, 0), (n_i, 1)$ it is clear that $(0, n_i + 1) \succ (n_i, 1)$ and $(n_i+1, 0) \succ (n_i, 1)$. So, $h_1(1) + h_2(n_i) \geq h_1(n_i+1) + h_2(0)$, $h_1(1) + h_2(n_i) \geq h_1(0) + h_2(n_i+1)$.

Consider a miner misreporting private chain length: $n_i = \{0, 1, n_i - k\}$. For the first case, if $\min(X') = 0$ then S_l payoffs are equal to S_p and S_w and miner is indifferent. If $\min(X') = 1$, S_l and S_p have equal payoffs with S_w having zero payoffs – again miner indifferent. Finally $\min(X') > 1$ then S_l payoffs are equal to S_p and S_w and miner is indifferent. Now consider reporting $n_i = 1$. If $\min(X') = 0$ then S_l again dominate S_p and S_w – because vectors $(2,0), (0,2)$ majorize $(1,1)$. If $\min(X') = 1$ then S_l dominates S_p and is equal to S_w – because vectors $(-1,2), (1,0)$ weakly majorize $(0,1)$. Finally, when $\min(X') > 1$, then if $\min(X') = 2$, S_l dominates S_p ($(-2,2) \succ (-1,1)$) and payoff from $S_w = 0$ ($g^{win}(0,0) = 0$). Otherwise, for any other value of $\min(X') > 1$, when miner i reports $n_i = 1$, then S_l payoffs are equal to S_p and S_w and miner is indifferent. Now consider reporting $n_i - k$. As shown, if $\min(X') = n_j < n_i - k$, then by same arguments as before $(-n_j, n_i - k + 1) \succ (n_i - k - n_j, 1)$ and $(n_i - k + 1 - n_j, 0) \succ (n_i - k - n_j, 1)$. Since misrepresenting private chain lengths does not impact payoffs, using Revelation Principle for Dominant Strategies then a direct mechanism is DSIC (dominant strategy incentive compatible).

C.6 Proof Proposition 5

Consider any non-negative value of blocks added by honest miners $l_h \geq 0$. As shown in Eyal and Sirer (2018); Sapirshtein et al. (2016), only when $\delta_i \geq 1 \Rightarrow n_i \geq l_h + 1$ do selfish miners consider either forking or withholding. Hence we only consider those cases in the following proof.

By majorization, among vectors $(-l_h, n_i+1), (n_i+1-l_h, 0), (n_i - l_h, 1)$, it is clear that $(-l_h, n_i+1) \succ (n_i - l_h, 1)$ and $(n_i + 1 - l_h, 0) \succ (n_i - l_h, 1)$. By Schur-concavity then, $g^{\text{win}}(n_i - l_h, 1) \geq g^{\text{win}}(-l_h, n_i + 1)$ and $g^{\text{win}}(n_i - l_h, 1) \geq g^{\text{win}}(n_i + 1 - l_h, 0)$. Hence, S_l is the dominant strategy.

Now consider miner i misreporting private chain length. Clearly, on reporting $n_i = \{1, 2, 3, .., n_i - k\}$ majorization and Schur-concavity produce the same result. Further, on reporting $n_i = 0$, if honest mining increments $l_h > 0$ then by Eyal and Sirer (2018), miner mines honestly. In the rare case where honest mining increment $l_h = 0$ (which can happen if selfish miner wins consecutive rounds), even then reporting $n_i = 0$ makes miner indifferent between actions (since $n_i < l_h + 1$ when $n_i = l_h = 0$). Hence, the mechanism is strategy-proof.