Shapley Value-based Approach for Redistributing Revenue of Matchmaking of Private Transactions in Blockchains

Rasheed
Machine Learning Lab
IIIT Hyderabad
Hyderabad, India
mohammad.ahmed@research.iiit.ac.in

Parth Desai
Machine Learning Lab
IIIT Hyderabad
Hyderabad, India
parth.desai@research.iiit.ac.in

Yash Chaurasia
Machine Learning Lab
IIIT Hyderabad
Hyderabad, India
cayshvk@protonmail.com

Sujt Gujar
Machine Learning Lab
IIIT Hyderabad
Hyderabad, India
sujit.gujar@iiit.ac.in

February 22, 2025

ABSTRACT

In the context of blockchain, MEV refers to the maximum value that can be extracted from block production through the inclusion, exclusion, or reordering of transactions. Searchers often participate in order flow auctions (OFAs) to obtain exclusive rights to private transactions, available through entities called *matchmakers*, also known as order flow providers (OFPs). Most often, redistributing the revenue generated through such auctions among transaction creators is desirable. In this work, we formally introduce the *matchmaking* problem in MEV, its desirable properties, and associated challenges. Using cooperative game theory, we formalize the notion of fair revenue redistribution in matchmaking and present its potential possibilities and impossibilities. Precisely, we define a characteristic form game, referred to as `RST-Game`, for the transaction creators. We propose to redistribute the revenue using the Shapley value of `RST-Game`. We show that the corresponding problem could be SUBEXP (i.e. $2^{o(n)}$, where n is the number of transactions); therefore, approximating the Shapley value is necessary. Further, we propose a randomized algorithm for computing the Shapley value in `RST-Game` and empirically verify its efficacy.

1 Introduction

As defined in [1], *blockchain* is a distributed ledger of digital transactions maintained by a network of computers (or nodes) that reach consensus using one of a variety of mechanisms, such as *Proof-of-Work* (PoW) [2] or *Proof-of-Stake* (PoS) [3]. *Maximal Extractable Value* (MEV) in the blockchain context refers to "the maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding, and changing the order of transactions in a block" [4]. MEV extraction is an integral part of the Ethereum blockchain – it enhances revenue, supports sustainable post-block rewards, and contributes to the overall health of DeFi activities [5], [6], [7]. However, MEV extraction possesses certain negative externalities such as worse execution price to transaction creators due to MEV attacks such as front-running and sandwiching [8], consensus-security risks, centralization due to shift in economic structure among blockchain participants, and legal and ethical concerns [9], [10], [11].

As MEV extraction becomes increasingly vital for sustaining the Ethereum blockchain's economic ecosystem, developments in the Ethereum's landscape [12], such as its transition to Proof-of-Stake, have reformed how transactions are

processed. This shift introduced the concept of *proposer-builder separation* (PBS), where *builders* are responsible for gathering transactions from the network, assembling them into blocks, and then bidding these blocks to the proposer, who holds the authority to publish them on the blockchain [13]. Builders compete in an auction, known as the *PBS auction*, for the opportunity to get their block included in the current slot [14], [15]. Proposers are heavily invested in the staking process and prioritize earning through staking rewards rather than generating profits through block building and MEV extraction. *Searchers* are individual or institutional entities that actively seek to capitalize on profitable opportunities arising from various factors such as market inefficiencies during periods of high volatility [16], the price of execution driven by supply-demand dynamics, and delays in transaction processing [17]. They use techniques like front-running, back-running, sandwiching, etc [18], [19] to extract MEV. Occasionally, some participants take on dual roles as both builders and searchers to maximize their profits [13].

The current paper focuses on searchers and *transaction creators*. Typically, searchers find MEV extraction opportunities by analyzing unconfirmed transactions in the public mempool. Searchers strategically create a bundle of transactions to earn profit and bid (proportional to their potential profit) for block space with block builders. Unconfirmed transactions in a public mempool are accessible to all the blockchain participants, resulting in high competition among searchers [20]. Hence, searchers look to include private transactions to increase their chances of winning [13]. Private transactions, also called private order flows, are transactions that are not available in the public mempool.

Such MEV-rich private transactions are made available for sale by *order flow providers* (OFPs), which typically include wallet service providers. OFPs collect intents from transaction creators, process them into transactions, and auction them off to searchers in what is known as *order flow auctions* (OFAs) [21]. While this transaction pipeline is profitable for searchers, there are two crucial points: (i) it might result in worse execution prices for transaction creators [8], and (ii) some OFPs charge transaction creators for providing their wallet services and may aim to enhance the experience for transaction creators by sharing the revenue generated from the OFAs with them. This has led to the mechanism of *Matchmaking*.

Matchmaking is a mechanism to redistribute the revenue generated by the order flow auctions to the transaction creators in exchange for the value that can be extracted from their transactions [15]. A *matchmaker* in blockchain is an OFP with access to transaction creators' private transactions. If the transactions are directly sent to the builders enforcing no MEV extraction, the potential MEV that could have been generated in the system from the transactions is lost. So, the matchmaker instead auctions off the transactions to searchers for efficient extraction of MEV. In return, the matchmaker compensates the transaction creators for the value their transactions create [22], [23]. Figure 1 shows that as of 2024, private transactions made up more than 30% of all smart contract transactions on Ethereum (which was nearly 3 out of every 10 transactions). Though multiple authors have raised a need for such redistribution, as claimed in [24], [25], designing a matchmaking mechanism is an open problem. This paper addresses how a matchmaker should redistribute the revenue generated through an OFA among transaction creators in a *fair* manner. Some transactions add more value to the system or receive worse execution prices than others; thus, sharing the revenue equally is unfair. It should be shared proportional to how much value they add to the system. Hence, the Shapley values of an appropriately defined game become a natural way of redistributing revenue back to transaction creators.

In this paper, we define a cooperative game `RST-Game` over transaction creators based on the revenue generated in the system. We study `RST-Game` for two important types of valuations of the searchers-: (i) *additive* and (ii) *single-minded*. Additive value settings mean the total value a searcher derives from the transactions shared with it, is the addition of value for individual transactions.

Searchers may be interested in a bundle(s) of transactions, which is the more practical situation in the MEV world. We abstract it through a case of single-minded searchers. Here, each searcher is interested in a particular bundle of transactions. A single-minded searcher prefers not to be allocated any transactions than to be allocated a strict subset of his interested bundle of transactions. It does not mind being allocated a superset of its interested bundle. In general, computing the Shapley value of a game is EXP [26]. However, the researchers have shown that for certain games, it could be computed efficiently, e.g., [27], [28]. We provide efficient computation even for `RST-Game` for additive value settings. But, for single-minded cases, it is difficult to compute Shapley value efficiently. We provide examples where computing the Shapley value of `RST-Game` is possibly subexponential in terms of the number of transactions and exponential in terms of the number of searchers. Hence, we conjecture that the Shapley value of `RST-Game` with single-minded searchers is SUBEXP [1]. Since an analytical solution to the `RST-Game` is infeasible to compute for a large number of transactions or searchers, we resort to approximating the Shapley values. We design a polynomial time algorithm called Randomized ShapleY Procedure (`RSYP`) to compute the Shapley value of all transaction creators. `RSYP` computes the marginal contribution of a transaction for randomly selected $\mathcal{O}(n^2)$ subsets of transactions than all possible subsets and approximate Shapley value as an appropriately weighted combination of these

---

[1] Of the two commonly used definitions of SUBEXP, we use the following: SUBEXP(n) = $2^{o(n)}$
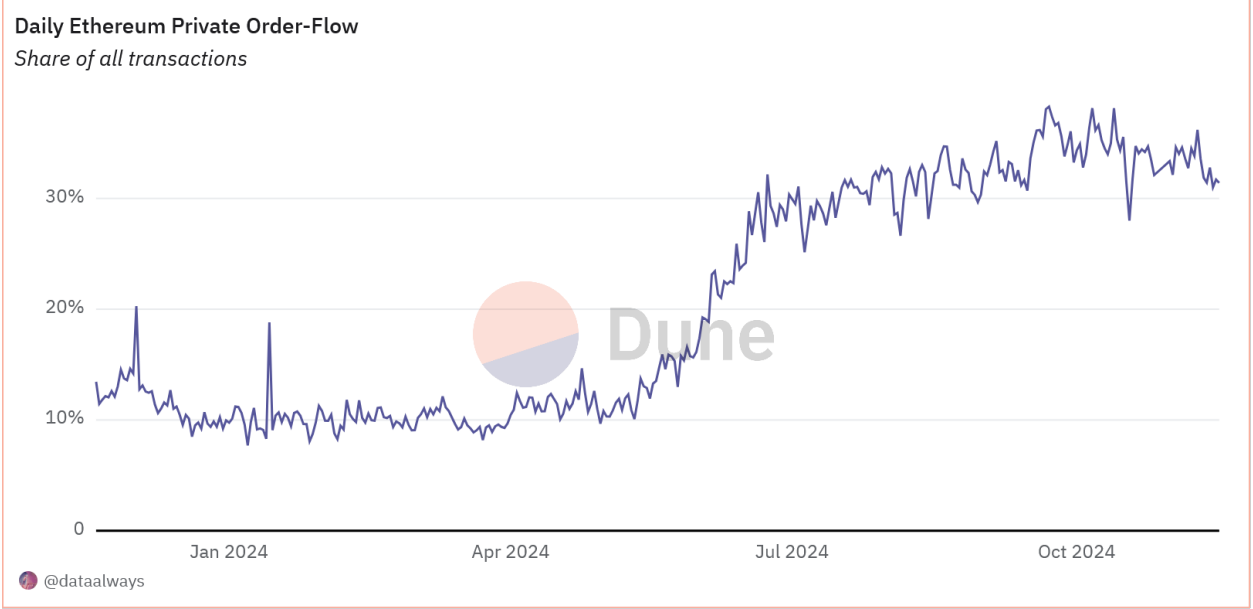
Figure 1: Private Transactions on Ethereum [29]

marginal contributions. We experimentally validate `RSYP`'s computing efficiency and approximation. In summary, the following are our contributions.

Contributions. (i) We define a cooperative game, `RST-Game`, over transaction creators based on the revenue generated, (ii) we prove that the Shapley value of transaction creators in the `RST-Game` is polynomial-time computable when the searcher valuations are additive, (iii) we motivate that computing Shapley value in the `RST-Game` when the searchers are single-minded bidders is possibly SUBEXP, (iv) we propose a randomized algorithm – Randomized ShapleY Procedure (`RSYP`) that closely estimates the exact Shapley value of transaction creators, (v) we empirically show the efficacy of our algorithm by comparing its outputs with the brute-force approach.

We believe our results provide valuable insights for the practical deployment of matchmaking in the future. We leave it for future work to examine what guarantees one can give around fair redistribution among transaction creators.

2 Related Work

MEV Auctions. [30] study various strategic interactions and auction setups of block builders with proposers. They evaluate how access to MEV opportunities and improved relay connectivity impact bidding performance. [31] propose an Ethereum gas auction model using the First Price Sealed-Bid Auction (FPSBA) between different bots and miners.

MEV redistributions.[32] model the MEV setting as a dynamical system with a fraction of MEV going to the miner as a dynamical variable updated with every time step. The miners and builders are assumed to be one entity, with the rest of the MEV returning to transaction creators. [33] discuss rebates in the context of liquidity providers in constant function market makers and discuss the auction between searcher and builders with the assumption of perfect MEV oracle that can compute the MEV extracted given the state of the blockchain and a new block of transactions. [34] proposes MEV redistribution as a dynamical system in which lending and staking portfolios of block proposer are chosen as a parameter that determines how much of the MEV extracted in a block is redistributed to staking.

Game Theory and Blockchains Researchers explored various game theoretic concepts in blockchains. E.g., the authors of [35, 36, 37] use concepts from mechanism design to design transaction fee mechanisms and fairness. [38, 39] study scalability issues in blockchains through game theory.[40] discusses on achieving fairness for Bitcoin in a transaction fee-only model. [41] studies the equilibrium behavior of the miners. In this work, we explore the use of cooperative game theory in matchmaking. [42] proposes a fair and secure distributed voting system that utilizes smart contracts to ensure that votes remain anonymous and are not tampered with during the voting process. [43] explores an AI framework designed for trustworthy data acquisition to enhance the reliability of data collection processes in multi-agent systems. Furthermore, [44] proposes a mechanism that promotes decentralization through block reward systems, aiming to enhance fairness and efficiency in blockchain networks.

3 Preliminaries

3.1 Matchmaking

Matchmaking executes in two steps: (i) the allocation of transactions to searchers and (ii) the redistribution of revenue generated through OFA. Consider a set of transactions $\mathcal{T} = \{t_1, t_2, \ldots t_n\}$ that can generate MEV, and a set of searchers $\mathcal{S} = \{s_1, s_2, \ldots s_m\}$, and a matchmaker M.

Matchmaking aims to assign these transactions to searchers to maximize their welfare. Each searcher s_i has valuation $v_{s_i} : 2^{\mathcal{T}} \rightarrow \mathbb{R}_+$. M an auction among the searchers. Each searcher makes appropriate bids. Each transaction is allocated to one searcher based on the searcher's bids. Then, the matchmaker collects payments p_{s_i} from each searcher s_i. The utility gained by searchers is due to the private transactions. Thus, transaction creators also play a significant role in maintaining the MEV ecosystem. In order to compensate them, the matchmaker shares the revenue generated by the auction, $\mathcal{R} = \sum_i p_{s_i}$, among the transaction creators.

Definition 1 (Matchmaking). *We define matchmaking as mechanism $\mathcal{M}$ which takes, $(\mathcal{T}, \mathcal{S}, (v_{s_i})_{s_i \in \mathcal{S}})$ as inputs, (conducts auction amongst $\mathcal{S}$ for $\mathcal{T}$,) and outputs (A, Γ) where A represents allocation of $\mathcal{T}$ and Γ represents the revenue distribution of $\mathcal{R}$. Reward to t_j is given by $r_{t_j} = \Gamma_{t_j} \mathcal{R}$ and $\sum_{t_j \in \mathcal{T}} \Gamma_{t_j} = 1$.*

Before discussing matchmaking mechanisms, we first discuss the possible valuation structures and corresponding type of auction and its payments in the following sections.

3.2 Searcher-Matchmaker Auctions

The searcher-matchmaker auction is combinatorial in nature, with searchers competing for a subset of transactions. Technically, the valuations for different transactions and bundles may have complex relationships. However, commonly it is seen in two forms: one where the searcher values each transaction separately and another where the searchers bid for a bundle of transactions. The former can be seen as searchers with *additive valuations* and the latter as searchers with *single-minded valuations*.

Additive Valuations. Searchers with additive valuations compete for the subset of transactions for which they have positive valuations. The valuation of any subset of items for a searcher is simply the sum of the individual valuations for the transactions in that subset, $v_{s_i}(B) = \sum_{t_j \in B} v_{s_i}(t_j)$. This model assumes that searchers value transactions independently of each other. Each searcher $s_i \in \mathcal{S}$ submits the n-tuple b_{s_i}

Definition 2 (Additive Valuations). *A valuation v is called additive if $v(B) = \sum_{i \in B} v(i)$, where $v(i)$ is the value of transaction i and B is any subset of transactions.*

The optimal allocation in such auctions is to give each transaction to the searcher that values it the most. The optimal allocation in such auctions—where searchers have additive valuations and bid for individual transactions—can indeed be implemented using second-price auctions with Vickrey-Clarke-Groves (VCG) payments individually for each transaction. VCG payments ensure desirable properties such as incentive compatibility, individual rationality, and optimal social welfare [45].

Single-Minded Valuations. To extract MEV, searchers often require the transactions in their bundles to be executed atomically, and hence, they only value a bundle if it is received in its entirety. Such searchers are referred to as single-minded searchers. A single-minded searcher values only one specific set or bundle of items, say B^* and has no interest in any other proper subset of B^*.

Definition 3 (Single-minded Valuations). *A valuation v is called single-minded if there exists a bundle of transactions B and a value $\bar{v} \in \mathbb{R}^+$ such that $v(B') = \bar{v}$ for all $B' \supseteq B$, and $v(B') = 0$ for all other B'.*

Finding the optimal allocation in this setting requires finding bundles that maximize social welfare while ensuring the bundles in optimal allocation are mutually disjoint. Both finding the optimal allocation and finding an optimal allocation that is better than $m^{\frac{1}{2}} - \epsilon$ is NP-hard [46]. Thus, such auctions are typically implemented using approximately social welfare auction mechanisms. In this paper, we use [46]'s ICA-SM, which greedily computes the best allocation and is $\sqrt{m}$-approximate optimal. ICA-SM ensures incentive compatibility and individual rationality and produces a $\sqrt{m}$-approximation of optimal social welfare.

3.3 Towards Matchmaking Mechanism

We address the matchmaking problem as follows. The value generated by each transaction need not be the same for all transaction creators. Thus, it would be equitable for all transaction creators to redistribute the generated revenue

---

Algorithm 1 ICA-SM [46]

1: **Input** : Bids $\{(B_{s_i}, b_{s_i})\}_{i=1}^n$
2: R $\leftarrow$ Sorted indices of searchers based on $b_{s_i}/\sqrt{|B_{s_i}|}$
3: $W \leftarrow \emptyset$.
4: **for** $k \in R$ **do**
5:    **if** $B_{s_k} \cap (\bigcup_{s_j \in W} B_{s_j}) = \emptyset$ **then**
6:       $W \leftarrow W \cup \{B_{s_k}\}$.
7:    **end if**
8: **end for**
9: **Payments** : For each $s_i \in W$, $p_{s_i} = b_{s_j}/\sqrt{|B_{s_j}|/|B_{s_i}|}$, where $j \in \{i+1, \ldots, n\}$ is the smallest index such that $B_{s_i} \cap B_{s_j} \neq \emptyset$, and for all $l < j, l \neq i$, $B_{s_l} \cap B_{s_j} = \emptyset$ (if no such s_j exists then $p_{s_i} = 0$).
10: **Output** : Set of Winners W

---

proportional to their respective contribution to the system. This naturally leads us to the solution concept of *Shapley value*. Towards this, we define a game known as `RST-Game`, and redistribute the revenue generated by the matchmaker according to the Shapley value of each transaction in this game.

3.4 Characteristic Form Games and Shapley Value

Cooperative game theory analyzes scenarios where players, or agents, can form coalitions to achieve collective goals. A *characteristic form game* (N, ν) is (i) a set of players, and (ii) $\nu : 2^N \to \mathbb{R}$, $\nu(S)$ represents the value $S \subset N$ can generate by forming a coalition. For a cooperative game, many solutions are proposed to redistribute value collectively among participants (or players).

Shapley Value Shapley value redistributes a cooperative game's total value or payoff to individual players based on their marginal contribution to every possible coalition. It is the only solution concept that satisfies all desirable properties of fair redistribution, such as efficiency, symmetry, and additivity [47]. $\varphi_j(\nu)$ of player j playing in characteristic form game (N, ν) is given as follows:

$$\varphi_j(\nu) = \sum_{S \subseteq \mathcal{N} \setminus j} \frac{|S|!(|\mathrm{N}| - |S| - 1)!}{|\mathrm{N}|!} \big(\nu(S \cup j) - \nu(S)\big) \tag{1}$$

Alternatively, Shapley value can be computed via permutations of players $\pi \in \Pi$, where Π is the set of all permutations of players in which players could join the coalition. $\pi(j)$ represents the set of players that precede j in the permutation π. The expression $\nu(\pi(j) \cup \{j\}) - \nu(\pi(j))$ is the marginal contribution of player j to the coalition $\pi(j)$.

$$\varphi_j(\nu) = \frac{1}{|N|!} \sum_{\pi \in \Pi} [\nu(\pi(j) \cup \{j\}) - \nu(\pi(j))] \tag{2}$$

4 Our Approach

4.1 `RST-Game`

`RST-Game` is a cooperative game $(\mathcal{T}, \nu)$ with $\mathcal{T}$, the transaction creators being the players. $\nu(T)$ where $T \subseteq \mathcal{T}$ is the value of transactions in T. We define it as the revenue collected by the matchmaker if only transactions T had been available i.e., the scenario when only searchers whose desired bundle $\tau \subseteq T$ are present. For each t_j, its marginal contribution to each $T \subseteq \mathcal{T} \setminus t_j$, requires finding the revenue with $T \cup t_j$ and T. $\Gamma_{t_j}^{SHAP}$ is computed as $\frac{\varphi_{t_j}}{\sum_{i \in [n]} \varphi_{t_i}}$.

For example, consider RST-Game with 3 searchers and 4 transactions, with corresponding (bundle, bid) pairs: $(\{1,2\}, 10), (\{3,4\}, 9), (\{2,4\}, 8)$. In this case, the winners are s_1, s_2 and each of them pays is $(8/\sqrt{(2)}) * \sqrt{2} = 8$ and the revenue is 16. $\Gamma_{t_1}^{SHAP} = \Gamma_{t_3}^{SHAP} = 0.154$, $\Gamma_{t_2}^{SHAP} = \Gamma_{t_4}^{SHAP} = 0.346$.

4.2 Shapley Value of `RST-Game` with Additive Valuation Searchers

Searchers bid for the subset of transactions and valuation for each transaction. Each searcher $s_i \in \mathcal{S}$ submits bid b_{s_i}, where $b_{s_i} \in \mathbb{R}^n$ is an n-tuple where $b_{s_i}[j]$ is s_i searcher's bid for transaction t_j.

M reduces this auction to n independent second-price auctions with VCG payments. For each transaction, $t_j \in \mathcal{T}$, M determines the searcher with the highest bid for t_j as the winner. The winner pays the amount of the second-highest bid. The algorithm for the winner determination in this case can be found in appendix.

The Shapley value of each winning transaction $t_j \in \mathcal{T}^*$ is computed using the permutation method. Let Π denote all the possible permutations of winning transaction set $\mathcal{T}^*$. For each permutation $\pi \in \Pi$, $\pi(t_j)$ denotes all the transactions present before t_j in π. We compute Shapley value of t_j as the average of the marginal contributions of t_j for each permutation π given by $\nu(\pi(t_j) \cup \{t_j\}) - \nu(\pi(t_j))$, where $\nu(\pi(t_j)) = \sum_{t_k \in \pi(t_j)} b_{s_{\text{second}}}[t_k]$.

$$\varphi_{t_j}(\nu) = \frac{1}{k!} \sum_{\pi \in \Pi} \nu(\pi(t_j) \cup \{t_j\}) - \nu(\pi(t_j))$$

Theorem 1. *The Shapley value of `RST-Game` $(\mathcal{T}, \nu))$ can be computed in polynomial time if ν is additive.*

Proof. As the searchers' valuations are additive, the marginal contribution of t_j in each $k!$ permutation is exactly the payment of the highest bidder $b_{s_{\text{second}}}[t_j]$. Hence, the Shapley value of t_j is $b_{s_{\text{second}}}[t_j]$ and redistribution fraction is $\Gamma_{t_j}^{\text{SHAP}} = \frac{b_{s_{\text{second}}}[t_j]}{\sum_{t_j \in T^*} b_{s_{\text{second}}}[t_j]}$. $\square$

4.3 Shapley Value of `RST-Game` for Single-Minded Searchers

Each searcher $s_i \in \mathcal{S}$ submits only a single subset $B_{s_i} \subseteq \mathcal{T}$ in bid $\{B_{s_i}, b_{s_i}\}$, where s_i's valuation v_{s_i} is single-minded. M reduces this auction to a combinatorial auction with single-minded bidders.

Let $\mathcal{T}^* \subseteq \mathcal{T}$ denote the winning transactions in the auction. In most instances of the `RST-Game` generated at random, the number of unique marginal contributions seems polynomial. However, we show in Theorem 2 that the number of unique values of the marginal contribution in `RST-Game` can be subexponential in certain instances due to the underlying (bundle, bid) structure.

Theorem 2. *The number of unique marginal contributions in the computation of the Shapley value of transaction creators in `RST-Game` can be $\Omega(2^{\sqrt{n}})$.*

Proof. Proof by construction:

Consider an instance of the `RST-Game` with set of transactions $\mathcal{T} = \{t_1, \dots t_n\}$. Let the set of searchers $\mathcal{S} = \{s_1, \dots s_m\}$ be divided into two classes of searchers with equal cardinality, $\mathcal{S}_0$ and $\mathcal{S}_1$ with corresponding set of bundles $\mathcal{B}_0$ and $\mathcal{B}_1$ satisfying the following 2 properties:

- None of the bundles in $\mathcal{B}_0$ or $\mathcal{B}_1$ intersects with any other bundle in $\mathcal{B}_0$ or $\mathcal{B}_1$, respectively, i.e., $\forall B_{s_i}, B_{s_j} \in \mathcal{B}_0, B_{s_i} \cap B_{s_j} = \phi$. In other words, bundles within $\mathcal{B}_0$ are mutually exclusive and bundles within $\mathcal{B}_1$ are mutually exclusive.

- Each bundle in $\mathcal{B}_0$ intersects with every bundle in $\mathcal{B}_1$ and vice versa, i.e., $\forall B_{s_i} \in \mathcal{B}_0, \forall B_{s_j} \in \mathcal{B}_1, B_{s_i} \cap B_{s_j} \neq \phi$.

Here is a construction satisfying the above properties:
Let $m = 2\sqrt{n}$. Thus, $|\mathcal{B}_0| = |\mathcal{B}_1| = m/2 = \sqrt{n}$. Let the size of each bundle be $\sqrt{n}$, i.e., $|B_{s_i}| = \sqrt{n}, \forall s_i \in \mathcal{S}$. Consider the arrangement of transactions as matrix E shown below:

$$E = \begin{bmatrix} t_1 & t_2 & t_3 & \cdots & t_{\sqrt{n}} \\ t_{\sqrt{n}+1} & t_{\sqrt{n}+2} & t_{\sqrt{n}+3} & \cdots & t_{2\sqrt{n}} \\ t_{2\sqrt{n}+1} & t_{2\sqrt{n}+2} & t_{2\sqrt{n}+3} & \cdots & t_{3\sqrt{n}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{n-\sqrt{n}+1} & t_{n-\sqrt{n}+2} & t_{n-\sqrt{n}+3} & \cdots & t_n \end{bmatrix}$$

$$\mathcal{B}_0 = \left\{ \begin{array}{c} \{t_1, t_2, \ldots, t_{\sqrt{n}}\}, \\ \{t_{\sqrt{n}+1}, t_{\sqrt{n}+2}, \ldots, t_{2\sqrt{n}}\}, \\ \ldots, \\ \{t_{n-\sqrt{n}+1}, t_{n-\sqrt{n}+2}, \ldots, t_n\} \end{array} \right\}$$

$$\mathcal{B}_1 = \left\{ \begin{array}{c} \{t_1, t_{\sqrt{n}+2}, t_{2\sqrt{n}+3} \ldots, t_n\}, \\ \{t_{\sqrt{n}+1}, t_{2\sqrt{n}+2}, \ldots, t_{n-1}, t_{\sqrt{n}}\}, \\ \ldots, \\ \{t_{n-\sqrt{n}+1}, t_2, t_{\sqrt{n}+3} \ldots, t_{n-\sqrt{n}}\} \end{array} \right\}$$

Bundles in $\mathcal{B}_0$ are essentially individual rows from the matrix E. Bundles in $\mathcal{B}_1$ contain one transaction from each row and each column of matrix E [2]. It can be shown that none of the bundles in $\mathcal{B}_0$ or $\mathcal{B}_1$ intersects with any other bundle in $\mathcal{B}_0$ or $\mathcal{B}_1$ respectively. It can also be shown that the intersection of a bundle from $\mathcal{B}_0$ and a bundle from $\mathcal{B}_1$ is a singleton [3].

Let us denote the bundles of $\mathcal{B}_0$ as $B_1^0, \ldots, B_{\sqrt{n}}^0$ and the corresponding bids as $b_1^0, b_2^0, \ldots, b_{\sqrt{n}}^0$ such that $b_1^0 > b_2^0 > \ldots > b_{\sqrt{n}}^0$. Similarly, we denote the bundles of $\mathcal{B}_1$ as $B_1^1, \ldots, B_{\sqrt{n}}^1$ and the corresponding bids as $b_1^1, b_2^1, \ldots, b_{\sqrt{n}}^1$ such that $b_1^1 > b_2^1 > \ldots > b_{\sqrt{n}}^1$. For ease of exposition, we also require the bid values to be $3^{(2\sqrt{n}-2i+1)}$ for b_i^0 and $3^{(2\sqrt{n}-2i)}$ for b_i^1. Thus,

$$b_1^0 = 3^{(2\sqrt{n}-1)} > b_1^1 = 3^{(2\sqrt{n}-2)} > b_2^0 = 3^{(2\sqrt{n}-3)} >$$

$$\ldots > b_{\sqrt{n}}^0 = 3^1 > b_{\sqrt{n}}^1 = 3^0$$

We now show that while computing Shapley values of all transactions using ICA-SM for the above construction, we will encounter at least $2^{\sqrt{n}} - 1$ unique marginal values. The main insight in our approach is that corresponding to any of the non-empty $2^{\sqrt{n}} - 1$ combinations of bundles from $\mathcal{B}_0$, there exists a unique transaction set T and transaction t_j such that $\nu(T) - \nu(T \setminus \{t_j\})$ gives a unique marginal contribution.

Transaction selection: Let the bundles selected from $\mathcal{B}_0$ in the combination be $B_a^0, \ldots, B_z^0$. Then, we define our transaction set as $T = \bigcup_{x=a}^{x=z} B_x^0 \cup B_x^1$. We note the following:

1. Let $\{t_x\} = B_x^0 \cap B_x^1$ and $\{t_y\} = B_y^0 \cap B_y^1$. Then, if $B_x^0 \neq B_y^0 \implies t_x \neq t_y$.
   We can prove this by contradiction. Suppose
   $$\exists B_x^0, B_y^0 | B_x^0 \neq B_y^0 \land t_x = t_y$$
   $$\implies t_x \in B_x^0 \land t_x \in B_y^0$$
   $$\implies t_x \in B_x^0 \cap B_y^0$$
   $$\implies B_x^0 \cap B_y^0 \neq \phi$$
   Given that all bundles in $\mathcal{B}_0$ are mutually exclusive, this is a contradiction.

2. Let $\{t_x\} = B_x^0 \cap B_x^1$. If B_x^0 is selected, $t_x \in T$.
   This is trivially true because $T = \bigcup B_x^0 \cup B_x^1$ for all selected bundles B_x^0.

3. Let $\{t_x\} = B_x^0 \cap B_x^1$. If B_x^0 is not selected, $t_x \notin T$.
   We prove this by contradiction. Let B_y^0 and B_y^1 represent any selected bundle. Suppose $t_x \in T$

   $$\implies (\exists B_y^0 | t_x \in B_y^0) \lor (\exists B_y^1 | t_x \in B_y^1)$$
   $$\implies (t_x \in B_x^0 \land \exists B_y^0 | t_x \in B_y^0) \lor$$
   $$(t_x \in B_x^1 \land \exists B_y^1 | t_x \in B_y^1)$$
   $$\implies (\exists B_y^0 | t_x \in B_y^0 \cap B_x^0) \lor (\exists B_y^1 | t_x \in B_y^1 \cap B_x^1)$$
   $$\implies (\exists B_y^0 | B_y^0 \cap B_x^0 \neq \phi) \lor (\exists B_y^1 | B_y^1 \cap B_x^1 \neq \phi)$$

---

[2]Note that $(\sqrt{n})!$ such selections of $\mathcal{B}_1$ are possible, given the same $\mathcal{B}_0$.

[3]More specifically, $B_x^1 \cap B_y^0$ is the transaction in $B_x^1 \in \mathcal{B}_1$ with the row number y in matrix E where bundle $B_y^0 \in \mathcal{B}_0$ is the bundle corresponding to row y in matrix E.

Given that all bundles within $\mathcal{B}_0$ and $\mathcal{B}_1$ are mutually exclusive, this is a contradiction.

4. While aggregating which searchers are allotted their bundles given the set of transactions T, only the following two cases are possible:

   - All allotted bundles are from $\mathcal{B}_0$ and their payments are some bids b_x^1, i.e. bid value of a bundle in $\mathcal{B}_1$.
   - All allotted bundles are from $\mathcal{B}_1$ and their payments are some bids b_x^0, i.e. bid value of a bundle in $\mathcal{B}_0$.

   This is true because our construction obeys the two properties mentioned above: i) mutual exclusion within $\mathcal{B}_0$ and $\mathcal{B}_1$, and, ii) non-empty intersection between any bundle from $\mathcal{B}_0$ and $\mathcal{B}_1$.

5. The ICA-SM payment [4] corresponding to B_x^0 is b_x^1.
   Transactions of both B_x^0 and B_x^1 are present in T. Also, according to our assigned bid values, $\nexists b_y | b_x^0 < b_y < b_x^1$, i.e., bid b_x^1 is the highest bid smaller than bid b_x^0. Given that B_x^0 and B_x^1 intersect, the searcher corresponding to bundle B_x^0 pays b_x^1.

6. The ICA-SM payment corresponding to the bundle B_x^1 is either 0 (if B_x^0 was the bundle with the least bid among the selected bundles) or b_y^0 for some bundle B_y^0, where b_y^0 is the highest bid less than b_x^1.

7. Let B_a^0 be the selected bundle with the highest bid. Let B_w^0 be one of the unselected bundles (if all bundles are selected, consider the least valued bundle B_z^0 instead). Thus, $\exists t_u \in B_a^0 \cap B_w^1$.
   When the transaction set is $\tau = T \setminus \{t_u\}$, $\nu(\tau \cup \{t_u\}) = \sum_x b_x^1$ and $\nu(\tau) = (\sum_x b_x^0) - b_a^0$, where B_a^0 is the bundle with the highest bid.
   Thus, the marginal contribution of coalition τ for Shapley value of t_u is $\sum_x b_x^1 - \sum_x b_x^0 + b_a^0$.

Using (1), (2) and (3), it can be argued that corresponding to every bundle B_x^0, there is a unique transaction t_x which belongs to T if and only if B_x^0 is selected. Thus, while considering all non-empty selections of bundles, we are considering $2^{\sqrt{n}} - 1$ unique subsets of $\mathcal{T}$. Each of these unique sets of transactions is involved in marginal contributions of some transaction t_u, as shown in (7). The marginal contributions $\sum_x b_x^1 - \sum_x b_x^0 + b_a^0$ are the sum of all bids with coefficients either $-1, 0$ or 1. Thus, for these bid values (powers of 3) and bundles and coefficients $-1, 0$, or 1, all possible summations, and hence the marginal contributions are unique. Refer to the Appendix for the proof.

Thus, we proved that there exist instances of RST-Game in which the number of unique marginal contributions:

   - in terms of n: is more than $(2^{\sqrt{n}} - 1)$. Thus, time complexity is $\Omega(2^{\sqrt{n}})$, i.e., SUBEXP in n.

   - in terms m: is more than $(2^{m/2} - 1)$. Thus, time complexity is $\Omega(2^{m/2})$, i.e., EXP in m.

$\square$

Games in which Shapley values can be computed in polynomial time often compute unique marginal contributions and find out how many times they occur. Both these steps must take polynomial time. In addition to these requirements, such games have a more well-defined structure that allows for optimizing the computation of Shapley value. RST-Game allows searchers to propose any arbitrary bundles. Any proposed algorithm must work for all such possible arbitrary bundles. With these two insights, we conjecture the following:

Conjecture 1. *Shapley value computation of transaction creators in RST-Game with single-minded searchers can be SUBEXP in number of transaction creators n.*

Unanimity Games and Shapley Value. The structure of RST-Game can be derived from unanimity games. Let $U_S = (\mathcal{T}, \omega_S)$ be unanimity game such that

$$\forall T \subseteq \mathcal{T}, \omega_S(T) = \begin{cases} 1 & S \subseteq T \\ 0 & \text{Otherwise} \end{cases} \tag{3}$$

The Shapley value of $t_j \in \mathcal{T}$ in U_S is given by $\varphi_{t_j} = \frac{1}{|S|}$. The set of all unianimity functions $W = \{\omega_S | S \subseteq T\}$ forms a basis for the characteristic function $\nu : 2^{\mathcal{T}} \to \mathbb{R}$ and ν can be represented as a linear combination of elements

---

[4] As the size of all bundles in $\mathcal{B}_0$ and $\mathcal{B}_1$ is $\sqrt{n}$, ICA-SM ordering is the same as ordering of the bids – the common factor $\sqrt{n}$ cancels out. Similarly, the payments (Step 9 in Algorithm 1) $p_{s_i} = b_{s_j}/\sqrt{|B_{s_j}|/|B_{s_i}|} = b_{s_j}$ as $|B_{s_j}| = |B_{s_i}| = \sqrt{n}$

of W, i.e., $\forall C \subseteq T \setminus \phi, \nu(C) = \sum_{T \in 2^{\mathcal{T}} \setminus \phi} \Delta_T w_T(C)$, where Δ_Ts are referred to as *Harsanyi dividends*. Based on unianimity game, the Shapley value can be written as

$$\varphi_{t_j} = \sum_{T \in 2^{\mathcal{T}} \setminus \phi,\ t_j \in T} \frac{\Delta_T}{|T|} \tag{4}$$

The Harsanyi dividends Δ_T can be computed using the following equation

$$\Delta_T = \sum_{C \subseteq \mathcal{T}} (-1)^{|\mathcal{T}| - |C|} \nu(C) \tag{5}$$

Note that Δ_T can be computed efficiently when $|\{\nu(C) | C \in 2^{\mathcal{T}} \setminus \phi\}|$ is polynomial in n and m i.e., the number of possible different revenues generated over all subset of searchers are polynomial. With the construction provided above, one can observe that $\forall x \in \{1, \dots \sqrt{n}\}, T_x = B_x^0 \cup B_x^1$ the value of $\nu(T_x)$ is unique and thus, the number of distinct possible revenues can be sub-exponential. Hence, computing the dividends requires finding all the values. Therefore, the Shapley value computation via Unamity games would be sub-exponential. Further, one can empirically verify Theorem 2 and observe that variation in the number of marginal contributions with an increasing number of transactions is sub-exponential. The details of our analysis are provided in the Appendix. To this end, we propose to use a randomized approach to approximate the Shapley value.

4.4 Approximating Shapley Value

The Shapley value computation can go sub-exponential due to the underlying structure of the game, as shown in our construction. The occurrence of such structures is typically rare as the real world closely follows some distribution [5]. Due to this behavior (the number of different bundles submitted $\ll$ the total number of all possible bundles), the number of unique marginal contributions in Shapley value computation is $\mathcal{O}(n)$ (since most of them would be 0). So, we propose `RSYP` a randomized algorithm to compute the approximate Shapley value of each transaction. Algorithm 2 describes `RSYP`. Let Π be the set of all permutations of transactions Π. Let $\bar{\Pi}$ the set of k different permutations sample from Π. Let $\bar{\Pi}_k$ denote the set of permutations sampled from Π. For each transaction t_j, the approximate Shapley value $\tilde{\varphi}_j$ is computed marginal contribution of t_j to each $\pi \in \Pi$, averaged over k. Among the winning transactions selected via greedy approximation, the fraction of revenue redistributed to transaction creator j is given by $\Gamma_{t_j}^{RSYP} = \frac{\tilde{\varphi}_{t_j}(\nu)}{\sum_{j \in [n]} \tilde{\varphi}_{t_j}(\nu)}$ using `RSYP`. We empirically show, for $k = \mathcal{O}(n^2), \forall t_j \in \mathcal{T}, \Gamma_{t_j}^{\text{RSYP}}$ computed via `RSYP` approaches $\varphi_{t_j}(\nu)$.

Algorithm 2 `RSYP`

1: **Input** : $\bar{\Pi}, n, k$
2: **for** $j = 1$ to n **do**
3:     $MC_{sum} = 0$
4:     **for** $\pi \in \bar{\Pi}$ **do**
5:         $MC = \nu(\pi(j) \cup j) - \nu(\pi(j))$
6:         $MC_{sum} \mathrel{+}= MC$
7:     **end for**
8:     $\varphi_{t_j}(\nu) = \frac{MC_{sum}}{k}$
9: **end for**
10: **for** $j = 1$ to n **do**
11:     $\Gamma_{t_j}^{RSYP} = \frac{\tilde{\varphi}_{t_j}(\nu)}{\sum_{j \in [n]} \tilde{\varphi}_{t_j}(\nu)}$
12: **end for**
13: **Output** :$\{ \Gamma_{t_j}^{RSYP} \}_{j \in [n]}$

4.4.1 Error Analysis

The computation of the Shapley value of any transaction t_j is essentially a sum of marginal contributions weighted by $\frac{1}{|N!|}$ as shown in Equation 2. A marginal contribution of t_j to $T \subseteq \mathcal{T}$ in `RST-Game` is the difference in revenue

---

[5]We often see some transactions being more lucrative than others to almost all of the searchers and occasionally, some transactions being relatively highly valued by only a few (specialized) searchers [48]

(sum of payments) when only the searchers $s_i : B_{s_i} \subseteq T \cup \{t_j\}$ are present and $\{s_i : B_{s_i} \subseteq T\}$ are present. Thus, the marginal contribution in φ_j computation is at most the maximum revenue and at least the minimum revenue.

Let Π^{ord} be set of all elements of Π, ordered with a some total order on Π. Let π_i represent the permutation at i^{th} index in Π^{ord}. Let X_i^j represent the marginal contribution of t_j to $\pi_i(j)$. Then φ_{t_j} can be written as $\frac{1}{N!} \sum_{i \in [N!]} X_i^j$. Let K represent the indices of permutations drawn uniformly at random from Π^{ord}, then we have, $\tilde{\varphi}_{t_j} = \frac{1}{k} \sum_{k \in K} X_k^j$.

We want to find out the following $P(\tilde{\varphi}_{t_j} - \varphi_{t_j} \geq t) \leq 1 - \delta$. Since X_i^j are bounded, we use Hoeffding's inequality to find the upper bound on $P(\tilde{\varphi}_{t_j} - \varphi_{t_j} \geq t)$. From Hoeffding's inequality, we know that, for $S_n = \sum_{i \in [n]} X_i$, where X_i are independent random variables and $X_i \in [a_i, b_i]$,

$$P(S_n - \mathbb{E}[S_n] \geq t) \leq e^{\frac{-2t^2 n^2}{\sum_{i \in [n]} (b_i - a_i)^2}} \tag{6}$$

$\mathbb{E}[\tilde{\varphi}_{t_j}] = \mathbb{E}\big[\frac{1}{k} \sum_{k \in K} X_k^j\big] = \frac{1}{N!} \sum_{i \in [N!]} X_i^j = \varphi_{t_j}$. Thus, $P(\tilde{\varphi}_j - \varphi_j \geq t) = P(\tilde{\varphi}_j - \mathbb{E}[\tilde{\varphi}_j] \geq t)$. Thus, we have,

$$P(\tilde{\varphi}_j - \varphi_j \geq t) \leq e^{\frac{-2t^2 k^2}{\sum_{k \in K} (b-a)^2}} = e^{\frac{-2t^2 k}{(b-a)^2}} \tag{7}$$

Let the sum of all bids $\sum_{i \in m} b_i = R^*$. Since, the revenue is at most R^*, we have $\forall i \in [N!], -R^* \leq X_i^j \leq R^*$, Using this, we get $k \geq \frac{2R^{*2}}{t^2} \ln(\frac{1}{1-\delta})$.

5 Experimental Analysis

5.1 Setup

We demonstrate the efficacy of `RSYP` in `RST-Game` by comparing the redistributions of Shapley values from the exact and approximation methods across 10K randomly generated `RST-Game` instances, each with varying searcher bids and transaction bundles.

5.2 Results

We observe the mean redistribution fraction via exact Shapley value and `RSYP` are almost the same. Figures 2 and 3 show similar behavior over all the transaction creators for varying n and m. Hence, $\Gamma_{\text{RSYP}} \to \Gamma_{t_j}^{SHAP}$ in `RSYP` with $k = \mathcal{O}(n^2)$.

6 Conclusion

In this work, we explored the problem of matchmaking in MEV. We defined a cooperative game `RST-Game` over transaction creators and proved that computing Shapley value for fair revenue redistribution among transaction creators is SUBEXP. We proposed a randomized algorithm that approximates the Shapley value very well for $\mathcal{O}(n^2)$ where n is the number of transactions.

Future Work. We leave the future to analyze the complexity of the fair revenue redistribution for more general valuations of searchers. We believe the complexity would be at least as much as in the single-minded case.

References

[1] Melanie Swan. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Satoshi Nakamoto*, 2008.

[3] Vitalik Buterin et al. Ethereum white paper. *GitHub repository*, 1:22–23, 2013.

[4] Ethereum. Maximal extractable value (MEV) | ethereum.org — ethereum.org. `https://ethereum.org/en/developers/docs/mev/`. [Accessed 23-09-2024].

[5] Chainlink. Maximal Extractable Value (MEV) | Chainlink — chain.link. `https://chain.link/education-hub/maximal-extractable-value-mev`. [Accessed 23-09-2024].
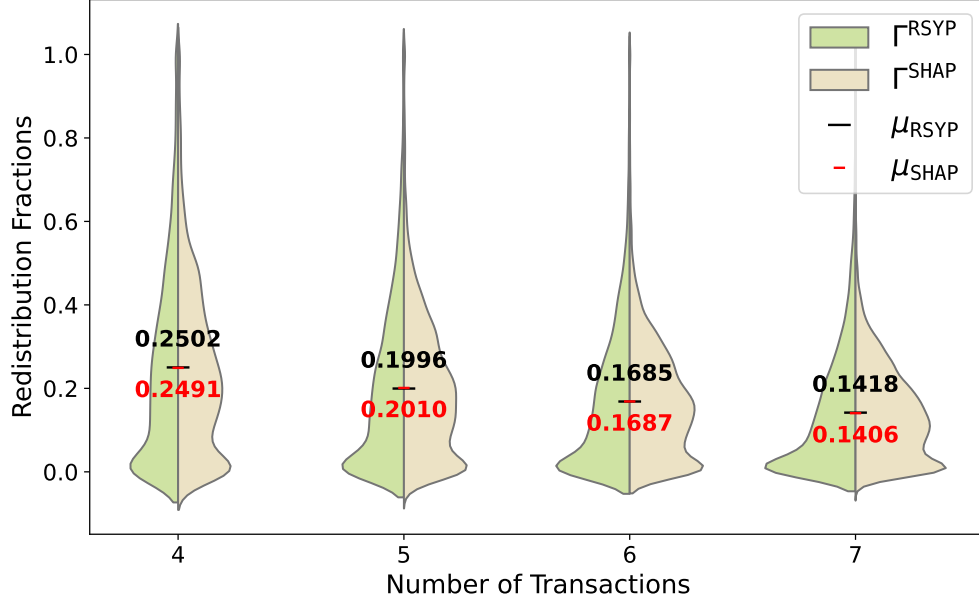
Figure 2: Distribution of Γ^{RSYP}, Γ^{SHAP} vs n for $m = 6$
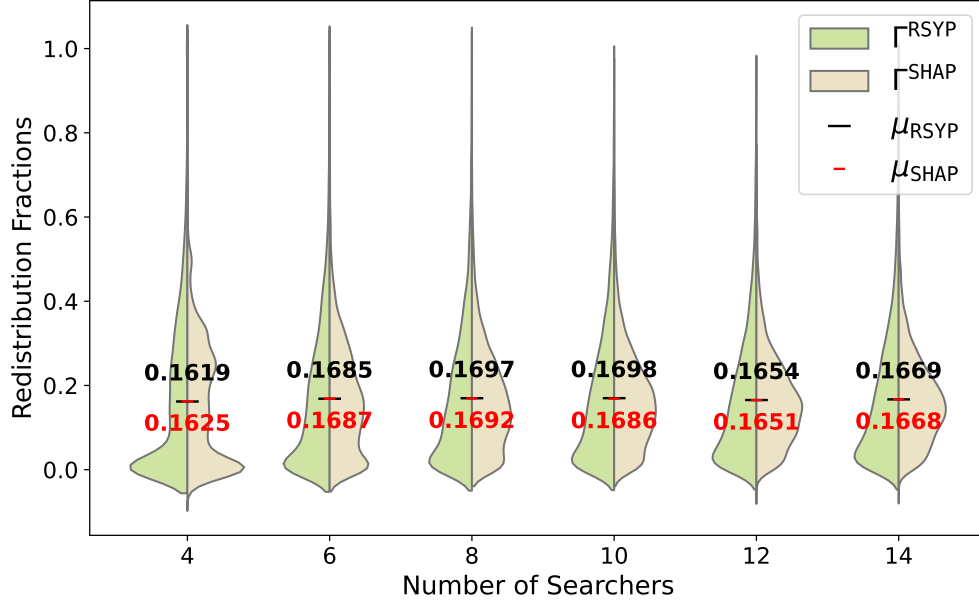
Figure 3: Distribution of Γ^{RSYP}, Γ^{SHAP} vs m for $n = 6$

[6] Jonah Burian. The future of mev, 2024.

[7] Christof Ferreira Torres, Albin Mamuti, Ben Weintraub, Cristina Nita-Rotaru, and Shweta Shinde. Rolling in the shadows: Analyzing the extraction of mev across layer-2 rollups, 2024.

[8] Luganodes. Luganodes | What is MEV?: Explained — luganodes.com. `https://www.luganodes.com/blog/mev-explained-maximal-extractable-value/`, 2023. [Accessed 1-10-2024].

[9] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927, 2020.

[10] Simona Ramos and Joshua Ellul. The mev saga: Can regulation illuminate the dark forest? In Marcela Ruiz and Pnina Soffer, editors, *Advanced Information Systems Engineering Workshops*, pages 186–196, Cham, 2023. Springer International Publishing.

[11] Yan Ji and James Grimmelmann. Regulatory implications of mev mitigations. In *Proceedings of the 5th Workshop on the Coordination of Decentralized Finance*, 2024.

[12] Yash Chaurasia, Parth Desai, Sujit Gujar, et al. Mev ecosystem evolution from ethereum 1.0. *arXiv preprint arXiv:2406.13585*, 2024.

[13] Tivas Gupta, Mallesh M Pai, and Max Resnick. The centralizing effects of private order flow on proposer-builder separation, 2023.

[14] Frontier Research. Builder Dominance and Searcher Dependence — frontier.tech. `https://frontier.tech/builder-dominance-and-searcher-dependence`, 2023. [Accessed 22-09-2024].

[15] https://twitter.com/zeroXbrock. Searching Post-Merge | Flashbots Writings — writings.flashbots.net. `https://writings.flashbots.net/searching-post-merge`, 2022. [Accessed 22-09-2024].

[16] Jan Arvid Berg, Robin Fritsch, Lioba Heimbach, and Roger Wattenhofer. An empirical study of market inefficiencies in uniswap and sushiswap. In *International Conference on Financial Cryptography and Data Security*, pages 238–249. Springer, 2022.

[17] The Crypto Cortex. Understanding Market Inefficiencies and Arbitrage in Crypto - The Crypto Cortex — thecryptocortex.com. `https://thecryptocortex.com/market-inefficiencies-and-arbitrage/`, 2024. [Accessed 22-09-2024].

[18] Tianyang Chi, Ningyu He, Xiaohui Hu, and Haoyu Wang. Remeasuring the arbitrage and sandwich attacks of maximal extractable value in ethereum. *arXiv preprint arXiv:2405.17944*, 2024.

[19] Ye Wang, Patrick Zuest, Yaxing Yao, Zhicong Lu, and Roger Wattenhofer. Impact and user perception of sandwich attacks in the defi ecosystem. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2022.

[20] Quintus Kilbourn. order flow, auctions and centralisation I - a warning | Flashbots Writings — writings.flashbots.net. `https://writings.flashbots.net/order-flow-auctions-and-centralisation`. [Accessed 02-10-2024].

[21] Max Resnick Mallesh Pai. Structural Advantages for Integrated Builders in MEV-Boost — arxiv.org. `https://arxiv.org/abs/2311.09083`, 2023.

[22] bert. MEV-Share: programmably private orderflow to share MEV with users — collective.flashbots.net. `https://collective.flashbots.net/t/mev-share-programmably-private-orderflow-to-share-mev-with-users/1264`, 2023. [Accessed 23-07-2024].

[23] shea. Announcing MEV-share beta — collective.flashbots.net. `https://collective.flashbots.net/t/announcing-mev-share-beta/1650`. [Accessed 25-07-2024].

[24] Flashbots. Mev-share: programmably private orderflow to share mev with users — collective.flashbots.net. `https://collective.flashbots.net/t/mev-share-programmably-private-orderflow-to-share-mev-with-users/1264`, 2023. [Accessed 10-10-2024].

[25] Flashbots Research Proposals. Frp-30: Quantifying shareable mev collective.flashbots.net. `https://collective.flashbots.net/t/frp-30-quantifying-shareable-mev/1618`, 2023. [Accessed 10-10-2024].

[26] Xiaotie Deng and Christos H Papadimitriou. On the complexity of cooperative solution concepts. *Mathematics of operations research*, 19(2):257–266, 1994.

[27] Tom C van der Zanden, Hans L Bodlaender, and Herbert JM Hamers. Efficiently computing the shapley value of connectivity games in low-treewidth graphs. *Operational Research*, 23(1):6, 2023.

[28] Tomasz P Michalak, Karthik V Aadithya, Piotr L Szczepanski, Balaraman Ravindran, and Nicholas R Jennings. Efficient computation of the shapley value for game-theoretic network centrality. *Journal of Artificial Intelligence Research*, 46:607–650, 2013.

[29] @dataalways/ Private Order Flow Monitor. Private order flow. `https://dune.com/dataalways/private-order-flow`, 2024. [Accessed 10-12-2024].

[30] Fei Wu, Thomas Thiery, Stefanos Leonardos, and Carmine Ventre. Strategic bidding wars in on-chain auctions. In *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 503–511, 2024.

[31] Congying Jin, Taotao Wang, Zhe Wang, Long Shi, and Shengli Zhang. First-price sealed-bid auction for ethereum gas auction under flashbots. In *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, pages 449–457, 2023.

[32] Georgios Chionas, Pedro Braga, Stefanos Leonardos, Carmine Ventre, Georgios Piliouras, and Piotr Krysta. Who gets the maximal extractable value? a dynamic sharing blockchain mechanism. In *Proceedings of the 23rd International Conference on Autonomous Agents and Multi-Agent Systems (AAMAS 2024)*, 2024.

[33] Bruno Mazorra and Nicolás Della Penna. Towards optimal prior-free permissionless rebate mechanisms, with applications to automated market makers & combinatorial orderflow auctions. *arXiv preprint arXiv:2306.17024*, 2023.

[34] Tarun Chitra and Kshitij Kulkarni. Improving proof of stake economic security via mev redistribution. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security*, pages 1–7, 2022.

[35] Tim Roughgarden. Transaction fee mechanism design. *Journal of the ACM*, 71(4):1–25, 2024.

[36] Sankarshan Damle, Manisha Padala, and Sujit Gujar. Designing redistribution mechanisms for reducing transaction fees in blockchains. *arXiv preprint arXiv:2401.13262*, 2024.

[37] Sankarshan Damle, Varul Srivastava, and Sujit Gujar. No transaction fees? no problem! achieving fairness in transaction fee mechanism design. *arXiv preprint arXiv:2402.04634*, 2024.

[38] Anurag Jain, Shoeb Siddiqui, and Sujit Gujar. We might walk together, but i run faster: Network fairness and scalability in blockchains. *arXiv preprint arXiv:2102.04326*, 2021.

[39] Lin Chen, Lei Xu, Zhimin Gao, Ahmed Imtiaz Sunny, Keshav Kasichainula, and Weidong Shi. A game theoretical analysis of non-linear blockchain system. *Distributed Ledger Technologies: Research and Practice*, 3(1):1–24, 2024.

[40] Shoeb Siddiqui, Ganesh Vanahalli, and Sujit Gujar. Bitcoinf: Achieving fairness for bitcoin in transaction-fee-only model. *arXiv preprint arXiv:2003.00801*, 2020.

[41] Anurag Jain, Sanidhay Arora, Sankarshan Damle, and Sujit Gujar. Tiramisu: Layering consensus protocols for scalable and secure blockchains. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–3. IEEE, 2022.

[42] Sankarshan Damle, Sujit Gujar, and Moin Hussain Moti. Fasten: Fair and secure distributed voting using smart contracts. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–3. IEEE, 2021.

[43] Boi Faltings and Sujit Gujar. Orthos: A trustworthy ai framework for data acquisition. In *Engineering Multi-Agent Systems: 8th International Workshop, EMAS 2020, Auckland, New Zealand, May 8–9, 2020, Revised Selected Papers*, volume 12589, page 100. Springer Nature, 2021.

[44] Varul Srivastava and Sujit Gujar. Decent-brm: Decentralization through block reward mechanisms. *arXiv preprint arXiv:2401.08988*, 2024.

[45] Yadati Narahari. *Game theory and mechanism design*, volume 4. World Scientific, 2014.

[46] Liad Blumrosen and Noam Nisan. *Algorithmic game theory*. Cambridge Univ. Press New York, NY, USA, 2007.

[47] Lloyd S Shapley. A value for n-person games. *Contribution to the Theory of Games*, 2, 1953.

[48] EigenPhi. Mev data | eigen phi — eigenphi.io. `https://eigenphi.io/`, 2022. [Accessed 1-10-2024].

A Matchmaking

A.1 Matchmaking vs OFA

A regular OFA only ensures that private transactions are sold off to the highest bidder but doesn't ensure the timely execution of the transaction. Consider the scenario where the searcher chooses not to send the transactions to a block builder and retain them for the future. While an OFA can introduce a penalty for the searcher that misses the slot, where an OFA waits for a deterministic amount of time and forwards the transaction by itself or auctions it again, it is hard to identify if the transactions did not make it to execution solely due to searcher and not due to network latency, high competition for blockspace. Hence, potentially enforcing cooperation is not easy. Further, the auctioneer can increase the revenue by selling multiple transactions simultaneously as a bundle to searchers rather than individually [22]. Matchmaking is a recent introduction in the MEV world, where a *matchmaker* aggregates transactions from transaction creators, exposes transaction data to searchers, collects bids along with partial bundles, creates final bundles, and bids to builders for inclusion [23]. Searchers bid different subsets of transactions, and the matchmaker computes to find optimal

allocation. This requires optimizing for the best bundles in a finite amount of time and redistributing the revenue back to the transaction creators to compensate for the value they create.

Desirable Properties of Matchmaking

We now discuss the desirable properties of matchmaking. Matchmaking involves allocating transactions to searchers and compensating transaction creators. Mathematically, let:

- v_i be the true valuation of searcher i for the allocation $A \in \mathcal{A}$ (set of possible allocations).
- b_i be the bid of searcher i.
- $A(b)$ be the allocation rule based on all bids $b = (b_1, b_2, \ldots, b_n)$.
- $p_i(b)$ be the payment rule for searcher i.
- $r_i(b)$ be the reward for transaction creator i

Some of the generally desired properties of auction mechanisms are:

1. Incentive Compatibility (Truthfulness): A mechanism is incentive-compatible (or truthful) if each searcher's best strategy is to bid their true valuation of the good, regardless of what others are doing. In such a mechanism, searchers have no incentive to misrepresent their preferences. The mechanism is incentive-compatible for searchers if:

$$v_i(A(b_i, b_{-i})) - p_i(b_i, b_{-i}) \geq v_i(A(b_i', b_{-i})) - p_i(b_i', b_{-i}), \tag{8}$$

for all b_i', where b_{-i} are the bids of all other agents.

2. Allocative Efficiency (Social Welfare) Allocative Efficiency or Social Welfare Maximizing allocation refers to the allocation that maximizes total value for all searchers, i.e.,

$$\max_{A \in \mathcal{A}} \sum_{i=1}^{m} v_i(A(b)). \tag{9}$$

3. Individual Rationality A matchmaking $\mathcal{M}$ is individually rational if it is individually rational for both searchers and transaction creators. Each searcher is at least as well off by participating in the matchmaking as they would be if they chose not to participate. Similarly, the utility of each transaction creator is at least as well by including it in matchmaking as they would if they choose not to be involved in matchmaking. Formally, the utility $u_i^{\mathcal{S}}$ of searcher i and utility $u_i^{\mathcal{T}}$ should be non-negative:

$$u_i^{\mathcal{S}} = v_i(A(b)) - p_i(b) \geq 0. \tag{10}$$

$$u_i^{\mathcal{T}} = r_i \geq 0 \tag{11}$$

4. No-deficit A matchmaking $\mathcal{M}$ is no-deficit if the total payments collected from the searcher $\mathcal{S}$ equal the total rebates paid to transaction creators of the winning transaction. That is, no money is lost from the process of matchmaking. The condition for no deficit is:

$$\sum_{i \in \mathcal{S}^*} p_i(b) = \sum_{i \in \mathcal{T}^*} r_i. \tag{12}$$

5. Fair redistribution A matchmaking $\mathcal{M}$ is fair to transaction creators if rebate to the transaction creator of each winning transaction $\mathcal{T}^*$ is such that (i) $\sum_{i \in \mathcal{T}^*} r_i = R$, where R is the revenue generated from searchers, (ii) $\forall i, j$ similar MEV transactions generating same value, $r_i = r_j$, and (iii) $r_i = 0$ for all transactions i that do not create any MEV.

A.2 Winner Determination with Additive Searchers

B Proving Uniqueness of Marginal Contributions

Theorem 3. $\forall (a_0, \ldots, a_{n-1}) \in \{-1, 0, 1\}^n$, the summation $s = \sum_{i=0}^{i=n-1} 3^i * a_i$ is unique.

Algorithm 3 SPA with VCG Payments

1: **Input:** Bids $b_{s_1}, b_{s_2}, \ldots, b_{s_m}$
2: Initialize $p_{s_i} = 0$ for each searcher s_i
3: **for** each transaction $t_j \in T$ **do**
4:    Find $b_{s_i}[t_j]$ of each searcher s_i.
5:    Let $s_i^* = \arg\max_{s_i} b_{s_i}[t_j]$ {Identify the participant with the highest bid}
6:    Let $b_{s_{\text{second}}}[t_j] = \max_{s_i \neq s_i^*} b_{s_i}[t_j]$ {Find the second-highest bid}
7:    **Payments:**
8:    **for** each searcher s_i **do**
9:       **if** $s_i = s_i^*$ **then**
10:          $p_{s_i} = p_{s_i} + b_{s_{\text{second}}}[t_j]$ {Winner pays the second-highest bid}
11:       **else**
12:          $p_{s_i} = p_{s_i} + 0$ {Non-winners pay nothing}
13:       **end if**
14:    **end for**
15: **end for**
16: **Output:** Winner s_i^* and payments $p_{s_1}, p_{s_2}, \ldots, p_{s_n}$

Proof. Proof by induction:
Base case: $n = 1$

For $a_0 \in \{-1, 0, 1\}$, the summation s can take value either $-1, 0$ or 1. Thus, all three possible summations for $n = 1$ are unique.
Inductive step: Assume the theorem to be true for $n = k$.

The minimum summation possible for $(a_0, \ldots, a_{k-1})$ is when all $a_i = -1$.

$$s_{\min} = -1 \times \frac{3^k - 1}{3 - 1} = -\frac{3^k - 1}{2}$$

. The maximum summation possible for $(a_0, \ldots, a_{k-1})$ is when all $a_i = 1$.

$$s_{\max} = 1 \times \frac{3^k - 1}{3 - 1} = \frac{3^k - 1}{2}$$

For $n = k + 1$, a_{k+1} can take values either $-1, 0$ or 1.

- $a_{k+1} = -1$: $s_{\min}^0 = -\frac{3^{k+1} - 1}{2}$ and $s_{\max}^0 = -\frac{3^k + 1}{2}$.

- $a_{k+1} = 0$: $s_{\min}^1 = -\frac{3^k - 1}{2}$ and $s_{\max}^1 = \frac{3^k - 1}{2}$

- $a_{k+1} = 1$: $s_{\min}^2 = \frac{3^k + 1}{2}$ and $s_{\max}^2 = \frac{3^k - 1}{2}$

As $s_{\max}^0 < s_{\min}^1$, $s_{\max}^0 < s_{\min}^2$ and $s_{\max}^1 < s_{\min}^2$, neither ranges of values overlap. Thus, if all possible summations for $n = k$ are unique, then the summations for $n = k + 1$ are also unique.
By the principle of mathematical induction, the summations $s = \sum_{i=0}^{i=n-1} 3^i * a_i$ are unique. $\qquad \square$

C Empirical Analysis

Figure 4 demonstrates the relationship between the number of unique values and the number of transactions, n. The observed growth rate of the number of unique values closely follows the theoretical prediction of $\Omega(2^{\sqrt{n}})$. This validates our theory that the number of unique values scales asymptotically as $\Omega(2^{\sqrt{n}})$ with respect to n, confirming the expected behavior.
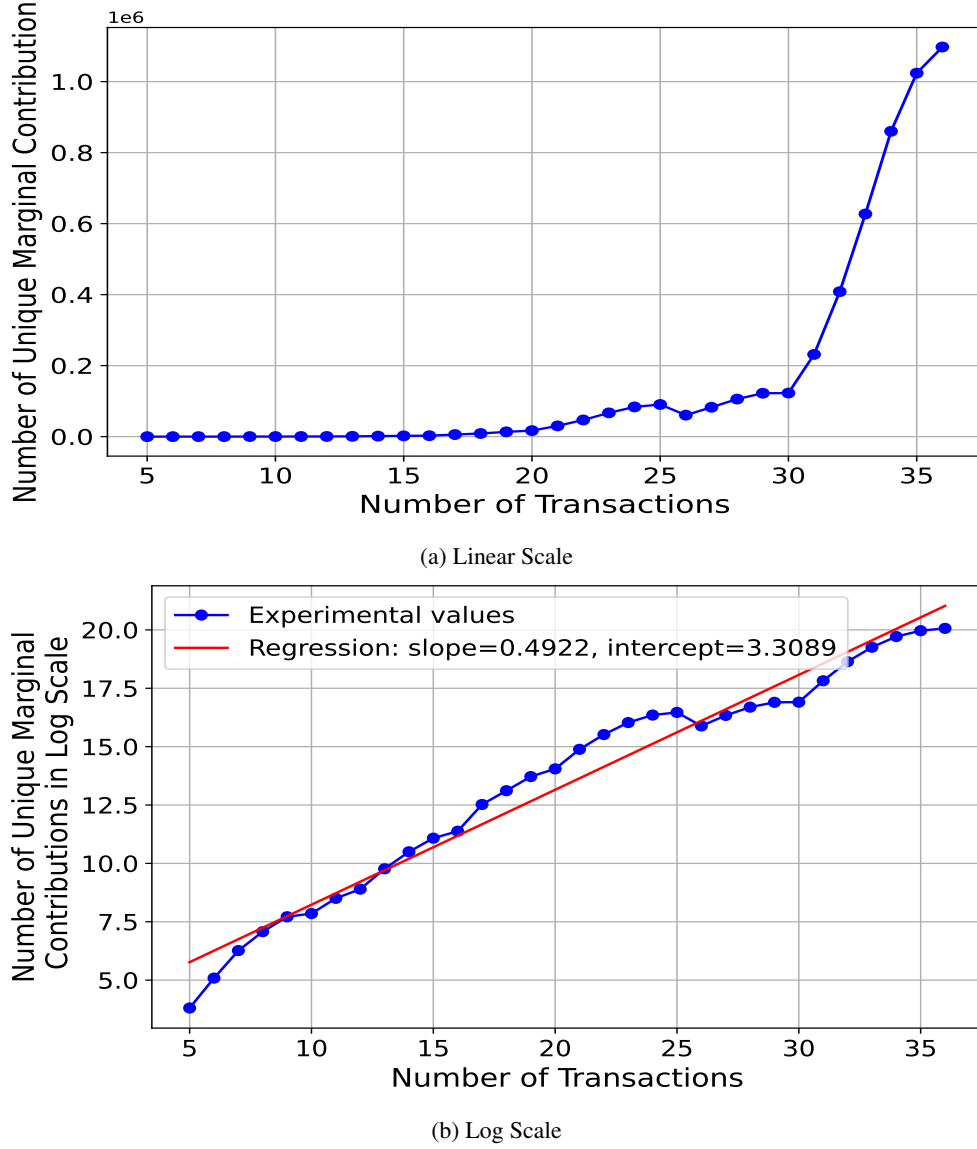
(a) Linear Scale

(b) Log Scale

Figure 4: Variation of Unique Marginal Contributions

D   Unianimity Games

A unanimity game is a fundamental concept in cooperative game theory, characterized by a coalition structure in which a specific subset of players, called a winning coalition, must act unanimously for any payoff to be generated. The game's value depends on whether a coalition contains the required subset.

Let N be a finite set of players, and let $S \subseteq N$ be a coalition (a subset of players). A unanimity game is represented by a characteristic function $v : 2^N \to \mathbb{R}$ defined as:

$$v(T) = \begin{cases} 1, & \text{if } S \subseteq T, \\ 0, & \text{otherwise.} \end{cases}$$

where S is the winning coalition, i.e., the minimal subset of players required to generate a value. T is any coalition under consideration. $v(T)$ gives the value of the coalition T. It is 1 if T contains all players in S, and 0 otherwise.

The Shapley value of `RST-Game` can derived from unanimity games in the following way. Let $U_S = (\mathcal{T}, \omega_S)$ be unanimity game defined on set of transactions $\mathcal{T}$ such that

$$\forall T \subseteq \mathcal{T}, \omega_S(T) = \begin{cases} 1 & S \subseteq T \\ 0 & \text{Otherwise} \end{cases} \tag{13}$$

Theorem 4. *$\forall T \subseteq \mathcal{T}$, the value function can be uniquely expressed in terms of unanimity functions in B_N with Harsanyi dividends as the coefficients*

$$\nu(T) = \sum_{S \in 2^{\mathcal{T}} \setminus \phi} \Delta_{\nu,S} \omega_S(T) \tag{14}$$

Proof. Let $E = 2^{\mathcal{T}} \setminus \phi$ i.e., $E = \{T_1, \ldots, T_{2^{|\mathcal{T}|}-1}\}$

Let Λ be the matrix formed using unanimity functions $\Lambda_{(i,j)} = \omega_{T_i}(T_j) \forall i, j \in \{0, \ldots, 2^{|\mathcal{T}|} - 1\}$

ω	$\mathbf{T_1}$	$\mathbf{T_2}$	$\mathbf{T_3}$	$\mathbf{T_4}$	$\cdots$	$\cdots$	$\mathbf{T_{2^{|\mathcal{T}|}-1}}$
ω_{T_1}	1	0	0	1	$\cdots$	$\cdots$	1
ω_{T_2}	0	1	0	1	$\cdots$	$\cdots$	1
ω_{T_3}	0	0	1	0	$\cdots$	$\cdots$	1
ω_{T_4}	0	0	0	1	$\cdots$	$\cdots$	1
ω_{T_5}	0	0	0	0	$\cdots$	$\cdots$	1
ω_{T_6}	0	0	0	0	1	$\cdots$	1
ω_{T_7}	0	0	0	0	0	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\omega_{T_{2^{|\mathcal{T}|}-1}}$	0	0	0	0	0	0	1

Assume there is a linear combination of unanimity functions that equals the zero function:

$$\sum_{S \in E} b_S \omega_S(T) = 0, \quad \forall T \in E$$

For this to hold, b_S must be zero for all $S \subseteq \mathcal{T}$. The unanimity function $\omega_S(T)$ is nonzero (equal to 1) if and only if $S \subseteq T$. This means $\omega_S(T)$ activates only those terms where $S \subseteq T$. If $b_S \neq 0$ for some $S \subseteq \mathcal{T}$, then $\sum_{S \subseteq \mathcal{T}} b_S \omega_S(T) \neq 0$ for some T. This contradicts the assumption that the sum equals 0 for all T. Thus, $b_S = 0$ for all S. This proves $\{\omega_S : S \in E\}$ are linearly independent.

Further, consider the following equations:

$$\nu(T_1) = \sum_{S \in E} b_S \omega_S(T_1)$$

$$\nu(T_2) = \sum_{S \in E} b_S \omega_S(T_2)$$

$$\nu(T_3) = \sum_{S \in E} b_S \omega_S(T_3)$$

$$\vdots$$

$$\nu(T_{2^{|\mathcal{T}|}-1}) = \sum_{S \in E} b_S \omega_S(T_{2^{|\mathcal{T}|}-1})$$

From the Λ, it can be observed that there are $2^{|\mathcal{T}|} - 1$ independent equations and $2^{|\mathcal{T}|} - 1$ variables, hence there exists unique solution $\{b_T : T \subseteq \mathcal{T}\}$.

Hence, $B_{\mathcal{T}} = \{\omega_T : T \subseteq \mathcal{T} \setminus \phi\}$ forms the basis for the characteristic function ν. These b_S are nothing but Harsanyi dividends represented as $\Delta_{\nu,S}$.

$$\nu(T) = \sum_{S \in 2^{\mathcal{T}} \setminus \phi} \Delta_{\nu,S} \omega_S(T)$$

$\square$

Theorem 5. *The Shapley value of t_j in the unanimity game $(\mathcal{T}, \omega_T)$ is:*

$$\varphi_{t_j}(\omega_T) = \begin{cases} \frac{1}{|T|}, & \text{if } t_j \in T, \\ 0, & \text{if } t_j \notin T. \end{cases}$$

Proof.

$$\Delta \omega_T(C)(t_j) = \begin{cases} 1, & T \setminus \{t_j\} \subseteq C, \\ 0, & T \setminus \{t_j\} \nsubseteq C. \end{cases}$$

$$\implies \forall t_j \notin S, \quad \varphi_{t_j}(\omega_T) = 0.$$

$$\omega_T(\mathcal{T}) = 1.$$

$$\varphi_{t_j}(\omega_T) = \frac{1}{N!} \sum_{C \subseteq \mathcal{N}_i} |C|!(N - |C| - 1)!\big(\omega_T(C \cup \{t_j\}) - \omega_T(C)\big) \tag{15}$$

From symmetry, each transaction in S receives an equal share of $\nu(\mathcal{T})$:

$$\implies \forall i \in S, \quad \varphi_{t_j}(\omega_T) = \frac{1}{|T|}.$$

$\square$

Theorem 6. *Any characterisitic function $\nu : 2^{\mathcal{T}} \setminus \{\emptyset\} \to \mathbb{R}_+$, the Shapley value can be expressed in terms of the Harsanyi dividends as:*

$$\varphi_{t_j}(\nu) = \sum_{T \subseteq 2^{\mathcal{T}} \setminus \{\emptyset\}, t_j \in T} \frac{\Delta_{\nu,T}}{|T|}.$$

Proof. Let $N_S = |C|! \, (|\mathcal{T}| - |C| - 1)!$

$$\varphi_{t_j}(\nu) = \frac{1}{|\mathcal{T}|!} \sum_{C \subseteq \mathcal{T} \setminus \{t_j\}} N_C \{\nu(C \cup \{t_j\}) - \nu(C)\}.$$

From Theorem $4, 5$, we have

$$\nu(C) = \sum_{T \subseteq 2^{\mathcal{T}} \setminus \{\emptyset\}} \Delta_{\nu,T} \omega_T(C) \text{ and}$$

$$\varphi_{t_j}(\omega_T) = \frac{1}{|T|} \quad \text{or } 0.$$

$$\varphi_{t_j}(\nu) = \frac{1}{|\mathcal{T}|!} \sum_{C \subseteq \mathcal{T} \setminus \{t_j\}} N_C \{\nu(C \cup \{t_j\}) - \nu(C)\}$$

$$= \frac{1}{|\mathcal{T}|!} \sum_{C \subseteq \mathcal{T} \setminus \{t_j\}} N_C \left(\sum_{T \subseteq 2^{\mathcal{T}} \setminus \emptyset} \Delta_{\nu,T} \omega_T(C \cup \{t_j\}) - \right.$$

$$\left. \sum_{T \subseteq 2^{\mathcal{T}} \setminus \emptyset} \Delta_{\nu,T} \omega_T(C) \right)$$

$$= \frac{1}{|\mathcal{T}|!} \sum_{C \subseteq \mathcal{T} \setminus \{t_j\}} \sum_{T \subseteq 2^{\mathcal{T}} \setminus \emptyset} N_C \Delta_{\nu,T} \big(\omega_T(C \cup \{t_j\}) - \omega_S(C) \big)$$

$$= \frac{1}{|\mathcal{T}|!} \sum_{C \subseteq \mathcal{T} \setminus \{t_j\}} \sum_{T \subseteq 2^{\mathcal{T}} \setminus \emptyset, t_j \in T} N_C \Delta_{\nu,T} \big(\omega_T(C \cup \{t_j\}) - \omega_T(C) \big)$$

$$= \frac{1}{|\mathcal{T}|!} \sum_{T \subseteq 2^{\mathcal{T}} \setminus \emptyset, i \in T} \sum_{T \subseteq \mathcal{T} \setminus \{t_j\}} N_C \Delta_{\nu,T} \big(\omega_T(C \cup \{i\}) - \omega_T(C) \big)$$

$$= \frac{1}{|\mathcal{T}|!} \sum_{T \subseteq 2^{\mathcal{T}} \setminus \emptyset, t_j \in T} \Delta_{\nu,T} \sum_{C \subseteq \mathcal{T} \setminus \{t_j\}} N_C \big(\omega_T(C \cup \{i\}) - \omega_T(C) \big)$$

$$= \sum_{T \subseteq 2^{\mathcal{T}} \setminus \emptyset, t_j \in T} \Delta_{\nu,T} \left(\frac{1}{|\mathcal{T}|!} \sum_{C \subseteq \mathcal{T} \setminus t_j} N_C \big(\omega_T(C \cup \{t_j\}) - \omega_T(C) \big) \right)$$

$$= \sum_{T \subseteq 2^{\mathcal{T}} \setminus \emptyset, t_j \in T} \Delta_{\nu,T} \varphi_{t_j}(\omega_T)$$

$$= \sum_{T \subseteq 2^{\mathcal{T}} \setminus \phi, t_j \in T} \frac{\Delta_{\nu,T}}{|T|}$$

$\square$