The Cost of MEV

Quantifying Economic (un)Fairness in the Decentralized World

Guillermo Angeris [1] **Tarun Chitra** [2] Theo Diamandis [3]
Kshitij Kulkarni [4]

[1]Bain Capital Crypto

[2]Gauntlet

[3]MIT

[2]UC Berkeley

SBC MEV Workshop
August 31, 2023

Outline

Can you really define MEV?

Fairness

Smooth Functions

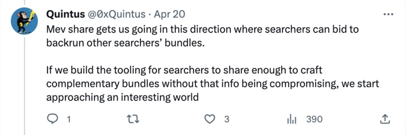
Spectral Analysis

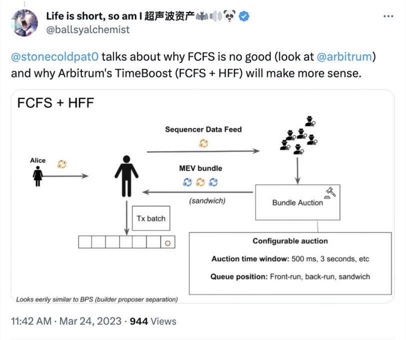
Conclusion

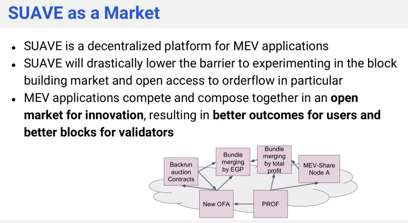
References

The problem

Is it possible to compare the economic equilibria of claims for things like fair ordering, SUAVE, timeboost, etc.?







Without formalism, here's what these claims sound like

My definition is just MEV

Ok, so what do we really want?

- Dynamic ordering mechanisms (Timeboost, SUAVE, Anoma) restrict orderings of n transactions to permutations $A \subset S_n$
- Given a payment f to validators for enforcing the restriction A, how 'fair' is the choice of A vs. another set $B \subset S_n$?
  - Fairness: "The worst-case payoff isn't so different from the average-case payoff"

HAL R. VARIAN

Distributive Justice,
Welfare Economics,
and the Theory of Fairness

What is MEV?

- “MEV is any excess value that a validator can extract by adding, removing, or reordering transactions”

What is MEV?

- "MEV is any excess value that a validator can extract by adding, removing, or reordering transactions"

What is MEV?

- "MEV is any excess value that a validator can extract by adding, removing, or reordering transactions"
- To define MEV we need:
  - Set of possible transactions, $\mathcal{T}$

What is MEV?

- "MEV is any excess value that a validator can extract by adding, removing, or reordering transactions"

- To define MEV we need:
  - Set of possible transactions, $\mathcal{T}$
  - Measure of Value, $f(T, \pi) \in \mathbf{R}$
    - $T \subset \mathcal{T}$: Set of transactions
    - $\pi \in S_n$: Permutation representing an ordering of T
    - Intuition: Payoff to validator for including T with ordering π

What is MEV?

- "MEV is any excess value that a validator can extract by adding, removing, or reordering transactions"
- To define MEV we need:
  - Set of possible transactions, $\mathcal{T}$
  - Measure of Value, $f(T, \pi) \in \mathbf{R}$
    - $T \subset \mathcal{T}$: Set of transactions
    - $\pi \in S_n$: Permutation representing an ordering of T
    - Intuition: Payoff to validator for including T with ordering π
  - Changes to value from addition, removal (censorship) or reordering of transactions
    - Bound on $\max_{S \subseteq T, \pi'} |f(T, \pi) - f(S, \pi')|$
    - Maximum bounds the notion of 'excess'

What are $\mathcal{T}$ and f?

- Isn't $\mathcal{T}$ way too large?
  - Yes: set of all transactions is too large to analyze combinatorially
  - **But**: Can restrict to transactions of a particular application
    - CFMM:
      $\mathcal{T} = \{\mathrm{Trade}(\Delta), \mathrm{ChangeLiquidity}(R) : \Delta, R \in \mathbf{R}^n\}$
    - Lending:
      $\mathcal{T} = \{\mathrm{Supply}(R), \mathrm{Borrow}(R), \mathrm{Liquidate}(R) : R \in \mathbf{R}_+\}$
- How should one think of f?
  - Take $S = \{t_1, \ldots, t_n\} \subset \mathcal{T}$, $\pi \in S_n$
  - Simulate contract with transactions $t_{\pi(1)}, \ldots, t_{\pi(n)}$ (in order)
  - Measure payoff $f(T, \pi)$

Why is it hard to quantify MEV?

- What is the domain of f?
  - Intuition: Any $S \subset \mathcal{T}$ and permutation π on $|S|$ elements

Why is it hard to quantify MEV?

- What is the domain of f?
  - Intuition: Any $S \subset \mathcal{T}$ and permutation π on $|S|$ elements
  - Formal: $\mathbf{dom}\, f = \bigcup_{k=0}^{|\mathcal{T}|} \binom{\mathcal{T}}{k} \times S_k$

Why is it hard to quantify MEV?

- What is the domain of f?
  - Intuition: Any $S \subset \mathcal{T}$ and permutation π on $|S|$ elements
  - Formal: $\mathbf{dom}\, f = \bigcup_{k=0}^{|\mathcal{T}|} \binom{\mathcal{T}}{k} \times S_k$
    1. $\binom{\mathcal{T}}{k} = \{T \subset \mathcal{T} : |T| = k\}$
    2. S_k: Symmetric group on k elements
       (*i.e.* set of $k!$ permutations on k elements)

Why is it hard to quantify MEV?

- What is the domain of f?
  - Intuition: Any $S \subset \mathcal{T}$ and permutation π on $|S|$ elements
  - Formal: $\mathbf{dom}\, f = \bigcup_{k=0}^{|\mathcal{T}|} \binom{\mathcal{T}}{k} \times S_k$
    1. $\binom{\mathcal{T}}{k} = \{T \subset \mathcal{T} : |T| = k\}$
    2. S_k: Symmetric group on k elements
       (*i.e.* set of $k!$ permutations on k elements)
- How big is the domain of f?
  - $|\,\mathbf{dom}\, f|$ controls ease of estimating 'worst-case' MEV to the user ($\max f$) vs. 'average-case' ($\mathbf{E}[f]$)

$$|\,\mathbf{dom}\, f| = \sum_{i=1}^{|\mathcal{T}|} \binom{\mathcal{T}}{k} \cdot k! = \sum_{i=1}^{|\mathcal{T}|} \frac{|\mathcal{T}|!}{(|\mathcal{T}| - k)!} \leq e|\mathcal{T}|!$$

- **tl;dr**: The space of payoffs is *very large*, $f \in \mathbf{R}_{+}^{\Theta(|\mathcal{T}|!)}$

Outline

Can you really define MEV?

Fairness

Smooth Functions

Spectral Analysis

Conclusion

References

What does it mean for a payoff to be fair?

- Intuition: Worst-case payoff (for users) is not “too” different from a random payoff

What does it mean for a payoff to be fair?

- Intuition: Worst-case payoff (for users) is not "too" different from a random payoff
- Worst-Case Payoff: $\max_{(S,\pi)\in \mathbf{dom}\, f} f(S,\pi)$

What does it mean for a payoff to be fair?

- Intuition: Worst-case payoff (for users) is not "too" different from a random payoff
- Worst-Case Payoff: $\max_{(S,\pi)\in \mathbf{dom}\, f} f(S,\pi)$
- Average-Case Payoff: $\mathbf{E}[f] = \frac{1}{|\mathbf{dom}\, f|} \sum_{x \in \mathbf{dom}\, f} f(x)$

What does it mean for a payoff to be fair?

- Intuition: Worst-case payoff (for users) is not "too" different from a random payoff
- Worst-Case Payoff: $\max_{(S,\pi)\in\mathbf{dom}\, f} f(S,\pi)$
- Average-Case Payoff: $\mathbf{E}[f] = \frac{1}{|\mathbf{dom}\, f|}\sum_{x\in\mathbf{dom}\, f} f(x)$
- Define the **Cost of Fairness**:

$$C(f) = \max_{(S,\pi)\in\mathbf{dom}\, f} f(S,\pi) - \mathop{\mathbf{E}}_{S,\pi}[f(S,\pi)]$$

- A payoff f is fair if $C(f)$ is 'small'
  - Will need bounds, examples to understand what 'small' is

$C(f)$ for reordering

- Remainder of the talk: fix $S \subset \mathcal{T}$ with $|S| = n$ and look at

$$C(f, S) = \max_{\pi \in S_n} f(S, \pi) - \mathop{\mathbf{E}}_{\pi \in S_n}[f(S, \pi)]$$

  - Quantifies fairness for reordering a fixed set
  - Will drop S dependence — can consider $C(f) = \max_S C(f, S)$

$C(f)$ for reordering

- Remainder of the talk: fix $S \subset \mathcal{T}$ with $|S| = n$ and look at

$$C(f, S) = \max_{\pi \in S_n} f(S, \pi) - \mathop{\mathbf{E}}_{\pi \in S_n}[f(S, \pi)]$$

  - Quantifies fairness for reordering a fixed set
  - Will drop S dependence — can consider $C(f) = \max_S C(f, S)$

- Assumption: there exist no non-trivial invariant subsets of S
  - Formal: $\nexists A \subset S$ s.t $f(A, \pi) = f(A, \pi')\ \forall \pi, \pi' \in S_{|A|}$
  - Assumption can be removed with the orbit-stabilizer theorem

Upper Bound: Sharpening our intution

- Consider the simple bound

$$\mathop{\mathbf{E}}_{\pi \in S_n}[f(\pi)] = \frac{1}{n!} \sum_{\pi \in S_n} f(\pi) \geq \frac{1}{n!} \max_{\pi \in S_n} f(\pi)$$

Upper Bound: Sharpening our intution

- Consider the simple bound

$$\mathop{\mathbf{E}}_{\pi \in S_n}[f(\pi)] = \frac{1}{n!} \sum_{\pi \in S_n} f(\pi) \geq \frac{1}{n!} \max_{\pi \in S_n} f(\pi)$$

- This implies an upper bound on $C(f)$

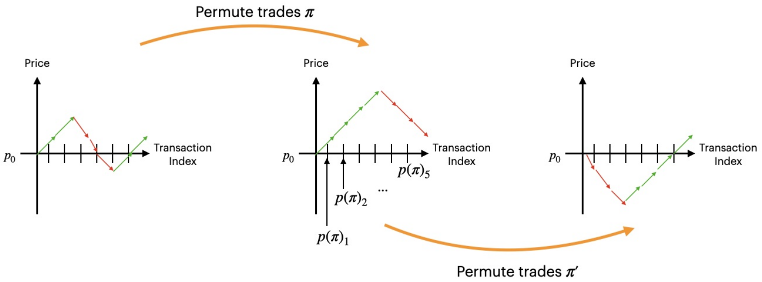
$$C(f) = \max_{\pi \in S_n} f(\pi) - \mathop{\mathbf{E}}_{\pi \in S_n}[f(\pi)] \leq \left(1 - \frac{1}{n!}\right) \left(\max_{\pi \in S_n} f(\pi)\right)$$

- Achieve upper bound via the payoff $f(\pi) = \mathbf{1}_{\{\pi'\}}$ for fixed $\pi' \in S_n$ where $\mathbf{1}_A$ for $A \subset S_n$ is

$$\mathbf{1}_A(\pi) = \begin{cases} 1 & \pi \in A \\ 0 & \pi \notin A \end{cases}$$

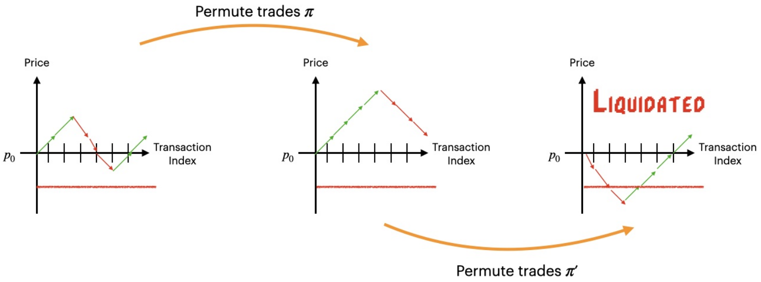
Worst Case Functions: Liquidations

- Converse is true: All f with $C(f) = \left(1 - \frac{1}{n!}\right) \max_\pi f(\pi)$ is an indicator function supported on 1 element
- This payoff can be viewed as a DeFi liquidation:



Worst Case Functions: Liquidations

- Converse is true: All f with $C(f) = \left(1 - \frac{1}{n!}\right) \max_\pi f(\pi)$ is an indicator function supported on 1 element
- This payoff can be viewed as a DeFi liquidation:



Properties of $C(f)$

- Basic Axioms:
  - *Positivity*: $C(f) \geq 0$ which is achieved by $f(\pi) = c$ for $c \geq 0$
  - *Homogeneity*: $C(\alpha f) = \alpha C(f)$
  - *Translation Invariance*: For $\alpha \geq 0$, $C(f + \alpha) = C(f)$

Properties of $C(f)$

- Basic Axioms:
  - *Positivity*: $C(f) \geq 0$ which is achieved by $f(\pi) = c$ for $c \geq 0$
  - *Homogeneity*: $C(\alpha f) = \alpha C(f)$
  - *Translation Invariance*: For $\alpha \geq 0$, $C(f + \alpha) = C(f)$

- Homogeneity and Translation invariance imply that we only need to consider payoffs $f : S_n \to [0, 1]$ as

$$\tilde{f}(\pi) = \frac{f(\pi) - \min_{\pi \in S_n} f(\pi)}{\max_{\pi \in S_n} f(\pi) - \min_{\pi \in S_n} f(\pi)}$$

  satisfies

$$C(f) = \left(\max_{\pi \in S_n} f(\pi) - \min_{\pi \in S_n} f(\pi) \right) C(\tilde{f})$$

Properties of $C(f)$

- Basic Axioms:
  - *Positivity*: $C(f) \geq 0$ which is achieved by $f(\pi) = c$ for $c \geq 0$
  - *Homogeneity*: $C(\alpha f) = \alpha C(f)$
  - *Translation Invariance*: For $\alpha \geq 0$, $C(f + \alpha) = C(f)$

- Homogeneity and Translation invariance imply that we only need to consider payoffs $f : S_n \to [0, 1]$ as

$$\tilde{f}(\pi) = \frac{f(\pi) - \min_{\pi \in S_n} f(\pi)}{\max_{\pi \in S_n} f(\pi) - \min_{\pi \in S_n} f(\pi)}$$

satisfies

$$C(f) = \left(\max_{\pi \in S_n} f(\pi) - \min_{\pi \in S_n} f(\pi)\right) C(\tilde{f})$$

- Restricting to normalized function $f : S_n \to [0, 1]$ yields

$$0 \leq C(\tilde{f}) \leq 1 - \frac{1}{n!}$$

What does it mean to be small?

- A tale of two extremes:
  - 'Sharp' indicator function $\mathbf{1}_{\{\pi\}}$ maximizes the bound on $C(f)$
  - 'Flat' constant function minimizes $C(f)$
- Utopia: There is a simple threshold for smallness, like $C(\tilde{f}) = O(2^{-|\mathcal{T}|})$ or $C(\tilde{f}) = O\left(\frac{1}{|\mathcal{T}|!}\right)$
- Reality: Depends on fine structure; 'smoothness' of f
- We will quantify smoothness in two ways:
  1. Global Smoothness: Metric or Lipschitz
  2. Local Smoothness: Fourier Transform over S_n

Aside: Why use an additive measure of fairness?

- 'Fairness' in algorithmic game theory is often measured multiplicatively, *e.g.* Price of Anarchy or a competitve ratio:

$$PoA(f) = \frac{\max_{x \in \mathbf{dom}\, f} f(x)}{\min_{x \in \mathbf{dom}\, f} f(x)} \qquad CR(f) = \frac{\max_{x \in \mathbf{dom}\, f} f(x)}{\mathbf{E}_{x \sim \mathbf{dom}\, f}[f(x)]}$$

Aside: Why use an additive measure of fairness?

- 'Fairness' in algorithmic game theory is often measured multiplicatively, *e.g.* Price of Anarchy or a competitve ratio:

$$PoA(f) = \frac{\max_{x \in \mathbf{dom}\, f} f(x)}{\min_{x \in \mathbf{dom}\, f} f(x)} \qquad CR(f) = \frac{\max_{x \in \mathbf{dom}\, f} f(x)}{\mathbf{E}_{x \sim \mathbf{dom}\, f}[f(x)]}$$

- However, these measures are not 'smooth' in that small changes to a function that make $PoA(f), CR(f)$ grow arbitrarily large
  - *e.g.* $PoA(\mathbf{1}_{\{\pi\}}) = \infty$ and $CR(\mathbf{1}_{\{\pi\}}) = n!$

Aside: Why use an additive measure of fairness?

- 'Fairness' in algorithmic game theory is often measured multiplicatively, *e.g.* Price of Anarchy or a competitve ratio:

$$PoA(f) = \frac{\max_{x \in \mathbf{dom}\, f} f(x)}{\min_{x \in \mathbf{dom}\, f} f(x)} \qquad CR(f) = \frac{\max_{x \in \mathbf{dom}\, f} f(x)}{\mathbf{E}_{x \sim \mathbf{dom}\, f}[f(x)]}$$

- However, these measures are not 'smooth' in that small changes to a function that make $PoA(f), CR(f)$ grow arbitrarily large
  - *e.g.* $PoA(\mathbf{1}_{\{\pi\}}) = \infty$ and $CR(\mathbf{1}_{\{\pi\}}) = n!$

- Additive is better as we need to compare 'smooth' MEV (*i.e.* sandwich attacks) to 'sharp' MEV (*i.e.* liquidations)

Outline

Can you really define MEV?

Fairness

Smooth Functions

Spectral Analysis

Conclusion

References

Metric Smoothness

- *Permutation Independent Metrics:* Given $S \subset \mathcal{T}$,$d : S \times S \to \mathbf{R}_+$ satisfying

$$\forall x, y \in S \quad d(\pi(x), \pi(y)) = d(x, y)$$

e.g. L^p-norms induce permutation independent metrics

- $f : S \to \mathbf{R}_+$ is L-smooth for a P. I. metric if for all $x, y \in S$,

$$|f(x) - f(y)| \leq Ld(x, y)$$

- Note:This is *global* notion of smoothness
  - *e.g.* L has hold for all pairs $x, y \in S$

- **Fact**: f is L-smooth $\longrightarrow C(f)$ is $2L$-smooth

Example: CFMM Frontrunning

- **Actions,** $\mathcal{T}$: Trades Δ_i, δ_i from the user, validator, resp., of maximum size M[1]
- **Metric,** d: $\sum_{i=1}^{n} \max\{|\Delta_i|, |\delta_i|, |\Delta_i - \delta_i|\}$
- **Payoff,** f: $f(\delta) = G(\Delta_1 + \cdots + \Delta_k + \delta) - G(\Delta_1 + \cdots + \Delta_k)$ [2]
- **Bound on** $C(f)$:

$$C(f) \leq 8G'(0)M$$

[1] The are some constraints on Δ, δ, see the paper

[2] G is a measure of slippage of a CFMM (*i.e. forward exchange function*)

Example: CFMM Sandwich Attacks

- **Actions,** $\mathcal{T}$: Triples of user trades Δ_i and front/backrun trades δ_i, γ_i of maximum size M
- **Metric,** d: $\max(\|\Delta\|_1, \|\delta + \gamma\|_1)$
- **Payoff,** f: $f(\delta, \gamma) = -(\delta + \gamma)$
- **Bound on** $C(f)$:

$$C(f) \leq M$$

Outline

Can you really define MEV?

Fairness

Smooth Functions

Spectral Analysis

Conclusion

References

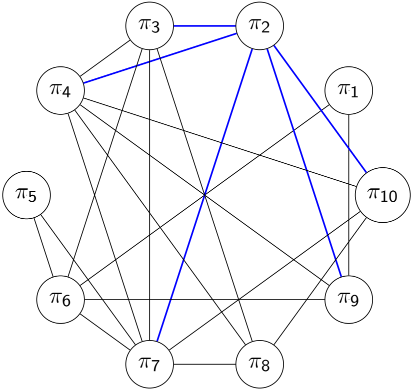
Localized smoothness

- **Problem:** Lipschitz smoothness is global, liquidations are not generically globally smooth
- Can we 'localize' smoothness (e.g. a bound dependent on the particular permutations involved)?

Localized smoothness

- **Problem:** Lipschitz smoothness is global, liquidations are not generically globally smooth
- Can we 'localize' smoothness (e.g. a bound dependent on the particular permutations involved)?
- **Idea:** Represent the local structure as a graph, look at local bounds on how f changes in a neighborhood of a permutation

Permutation Graphs



- Bound $\max_\pi |f(\pi) - f(\pi_2)|$ by looking at behavior on neighbors
- Permutations with more neighbors can be 'less smooth'
- Independent cliques are separate ordering rules $A \subset S_n$

Spectral Cost of MEV

- For a graph $G = (S_n, E)$, construct *spectral cost of MEV*

$$C_G(f) = f^T L f = \sum_{(\pi,\pi') \in E} (f(\pi) - f(\pi'))^2$$

  where L is the graph Laplacian

- Having bounds on $C_G(f)$ locally bounds $|f(\pi) - f(\pi')|$ if π, π' is an edge in a permutation graph

Spectral Cost of MEV

- For a graph $G = (S_n, E)$, construct *spectral cost of MEV*

$$C_G(f) = f^T L f = \sum_{(\pi,\pi')\in E} (f(\pi) - f(\pi'))^2$$

  where L is the graph Laplacian

- Having bounds on $C_G(f)$ locally bounds $|f(\pi) - f(\pi')|$ if π, π' is an edge in a permutation graph

- Properties
  - Translation invariant: $C_G(f + \alpha \mathbf{1}) = C_G(f)$
  - Homogeneous of degree-2: $C_G(\alpha f) = \alpha^2 C_G(f)$

Fourier Analysis on Graphs

- Bounds on $C_G(f) \iff$ bounds on eigenvalues $\lambda_1, \ldots \lambda_{n!}$ of L
- When $L = U^T \Sigma U$, the *graph Fourier transform* of f is $\hat{f} = Uf$
- How do we interpret $\hat{f}$?
  - $\hat{f}_1, \ldots, \hat{f}_{n!}$: Frequencies of $\hat{f}$
  - Function is 'locally' smooth if f_i is small for most i
- **Fact**: $C(f) = 0$ iff $\hat{f}_i = 0$ for all $i \geq 2$

Spectral Bounds

- One can bound $C(f)$ with $C_G(f)$:

$$\sqrt{\frac{C_G(f)}{\lambda_{n!}n!}} \leq C(f) \leq \sqrt{\frac{C_G(f)}{\lambda_2}}$$

- This means we can bound $C(f)$ using only linear algebra!
- Yes, you should be reminded of Cheeger's inequality!

How can you use spectral bounds in practice?

- SUAVE or Anoma: Restrict sets of orderings π to $A \subset S_n$
- This implicitly defines a graph G
  - Edge exists between π, π' if $\sigma \in A$ s.t. $\pi = \sigma \circ \pi'$
- Developer can compute $C_G(f)$, bounds provide explicit economic fairness guarantees
- Two main problems:
  1. Computing $C_G(f)$ is hard
  2. The bounds are too loose

Representation Theory and Uncertainty

- One can improve the bounds on $C(f)$ using representation theory ('Fourier analysis for non-abelian groups')

- Beyond the scope of this talk (but see Chitra 2023) but high-level idea:
  - RT lets one write $L = L_1 \oplus \cdots \oplus L_k$
  - Bound spectra of each L_i independently
  - Maximize over bounds for each L_i

- Uncertainty Principle of Wigderson, et. al:

$$\frac{\mathbf{E}[f]}{\max f} \geq \frac{\|\hat{f}\|_\infty}{\|\hat{f}\|_1}$$

  - Chitra 2023 uses this to get much sharper lower bound

Outline

Can you really define MEV?

Fairness

Smooth Functions

Spectral Analysis

Conclusion

References

Conclusions

- We formalized MEV in a combinatorial manner in terms of payoff functions
- Defined a notion of fairness for MEV and demonstate that spectral analysis can be used to bound the fairness
- Bounds can be improved and used to provide users with certificates of fairness when using things like SUAVE
- Demonstates that the combinatorial structure of MEV is closely related to Fourier analysis over the symmetric group

Paper

Outline

Can you really define MEV?

Fairness

Smooth Functions

Spectral Analysis

Conclusion

References

References

Chitra, Tarun (2023). "Towards a Theory of MEV II: Uncertainty". In.

Outline

Censorship

Can Fourier Analysis quantify the cost of censorship?

- Recall: We can write the domain of f as $T \times S_{|T|}$ for $T \subset \mathcal{T}$
- Fourier Transform of a boolean function $g : \{0,1\}^n \to \mathbf{R}$ is the multilinear polynomial

$$g(x) = \sum_{T \subset 2^{[n]}} \hat{g}(T) \prod_{i \in T} x_i$$

- We can view $\tilde{f}(T) = \max_{\pi \in S_{|T|}} f(T, \pi)$ as a Fourier transform of a boolean function
- Combine spectral methods over $\mathbf{Z}_2^n$ with those over S_n to get bounds

Why the bounds are likely to be looser than reordering

- For a boolean function g the maximum value of $\hat{g}$ will be bounded by

$$\max_{T \subset [n]} \max_{i \in [n] - T} |\hat{g}(T \cup \{i\}) - \hat{g}(T)|$$

- This is the *maximum influence* of a boolean random variable
- Kahn-Kalai-Linial: Maximum influence $= \Omega\left(\frac{\log n}{n}\right)$
- This means there are likely "large" influence transactions (e.g. oracle updates) that will bias the spectral measurements