The Complexity of Somewhat Approximation Resistant Predicates

Pratik Worah

Joint work with Subhash Khot and Madhur Tulsiani.

August 24, 2013

k-CSPs are everywhere

- k-CSP(f)s, for $f : \{0,1\}^k \rightarrow \{0,1\}$, are well studied in Theoretical Computer Science.

k-CSPs are everywhere

- k-CSP(f)s, for $f : \{0,1\}^k \to \{0,1\}$, are well studied in Theoretical Computer Science.
- Example: $f = \vee$ or $f = \oplus$.

k-CSPs are everywhere

- k-CSP(f)s, for $f : \{0,1\}^k \to \{0,1\}$, are well studied in Theoretical Computer Science.
- Example: $f = \vee$ or $f = \oplus$.
- For example k-CNF and k-XOR are at the intersection of many algorithmic and lower bound results.
  - Classical NP-Completeness reductions Eg. [Karp].
  - Dichotomy Theorems Eg. [Schaefer].
  - PCP based conditional lowerbounds Eg. [Håstad].
  - Lowerbounds in weak proof systems Eg. [Grigoriev et al].
  - Approximation algorithms for MAX-k-CSPs Eg. [Hast].

The list of references above runs long.

Our Problem Space

- The problem of finding an assignment which satisfies maximum fraction of constraints is an important one - **MAX**-k-**CSP**(f).

Our Problem Space

- The problem of finding an assignment which satisfies maximum fraction of constraints is an important one - **MAX**-k-**CSP**(f).
- A k-ary constraint f_i is *derived* from f by choosing tuples of k variables (or their negations) as inputs to f.

Our Problem Space

- The problem of finding an assignment which satisfies maximum fraction of constraints is an important one - **MAX**-k-**CSP**(f).
- A k-ary constraint f_i is *derived* from f by choosing tuples of k variables (or their negations) as inputs to f.
- Formally, given m k-ary constraints f_i, each derived from predicate f, on n variables $\{x_1, .., x_n\}$ we wish to find:

$$\max_{\alpha \in \{0,1\}^n} \frac{1}{m} \sum_{i=1}^{m} f_i(\alpha_{|f_i}).$$

A Trivial Algorithm

- Solving MAX-k-CSP(f) exactly is NP-Hard [Cook-Levin].

A Trivial Algorithm

- Solving MAX-k-CSP(f) exactly is NP-Hard [Cook-Levin].
- *What if we are willing to settle for a polynomial time algorithm which outputs an approximately optimal solution always within a small constant factor away from the optimum?*

A Trivial Algorithm

- Solving MAX-k-CSP(f) exactly is NP-Hard [Cook-Levin].
- *What if we are willing to settle for a polynomial time algorithm which outputs an approximately optimal solution always within a small constant factor away from the optimum?*
- Let $\rho(f)$ denote the density of accepting assignments of predicate f i.e. $\rho(f) := \frac{|f^{-1}(1)|}{2^k}$.

A Trivial Algorithm

- Solving MAX-k-CSP(f) exactly is NP-Hard [Cook-Levin].
- *What if we are willing to settle for a polynomial time algorithm which outputs an approximately optimal solution always within a small constant factor away from the optimum?*
- Let $\rho(f)$ denote the density of accepting assignments of predicate f i.e. $\rho(f) := \frac{|f^{-1}(1)|}{2^k}$.
- Solution: Choose a uniform random assignment $\alpha \in \{0, 1\}^n$. It will satisfy $\rho(f)$ fraction of constraints in expectation.

Conditional Hardness

- *Can we do better than the above trivial algorithm?*

Conditional Hardness

- *Can we do better than the above trivial algorithm?*
- Beating the random assignment for MAX-k-CSP($\oplus$) is NP-Hard [Håstad] for $k \geq 3$.

Conditional Hardness

- *Can we do better than the above trivial algorithm?*
- Beating the random assignment for MAX-k-CSP($\oplus$) is NP-Hard [Håstad] for $k \geq 3$.
- For $k \geq 3$ and small enough $\varepsilon > 0$, it is NP-Hard to distinguish between a $\mathbf{1} - \varepsilon$ satisfiable instance of MAX-k-XOR and a $\mathbf{1}/\mathbf{2} + \varepsilon$ satisfiable instance of MAX-k-XOR.

Conditional Hardness

- *Can we do better than the above trivial algorithm?*
- Beating the random assignment for MAX-k-CSP($\oplus$) is NP-Hard [Håstad] for $k \geq 3$.
- For $k \geq 3$ and small enough $\varepsilon > 0$, it is NP-Hard to distinguish between a $\mathbf{1} - \varepsilon$ satisfiable instance of MAX-k-XOR and a $\mathbf{1/2} + \varepsilon$ satisfiable instance of MAX-k-XOR.
- A predicate f which is $\mathbf{1} - \varepsilon$ vs. $\rho(\mathbf{f}) - \varepsilon$ hard, in the above sense, is popularly known as **approximation resistant**.

More Conditional Hardness

- *What about predicates other than* $\oplus$*?*

More Conditional Hardness

- *What about predicates other than $\oplus$?*
- $f : \{0,1\}^k \rightarrow \{0,1\}$ is said to *support a probability distribution* $\mu : \{0,1\}^k \rightarrow \mathbb{R}$ if $\mu(x) > 0$ only when $x \in f^{-1}(1)$.

More Conditional Hardness

- *What about predicates other than $\oplus$?*
- $f : \{0,1\}^k \rightarrow \{0,1\}$ is said to *support a probability distribution* $\mu : \{0,1\}^k \rightarrow \mathbb{R}$ if $\mu(x) > 0$ only when $x \in f^{-1}(1)$.
- A **linear predicate** L corresponds to a set of assignments $L^{-1}(1)$ which form an affine subspace of $\mathbb{F}_2^k$.

More Conditional Hardness

- *What about predicates other than* $\oplus$*?*
- $f : \{0,1\}^k \rightarrow \{0,1\}$ is said to *support a probability distribution* $\mu : \{0,1\}^k \rightarrow \mathbb{R}$ if $\mu(x) > 0$ only when $x \in f^{-1}(1)$.
- A **linear predicate** L corresponds to a set of assignments $L^{-1}(1)$ which form an affine subspace of $\mathbb{F}_2^k$.
- k-XOR is a linear predicate.

More Conditional Hardness

- A well distributed linear predicate L is a linear predicate where the uniform distribution μ supported on the set $L^{-1}(1)$ is balanced and pairwise independent.

$$\forall i, j \in [k] \quad \mu(x_i = 1) = 1/2, \ \mu(x_i = 1, x_j = 1) = 1/4.$$

More Conditional Hardness

- A well distributed linear predicate L is a linear predicate where the uniform distribution μ supported on the set $L^{-1}(1)$ is balanced and pairwise independent.

$$\forall i, j \in [k] \quad \mu(x_i = 1) = 1/2,\ \mu(x_i = 1, x_j = 1) = 1/4.$$

- Easy to see k-XOR is a well distributed linear predicate.

More Conditional Hardness

- A <u>well distributed linear predicate</u> L is a linear predicate where the uniform distribution μ supported on the set $L^{-1}(1)$ is balanced and pairwise independent.

$$\forall i, j \in [k] \quad \mu(x_i = 1) = 1/2,\ \mu(x_i = 1, x_j = 1) = 1/4.$$

- Easy to see k-XOR is a well distributed linear predicate.
- For $k \geq 3$, $\varepsilon > 0$ and L a well distributed linear predicate then L is approximation resistant [Chan].

More Conditional Hardness

- A well distributed linear predicate L is a linear predicate where the uniform distribution μ supported on the set $L^{-1}(1)$ is balanced and pairwise independent.

$$\forall i, j \in [k] \quad \mu(x_i = 1) = 1/2, \; \mu(x_i = 1, x_j = 1) = 1/4.$$

- Easy to see k-XOR is a well distributed linear predicate.
- For $k \geq 3$, $\varepsilon > 0$ and L a well distributed linear predicate then L is approximation resistant [Chan].
- **Q1:** *Exactly which non-linear predicates are "hard to approximate", assuming $P \neq NP$?*

τ-Resistance

- For $\tau > \rho(f)$, f is said to be τ-**resistant** if for arbitrary small enough constant $\varepsilon > 0$, it is NP-Hard to distinguish instances where a $\tau - \varepsilon$ fraction of constraints can be simultaneously satisfied from those where at most $\rho(f) + \varepsilon$ fraction of the constraints can be simultaneously satisfied.

τ-Resistance

- For $\tau > \rho(f)$, f is said to be τ-**resistant** if for arbitrary small enough constant $\varepsilon > 0$, it is NP-Hard to distinguish instances where a $\tau - \varepsilon$ fraction of constraints can be simultaneously satisfied from those where at most $\rho(f) + \varepsilon$ fraction of the constraints can be simultaneously satisfied.
- Approximation Resistance $\equiv$ 1-resistance.

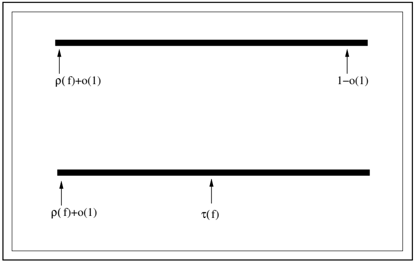
τ-Resistance

- For $\tau > \rho(f)$, f is said to be τ-**resistant** if for arbitrary small enough constant $\varepsilon > 0$, it is NP-Hard to distinguish instances where a $\tau - \varepsilon$ fraction of constraints can be simultaneously satisfied from those where at most $\rho(f) + \varepsilon$ fraction of the constraints can be simultaneously satisfied.
- Approximation Resistance $\equiv$ 1-resistance.
- We address a weak version of our original goal (Qn1).

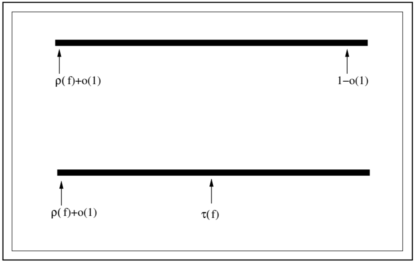
τ-Resistance

- For $\tau > \rho(f)$, f is said to be τ-**resistant** if for arbitrary small enough constant $\varepsilon > 0$, it is NP-Hard to distinguish instances where a $\tau - \varepsilon$ fraction of constraints can be simultaneously satisfied from those where at most $\rho(f) + \varepsilon$ fraction of the constraints can be simultaneously satisfied.
- Approximation Resistance $\equiv$ 1-resistance.
- We address a weak version of our original goal (Qn1).
- Goal: Given f, characterize the gap: $\tau(f) - \rho(f)$.

τ-Resistance

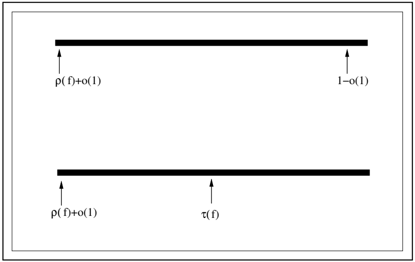


τ-Resistance



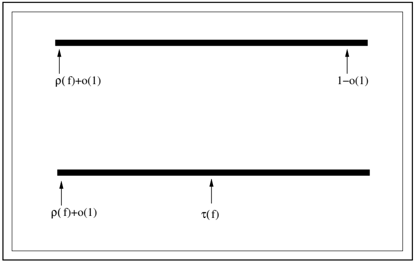
- f is said to be **somewhat approximation resistant** if there exists a constant $\tau > \rho(f)$ so that f is τ-resistant [Håstad].

τ-Resistance



- f is said to be **somewhat approximation resistant** if there exists a constant $\tau > \rho(f)$ so that f is τ-resistant [Håstad].
- τ-resistance is a more precise version of somewhat resistance.

τ-Resistance



- f is said to be **somewhat approximation resistant** if there exists a constant $\tau > \rho(f)$ so that f is τ-resistant [Håstad].
- τ-resistance is a more precise version of somewhat resistance.
- We characterize $\tau(f) - \rho(f)$ upto a factor of $O(k^5)$.

Somewhat Approximation Resistance

- Let $\mathcal{Q}$ be the set of k-ary boolean predicates having no Fourier mass at level 3 or above.

Somewhat Approximation Resistance

- Let $\mathcal{Q}$ be the set of k-ary boolean predicates having no Fourier mass at level 3 or above.
- Example: $f(\vec{x}) := \frac{1+(-1)^{x_1}+(-1)^{x_2}+(-1)^{x_1+x_2}}{4}$.

Somewhat Approximation Resistance

- Let $\mathcal{Q}$ be the set of k-ary boolean predicates having no Fourier mass at level 3 or above.
- Example: $f(\vec{x}) := \frac{1+(-1)^{x_1}+(-1)^{x_2}+(-1)^{x_1+x_2}}{4}$.
- If the normalized Hamming distance $\Delta(f, \mathcal{Q}) > 0$ i.e. $f \notin \mathcal{Q}$, then f is somewhat approximation resistant [Håstad].

Somewhat Approximation Resistance

- Let $\mathcal{Q}$ be the set of k-ary boolean predicates having no Fourier mass at level 3 or above.
- Example: $f(\vec{x}) := \frac{1+(-1)^{x_1}+(-1)^{x_2}+(-1)^{x_1+x_2}}{4}$.
- If the normalized Hamming distance $\Delta(f, \mathcal{Q}) > 0$ i.e. $f \notin \mathcal{Q}$, then f is somewhat approximation resistant [Håstad].
- But the value of τ in [Håstad] can be exponentially small in k.

Somewhat Approximation Resistance

- Let $\mathcal{Q}$ be the set of k-ary boolean predicates having no Fourier mass at level 3 or above.
- Example: $f(\vec{x}) := \frac{1+(-1)^{x_1}+(-1)^{x_2}+(-1)^{x_1+x_2}}{4}$.
- If the normalized Hamming distance $\Delta(f, \mathcal{Q}) > 0$ i.e. $f \notin \mathcal{Q}$, then f is somewhat approximation resistant [Håstad].
- But the value of τ in [Håstad] can be exponentially small in k.
- Conversely, if $\Delta(f, \mathcal{Q}) = 0$, then f depends on at most 4 variables [Håstad]. Moreover, f is not somewhat approximation resistant [Håstad].

Main Theorem

Assume $k \geq k_0$ and $f : \{0,1\}^k \to \{0,1\}$ be a predicate with $\Delta(f, \mathcal{Q}) > 0$.

1. If $\Delta(f, \mathcal{Q}) \geq 1/k^3$, then

$$\tau(f) \geq \rho(f) + \Omega(1/k^5).$$

   Else, $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$, and let $g \in \mathcal{Q}$ s.t. $\Delta(f, g) = \delta$.

2. If $\exists x \in \{0,1\}^k$ such that $f(x) = 1 \wedge g(x) = 0$ then

$$\tau(f) \geq \rho(f) + \Omega(1/k).$$

3. Else, g is monotonically above f. In this case,

$$\rho(f) + \Omega\left(\frac{\delta}{k^2}\right) \leq \tau(f) \leq \rho(f) + O(k^3\delta).$$

A Comparison with Previous Results

k-XOR [Håstad]	$\tau(f) \simeq 1$
Well distributed predicates [Chan]	$\tau(f) \simeq 1.$
$\Delta(f, \mathcal{Q}) > 0$ [Håstad]	$\tau(f) \geq \rho(f) + \frac{1}{2^{\Theta(k)}}.$
$\Delta(f, \mathcal{Q}) = 0$ [Håstad]	$\tau(f) \leq \rho(f) + \varepsilon \ (\forall \varepsilon > 0).$
$\Delta(f, \mathcal{Q}) \geq 1/k^3$ [KTW]	$\tau(f) \geq \rho(f) + \Omega(1/k^5).$
$\Delta(f, \mathcal{Q}) \leq 1/k^3$ and $g \not\geq f$ [KTW]	$\tau(f) \geq \rho(f) + \Omega(1/k).$
$\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ and $g \geq f$ [KTW]	$\rho(f) + \Omega\left(\frac{\delta}{k^2}\right) \leq \tau(f)$ $\tau(f) \leq \rho(f) + O(k^3\delta).$

Unconditional Hardness

- Lower bounds for k-CSPs in an a unconditional sense are also known in "weak" models of computation.

Unconditional Hardness

- Lower bounds for k-CSPs in an a unconditional sense are also known in “weak” models of computation.
- A LP or SDP hierarchy generates stronger and stronger relaxations which require progressively more time to solve.

Unconditional Hardness

- Lower bounds for k-CSPs in an a unconditional sense are also known in "weak" models of computation.
- A LP or SDP hierarchy generates stronger and stronger relaxations which require progressively more time to solve.
- The trade-off here is between the integrality gap and efficiency of the algorithm.

Unconditional Hardness

- Lower bounds for k-CSPs in an a unconditional sense are also known in "weak" models of computation.
- A LP or SDP hierarchy generates stronger and stronger relaxations which require progressively more time to solve.
- The trade-off here is between the integrality gap and efficiency of the algorithm.
- *Why this model?* LP and SDP rounding gives non-trivial approximation algorithms for MAX-k-CSPs which beats the random assignment for some predicates.

Unconditional Hardness

- A predicate $f : \{0,1\}^k \rightarrow \{0,1\}$ is **approximation resistant** for Lasserre hierarchy if there exist MAX-k-CSP(f) instances with optimum value $\sim \rho(f)$ but the SDP relaxation obtained after $\Omega(n)$ rounds of Lasserre has value 1.

Unconditional Hardness

- A predicate $f : \{0,1\}^k \rightarrow \{0,1\}$ is **approximation resistant** for Lasserre hierarchy if there exist MAX-k-CSP(f) instances with optimum value $\sim \rho(f)$ but the SDP relaxation obtained after $\Omega(n)$ rounds of Lasserre has value 1.
- Natural to substitute Lasserre with a weaker hierachy like LS_+.

Unconditional Hardness

- A predicate $f : \{0,1\}^k \rightarrow \{0,1\}$ is **approximation resistant** for Lasserre hierarchy if there exist MAX-k-CSP(f) instances with optimum value $\sim \rho(f)$ but the SDP relaxation obtained after $\Omega(n)$ rounds of Lasserre has value 1.
- Natural to substitute Lasserre with a weaker hierachy like LS_+.
- MAX-k-XOR, for $k \geq 3$, is approximation resistant [Schoenebeck].

Unconditional Hardness

- A predicate $f : \{0,1\}^k \rightarrow \{0,1\}$ is **approximation resistant** for Lasserre hierarchy if there exist MAX-k-CSP(f) instances with optimum value $\sim \rho(f)$ but the SDP relaxation obtained after $\Omega(n)$ rounds of Lasserre has value 1.
- Natural to substitute Lasserre with a weaker hierachy like LS_+.
- MAX-k-XOR, for $k \geq 3$, is approximation resistant [Schoenebeck].
- Well distributed linear predicates are approximation resistant [Tulsiani].

Unconditional Hardness

- A predicate $f : \{0,1\}^k \rightarrow \{0,1\}$ is **approximation resistant** for Lasserre hierarchy if there exist MAX-k-CSP(f) instances with optimum value $\sim \rho(f)$ but the SDP relaxation obtained after $\Omega(n)$ rounds of Lasserre has value 1.
- Natural to substitute Lasserre with a weaker hierachy like LS_+.
- MAX-k-XOR, for $k \geq 3$, is approximation resistant [Schoenebeck].
- Well distributed linear predicates are approximation resistant [Tulsiani].
- **Q2:** *Exactly which non-linear predicates are "hard" i.e. have high integrality gap, for many rounds of Lasserre?*

τ^*-Resistance

- For $\tau^* > \rho(f)$, f is said to be τ^*-**resistant** if for an arbitrarily small constant $\varepsilon > 0$, there exists a constant $c = c(\varepsilon) > 0$ and instances with n variables and m constraints, for infinitely many values of n, such that the Lasserre relaxation after $\lfloor cn \rfloor$ rounds has value at least τ^* but the integral optimum is at most $\rho(f) + \varepsilon$.

τ^*-Resistance

- For $\tau^* > \rho(f)$, f is said to be τ^*-**resistant** if for an arbitrarily small constant $\varepsilon > 0$, there exists a constant $c = c(\varepsilon) > 0$ and instances with n variables and m constraints, for infinitely many values of n, such that the Lasserre relaxation after $\lfloor cn \rfloor$ rounds has value at least τ^* but the integral optimum is at most $\rho(f) + \varepsilon$.
- Approximation Resistance $_{\text{for Lasserre}} \equiv$ 1-resistance.

τ^*-Resistance

- For $\tau^* > \rho(f)$, f is said to be τ^*-**resistant** if for an arbitrarily small constant $\varepsilon > 0$, there exists a constant $c = c(\varepsilon) > 0$ and instances with n variables and m constraints, for infinitely many values of n, such that the Lasserre relaxation after $\lfloor cn \rfloor$ rounds has value at least τ^* but the integral optimum is at most $\rho(f) + \varepsilon$.
- Approximation Resistance $_{\text{for Lasserre}} \equiv$ 1-resistance.
- As before one extends the definition of somewhat resistance to the unconditional case.

τ^*-Resistance

- For $\tau^* > \rho(f)$, f is said to be τ^*-**resistant** if for an arbitrarily small constant $\varepsilon > 0$, there exists a constant $c = c(\varepsilon) > 0$ and instances with n variables and m constraints, for infinitely many values of n, such that the Lasserre relaxation after $\lfloor cn \rfloor$ rounds has value at least τ^* but the integral optimum is at most $\rho(f) + \varepsilon$.
- Approximation Resistance $_{\text{for Lasserre}} \equiv$ 1-resistance.
- As before one extends the definition of somewhat resistance to the unconditional case.
- Somewhat approximation resistance has not been investigated before in the context of SDP hierarchies.

Main Theorem

Assume $k \geq k_0$ and $f : \{0,1\}^k \to \{0,1\}$ be a predicate with $\Delta(f, \mathcal{Q}) > 0$.

1. If $\Delta(f, \mathcal{Q}) \geq 1/k^3$, then

$$\tau^*(f) \geq \rho(f) + \Omega(1/k^5).$$

   Else, $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$, and let $g \in \mathcal{Q}$ s.t. $\Delta(f, g) = \delta$.

2. If $\exists x \in \{0,1\}^k$ such that $f(x) = 1 \wedge g(x) = 0$ then

$$\tau^*(f) \geq \rho(f) + \Omega(1/k).$$

3. Else, g is monotonically above f. In this case,

$$\rho(f) + \Omega\left(\frac{\delta}{k^2}\right) \leq \tau^*(f) \leq \rho(f) + O(k^3\delta).$$

A Comparison with Previous Results

k-XOR [Schoenebeck],[Grigoriev]	$\tau^*(f) = 1.$
Well distributed predicates [Tulsiani]	$\tau^*(f) = 1.$
Promise predicates [Tulsiani W]	$\tau^*(f) = 1$ in Static-LS_+.
$\Delta(f, \mathcal{Q}) = 0$ [Håstad]	$\tau^*(f) \leq \rho(f) + \varepsilon \ (\forall \varepsilon > 0).$
$\Delta(f, \mathcal{Q}) \geq 1/k^3$ [KTW]	$\tau^*(f) \geq \rho(f) + \Omega(1/k^5).$
$\Delta(f, \mathcal{Q}) \leq 1/k^3$ and $g \not\geq f$ [KTW]	$\tau^*(f) \geq \rho(f) + \Omega(1/k).$
$\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ and $g \geq f$ [KTW]	$\rho(f) + \Omega\left(\frac{\delta}{k^2}\right) \leq \tau^*(f)$ $\tau^*(f) \leq \rho(f) + O(k^3\delta).$

Proof Outline

- Our result relies on the constructions of [Chan] in the conditional setting and [Tulsiani] in the unconditional setting.

Proof Outline

- Our result relies on the constructions of [Chan] in the conditional setting and [Tulsiani] in the unconditional setting.
- Essentially, [Chan], [Tulsiani] show that a linear predicate $L : \{0,1\}^k \rightarrow \{0,1\}$ is 1-resistant if $L^{-1}(1)$ is the dual space of an affine translate of a distance 3 code.

Proof Outline

- Our result relies on the constructions of [Chan] in the conditional setting and [Tulsiani] in the unconditional setting.
- Essentially, [Chan], [Tulsiani] show that a linear predicate $L : \{0,1\}^k \rightarrow \{0,1\}$ is 1-resistant if $L^{-1}(1)$ is the dual space of an affine translate of a distance 3 code.
- Roughly: Well-distributed linear predicates are hard.

Proof Outline

- Our result relies on the constructions of [Chan] in the conditional setting and [Tulsiani] in the unconditional setting.
- Essentially, [Chan], [Tulsiani] show that a linear predicate $L : \{0,1\}^k \longrightarrow \{0,1\}$ is 1-resistant if $L^{-1}(1)$ is the dual space of an affine translate of a distance 3 code.
- Roughly: Well-distributed linear predicates are hard.
- Well distributed linear predicates L, which have very few accepting assignments, are called "good" predicates.

Proof Outline (contd.)

- Example: $L^{-1}(1)$ corresponds to the Hadamard code.

Proof Outline (contd.)

- Example: $L^{-1}(1)$ corresponds to the Hadamard code.
- Non-Example: $L^{-1}(1)$ corresponds to the Hamming code.

Proof Outline (contd.)

- Example: $L^{-1}(1)$ corresponds to the Hadamard code.
- Non-Example: $L^{-1}(1)$ corresponds to the Hamming code.
- Intuition: We need to translate the known results about good predicates to weak results about **all** other predicates.

Proof Outline (contd.)

- Example: $L^{-1}(1)$ corresponds to the Hadamard code.
- Non-Example: $L^{-1}(1)$ corresponds to the Hamming code.
- Intuition: We need to translate the known results about good predicates to weak results about **all** other predicates.
- Correlation among predicates: $f : \{0,1\}^k \to \{0,1\}$ is said to be τ-**correlated** with L if a uniformly random satisfying assignment for L is a satisfying assignment for f with probability at least τ i.e.,

$$\mathbb{E}_{x \in L^{-1}(1)}[f(x)] = \frac{|L^{-1}(1) \cap f^{-1}(1)|}{|L^{-1}(1)|} \geq \tau.$$

Proof Outline (contd.)

- **Step 1**: If f is τ-correlated with a good predicate then f is τ-resistant (also τ^*-resistant).

Proof Outline (contd.)

- **Step 1**: If f is τ-correlated with a good predicate then f is τ-resistant (also τ^*-resistant).
- [Chan] shows that any well distributed predicate L is 1-resistant.

Proof Outline (contd.)

- **Step 1**: If f is τ-correlated with a good predicate then f is τ-resistant (also τ^*-resistant).
- [Chan] shows that any well distributed predicate L is 1-resistant.
- Main idea: Given any instance Φ_L construct an instance Φ_f such that
  1. YES case (Completeness): If $Val(\Phi_L) \geq 1 - \varepsilon$ then $Val(\Phi_f) \geq \tau - \varepsilon$.
  2. NO case (Soundness): If $Val(\Phi_L) \leq \rho(L) + \varepsilon$ then $Val(\Phi_f) \leq \rho(f) + \varepsilon$.

Proof Outline (contd.)

- **Step 1**: If f is τ-correlated with a good predicate then f is τ-resistant (also τ^*-resistant).
- [Chan] shows that any well distributed predicate L is 1-resistant.
- Main idea: Given any instance Φ_L construct an instance Φ_f such that
  1. YES case (Completeness): If $Val(\Phi_L) \geq 1 - \varepsilon$ then $Val(\Phi_f) \geq \tau - \varepsilon$.
  2. NO case (Soundness): If $Val(\Phi_L) \leq \rho(L) + \varepsilon$ then $Val(\Phi_f) \leq \rho(f) + \varepsilon$.
- We replace L_i with f_i for every constraint in Φ_L to obtain Φ_f. Now, if f and L are τ-correlated then calculations show that f must be τ-resistant.♠

Proof Outline (contd.)

- Summary: To show that f is τ-resistant it will suffice to show f τ-correlates with some good predicate.

Proof Outline (contd.)

- Summary: To show that f is τ-resistant it will suffice to show f τ-correlates with some good predicate.
- In the unconditional setting, we use the result of [Tulsiani] to link τ-correlation and Lasserre lower bounds i.e., τ^*-resistance.

Proof Outline (contd.)

- Summary: To show that f is τ-resistant it will suffice to show f τ-correlates with some good predicate.
- In the unconditional setting, we use the result of [Tulsiani] to link τ-correlation and Lasserre lower bounds i.e., τ^*-resistance.
- Next goal: Characterize the best possible correlation that f can have with some good predicate.

Proof Outline (contd.)

- Summary: To show that f is τ-resistant it will suffice to show f τ-correlates with some good predicate.
- In the unconditional setting, we use the result of [Tulsiani] to link τ-correlation and Lasserre lower bounds i.e., τ^*-resistance.
- Next goal: Characterize the best possible correlation that f can have with some good predicate.
- Remark: Any non-zero predicate f, $\Omega(1/k^2)$-correlates with some good predicate. But we need something better when $\rho(f)$ is large.

Proof Outline (contd.)

- Let $\gamma_r(f)$ denote the Fourier mass at level r and above i.e.

$$\gamma_r(f) := \sum_{|\alpha| \geq r} \hat{f}(\alpha)^2.$$

Proof Outline (contd.)

- Let $\gamma_r(f)$ denote the Fourier mass at level r and above i.e.

$$\gamma_r(f) := \sum_{|\alpha| \geq r} \hat{f}(\alpha)^2.$$

- **Step 2**: Any given f is τ-correlated with a good predicate (and hence τ-resistant) for some τ s.t.

$$\tau \geq \rho(f) + \Omega\left(\frac{\gamma_3(f)}{k^2}\right).$$

Proof Outline (contd.)

- Let $\gamma_r(f)$ denote the Fourier mass at level r and above i.e.

$$\gamma_r(f) := \sum_{|\alpha| \geq r} \hat{f}(\alpha)^2.$$

- **Step 2**: Any given f is τ-correlated with a good predicate (and hence τ-resistant) for some τ s.t.

$$\tau \geq \rho(f) + \Omega\left(\frac{\gamma_3(f)}{k^2}\right).$$

- The proof follows from a probabilistic argument.

Proof Outline (contd.)

- Working with γ is a bit cumbersome so we relate it to Δ.

Proof Outline (contd.)

- Working with γ is a bit cumbersome so we relate it to Δ.
- **Step 3**: If $k \geq 2^{2^{15}}$ and $\gamma_3(f) \leq 1/k^2$ then

$$\gamma_3(f) \leq \Delta(f, \mathcal{Q}) \leq C\gamma_3(f).$$

Proof Outline (contd.)

- Working with γ is a bit cumbersome so we relate it to Δ.
- **Step 3**: If $k \geq 2^{2^{15}}$ and $\gamma_3(f) \leq 1/k^2$ then

$$\gamma_3(f) \leq \Delta(f, \mathcal{Q}) \leq C\gamma_3(f).$$

- The claim above is similar in spirit to [FKN] which relates Fourier mass above level 1 to distance from dictator functions.

$$\gamma_2(f) \leq \Delta(f, \mathcal{L}) \leq C'\gamma_2(f),$$

where $\mathcal{L}$ denotes the set of dictator and constant boolean functions.

Proof Outline (contd.)

- Working with γ is a bit cumbersome so we relate it to Δ.
- **Step 3**: If $k \geq 2^{2^{15}}$ and $\gamma_3(f) \leq 1/k^2$ then

$$\gamma_3(f) \leq \Delta(f, \mathcal{Q}) \leq C\gamma_3(f).$$

- The claim above is similar in spirit to [FKN] which relates Fourier mass above level 1 to distance from dictator functions.

$$\gamma_2(f) \leq \Delta(f, \mathcal{L}) \leq C'\gamma_2(f),$$

  where $\mathcal{L}$ denotes the set of dictator and constant boolean functions.
- Our proof is closely based on Freidgut's theorem but the same results also follow from [Kindler-Safra].

Proof Outline (contd.)

- **Summary**: Steps 1, 2 and 3 together with the result of [Chan] imply case (1) of our main theorem i.e., If $\Delta(f, \mathcal{Q}) \geq 1/k^3$, then

$$\tau(f) \geq \rho(f) + \Omega(1/k^5)$$

and all that remains are cases 2 and 3 of our main theorem.

Proof Outline (contd.)

- **Summary**: Steps 1, 2 and 3 together with the result of [Chan] imply case (1) of our main theorem i.e., If $\Delta(f, \mathcal{Q}) \geq 1/k^3$, then

$$\tau(f) \geq \rho(f) + \Omega(1/k^5)$$

and all that remains are cases 2 and 3 of our main theorem.

- In the unconditional setting we get from the result of [Tulsiani]:

$$\tau^*(f) \geq \rho(f) + \Omega(1/k^5).$$

Proof Outline (contd.)

- **Step 4**: If $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ and if f does not dominate g then we show
$$\tau(f) \geq \rho(f) + \Omega(1/k).$$

Proof Outline (contd.)

- **Step 4**: If $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ and if f does not dominate g then we show
$$\tau(f) \geq \rho(f) + \Omega(1/k).$$
- For illustration, let $\rho(f) = \delta$ be tiny then $g \equiv 0$ and f trivially $\Omega(1/k^2)$-correlates with some well distributed linear predicate.

Proof Outline (contd.)

- **Step 4**: If $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ and if f does not dominate g then we show
$$\tau(f) \geq \rho(f) + \Omega(1/k).$$
- For illustration, let $\rho(f) = \delta$ be tiny then $g \equiv 0$ and f trivially $\Omega(1/k^2)$-correlates with some well distributed linear predicate.
- We prove a more general bound by a direct reduction from well distributed linear predicates to f. The details are left to the paper.

Proof Outline (contd.)

- **Step 4**: If $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ and if f does not dominate g then we show
$$\tau(f) \geq \rho(f) + \Omega(1/k).$$
- For illustration, let $\rho(f) = \delta$ be tiny then $g \equiv 0$ and f trivially $\Omega(1/k^2)$-correlates with some well distributed linear predicate.
- We prove a more general bound by a direct reduction from well distributed linear predicates to f. The details are left to the paper.
- This finishes our lower bounds.

Proof Outline (contd.)

- **Step 4**: If $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ and if f does not dominate g then we show
$$\tau(f) \geq \rho(f) + \Omega(1/k).$$
- For illustration, let $\rho(f) = \delta$ be tiny then $g \equiv 0$ and f trivially $\Omega(1/k^2)$-correlates with some well distributed linear predicate.
- We prove a more general bound by a direct reduction from well distributed linear predicates to f. The details are left to the paper.
- This finishes our lower bounds.
- Remark: In the last case $|\tau(f) - \rho(f)|$ is large even though $\gamma_3(f)$ may be very small in this case.

Proof Outline (contd.)

- **Step 5**: Finally, if $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ f dominates g and MAX-k-CSP(f) is $Ck^3\delta$ satisfiable then we show

$$\tau(f) \leq \rho(f) + O(k^3\delta).$$

Proof Outline (contd.)

- **Step 5**: Finally, if $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ f dominates g and MAX-k-CSP(f) is $Ck^3\delta$ satisfiable then we show

$$\tau(f) \leq \rho(f) + O(k^3\delta).$$

- We provide a SDP rounding algorithm which given a $\rho(f) + \varepsilon$ satisfiable instance outputs a $\rho(f) + \frac{c\varepsilon}{k^2 \log(1/\varepsilon)}$ satisfying assignment and hence can distinguish between $\sim \rho(f)$ vs $\sim \rho(f) + Ck^3\delta$ satisfiable instances.

Proof Outline (contd.)

- **Step 5**: Finally, if $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ f dominates g and MAX-k-CSP(f) is $Ck^3\delta$ satisfiable then we show

$$\tau(f) \leq \rho(f) + O(k^3\delta).$$

- We provide a SDP rounding algorithm which given a $\rho(f) + \varepsilon$ satisfiable instance outputs a $\rho(f) + \frac{c\varepsilon}{k^2 \log(1/\varepsilon)}$ satisfying assignment and hence can distinguish between $\sim \rho(f)$ vs $\sim \rho(f) + Ck^3\delta$ satisfiable instances.
- First, we note that the algorithm of [Charikar Wirth] satisfies $\rho(f) + \frac{c\varepsilon}{\log(1/\varepsilon)}$ constraints of a $\rho(g) + \varepsilon$ satisfiable MAX-k-CSP(g) instance, where $g \in \mathcal{Q}$.

Proof Outline (contd.)

- **Step 5**: Finally, if $\Delta(f, \mathcal{Q}) = \delta \leq 1/k^3$ f dominates g and MAX-k-CSP(f) is $Ck^3\delta$ satisfiable then we show

$$\tau(f) \leq \rho(f) + O(k^3\delta).$$

- We provide a SDP rounding algorithm which given a $\rho(f) + \varepsilon$ satisfiable instance outputs a $\rho(f) + \frac{c\varepsilon}{k^2 \log(1/\varepsilon)}$ satisfying assignment and hence can distinguish between $\sim \rho(f)$ vs $\sim \rho(f) + Ck^3\delta$ satisfiable instances.
- First, we note that the algorithm of [Charikar Wirth] satisfies $\rho(f) + \frac{c\varepsilon}{\log(1/\varepsilon)}$ constraints of a $\rho(g) + \varepsilon$ satisfiable MAX-k-CSP(g) instance, where $g \in \mathcal{Q}$.
- Now we substitute g for f in our MAX-k-CSP(f) instance and use the algorithm of [Charikar Wirth].

Proof Outline (contd.)

- The simple algorithm described previously does not work since the assignment obtained from solving the MAX-k-CSP(g) instance may fail *disproportionately* on the MAX-k-CSP(f) instance (recall $g \geq f$).

Proof Outline (contd.)

- The simple algorithm described previously does not work since the assignment obtained from solving the MAX-k-CSP(g) instance may fail *disproportionately* on the MAX-k-CSP(f) instance (recall $g \geq f$).
- To correct this, we re-reandomize each variable output by the algorithm independently with probability $1 - 1/2k$.

Proof Outline (contd.)

- The simple algorithm described previously does not work since the assignment obtained from solving the MAX-k-CSP(g) instance may fail *disproportionately* on the MAX-k-CSP(f) instance (recall $g \geq f$).
- To correct this, we re-reandomize each variable output by the algorithm independently with probability $1 - 1/2k$.
- Using a simple Chernoff type argument we show that re-randomized assignment satisfies $\rho(f) + \frac{c\varepsilon}{k^2 \log(1/\varepsilon)}$ fraction of constraints.

Proof Outline (contd.)

- The simple algorithm described previously does not work since the assignment obtained from solving the MAX-k-CSP(g) instance may fail *disproportionately* on the MAX-k-CSP(f) instance (recall $g \geq f$).
- To correct this, we re-reandomize each variable output by the algorithm independently with probability $1 - 1/2k$.
- Using a simple Chernoff type argument we show that re-randomized assignment satisfies $\rho(f) + \frac{c\varepsilon}{k^2 \log(1/\varepsilon)}$ fraction of constraints.
- This finishes the outline of our proof of the main theorem.

$\gamma_3(f)$ and $\tau(f)$

- **Claim**: Let $k \geq 16$ and $f : \{0,1\}^k \rightarrow \{0,1\}$ be a predicate. There exists

$$\tau \geq \sqrt{\rho(f)^2 + \frac{\gamma_3(f)}{100k^2}} \tag{1}$$

such that f τ-correlates with some well distributed linear predicate.

$\gamma_3(f)$ and $\tau(f)$

- **Claim**: Let $k \geq 16$ and $f : \{0,1\}^k \to \{0,1\}$ be a predicate. There exists
$$\tau \geq \sqrt{\rho(f)^2 + \frac{\gamma_3(f)}{100k^2}} \tag{1}$$
such that f τ-correlates with some well distributed linear predicate.
- Claim implies that f is τ-resistant (in both senses).

$\gamma_3(f)$ and $\tau(f)$

- **Claim**: Let $k \geq 16$ and $f : \{0,1\}^k \rightarrow \{0,1\}$ be a predicate. There exists
$$\tau \geq \sqrt{\rho(f)^2 + \frac{\gamma_3(f)}{100k^2}} \tag{1}$$
such that f τ-correlates with some well distributed linear predicate.
- Claim implies that f is τ-resistant (in both senses).
- Recall that a well distributed linear predicate L is of the form $L^{-1}(1) = S + z$, S is a subspace and $S^{\perp}$ is a distance (at least) 3 code.

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- We will show that choosing a random S and z ensures:
  1. L is well distributed and
  2. $$\mathbb{E}_{x \in S+z}[f(x)] \geq \sqrt{\hat{f}(0)^2 + \frac{\gamma_3(f)}{100k^2}}. \qquad (2)$$

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- We will show that choosing a random S and z ensures:
  1. L is well distributed and
  2. $$\mathbb{E}_{x \in S+z}[f(x)] \geq \sqrt{\hat{f}(0)^2 + \frac{\gamma_3(f)}{100k^2}}. \tag{2}$$
- Let $dim(S^{\perp}) := d$ and so

$$S + z := \{x \in \mathbb{F}_2^k : \alpha_i \cdot x = b_i, \; i \in [d]\}. \tag{3}$$

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- We will show that choosing a random S and z ensures:
  1. L is well distributed and
  2. $$\mathbb{E}_{x \in S+z}[f(x)] \geq \sqrt{\hat{f}(0)^2 + \frac{\gamma_3(f)}{100k^2}}. \qquad (2)$$
- Let $dim(S^{\perp}) := d$ and so
$$S + z := \{x \in \mathbb{F}_2^k : \alpha_i \cdot x = b_i, \ i \in [d]\}. \qquad (3)$$
- Subclaim: Equations 3 and 2 imply:
$$\mathbb{E}_{x \in S+z}[f(x)] = \sum_{\alpha \in S^{\perp}} (-1)^{\alpha \cdot z} \hat{f}(\alpha). \qquad (4)$$

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Subclaim is true because

$$\mathbb{E}_{x \in S+z}[f(x)] = \frac{2^k}{|S|}\mathbb{E}_{x \in \{0,1\}^k}[1_{S+z}(x) \cdot f(x)]$$

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Subclaim is true because

$$\mathbb{E}_{x\in S+z}[f(x)] = \frac{2^k}{|S|}\mathbb{E}_{x\in\{0,1\}^k}[1_{S+z}(x)\cdot f(x)]$$

- Expanding the indicator variable, we get:

$$\mathbb{E}_{x\in S+z}[f(x)] = 2^d\mathbb{E}_{x\in\{0,1\}^k}\left[\Pi_{i=1}^d\left(\frac{1+(-1)^{\alpha_i\cdot x+b_i}}{2}\right)\cdot f(x)\right].$$

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Subclaim is true because

$$\mathbb{E}_{x \in S+z}[f(x)] = \frac{2^k}{|S|}\mathbb{E}_{x \in \{0,1\}^k}[1_{S+z}(x) \cdot f(x)]$$

- Expanding the indicator variable, we get:

$$\mathbb{E}_{x \in S+z}[f(x)] = 2^d \mathbb{E}_{x \in \{0,1\}^k}\left[\Pi_{i=1}^d \left(\frac{1+(-1)^{\alpha_i \cdot x + b_i}}{2}\right) \cdot f(x)\right].$$

- Now we simplify the RHS by writing f in Fourier basis, expanding $\Pi_{i=1}^d \left(1+(-1)^{\alpha_i \cdot x + b_i}\right)$ and then computing the expectations.

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Subclaim is true because

$$\mathbb{E}_{x\in S+z}[f(x)] = \frac{2^k}{|S|}\mathbb{E}_{x\in\{0,1\}^k}[1_{S+z}(x)\cdot f(x)]$$

- Expanding the indicator variable, we get:

$$\mathbb{E}_{x\in S+z}[f(x)] = 2^d\mathbb{E}_{x\in\{0,1\}^k}\left[\Pi_{i=1}^d\left(\frac{1+(-1)^{\alpha_i\cdot x+b_i}}{2}\right)\cdot f(x)\right].$$

- Now we simplify the RHS by writing f in Fourier basis, expanding $\Pi_{i=1}^d\left(1+(-1)^{\alpha_i\cdot x+b_i}\right)$ and then computing the expectations.
- Simplification implies our subclaim:

$$\mathbb{E}_{x\in S+z}[f(x)] = \sum_{\alpha\in S^\perp}(-1)^{\alpha\cdot z}\hat{f}(\alpha).$$

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Squaring both sides and taking expectations over a uniform random choice of $z \in \{0,1\}^k$ gives:

$$\mathbb{E}_z \left[\mathbb{E}_{x \in S+z}[f(x)]\right]^2 = \hat{f}(0)^2 + \sum_{\alpha:|\alpha|\geq 3} \hat{f}(\alpha)^2 \cdot 1_{\alpha \in S^\perp}. \qquad (5)$$

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Squaring both sides and taking expectations over a uniform random choice of $z \in \{0,1\}^k$ gives:

$$\mathbb{E}_z \left[\mathbb{E}_{x \in S+z}[f(x)]\right]^2 = \hat{f}(0)^2 + \sum_{\alpha : |\alpha| \geq 3} \hat{f}(\alpha)^2 \cdot 1_{\alpha \in S^\perp}. \qquad (5)$$

- Now we let $d = k - 2\log_2 k - 2$ and take expectation (on both sides of Equation 5) over S by choosing $S^\perp$ uniformly from distance 3 codes in $\mathbb{F}_2^k$.

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Squaring both sides and taking expectations over a uniform random choice of $z \in \{0,1\}^k$ gives:

$$\mathbb{E}_z \left[\mathbb{E}_{x \in S+z}[f(x)]\right]^2 = \hat{f}(0)^2 + \sum_{\alpha : |\alpha| \geq 3} \hat{f}(\alpha)^2 \cdot 1_{\alpha \in S^\perp}. \qquad (5)$$

- Now we let $d = k - 2\log_2 k - 2$ and take expectation (on both sides of Equation 5) over S by choosing $S^\perp$ uniformly from distance 3 codes in $\mathbb{F}_2^k$.
- Heuristically, since $\frac{|S^\perp|}{2^k} \simeq \frac{1}{k^2}$ and since $S^\perp$ behaves as a random subset of $\mathbb{F}_2^k$ we will get:

$$\mathbb{E}_{S^\perp}[1_{\alpha \in S^\perp}] \geq \Omega(1/k^2),$$

which will prove our claim.

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Formally, let $\mathcal{C}$ be d dimension codes and $\mathcal{C}_3$ be d dimension codes of distance (at least) 3.

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Formally, let $\mathcal{C}$ be d dimension codes and $\mathcal{C}_3$ be d dimension codes of distance (at least) 3.
- Chosing $S^\perp$ to be a random code in $\mathcal{C}_3$ we get:

$$\mathbb{E}_{S^\perp}[1_{\alpha \in S^\perp}] \geq \mathbb{P}_{C \in \mathcal{C}}[\alpha \in C, C \in \mathcal{C}_3].$$

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Formally, let $\mathcal{C}$ be d dimension codes and $\mathcal{C}_3$ be d dimension codes of distance (at least) 3.
- Chosing $S^\perp$ to be a random code in $\mathcal{C}_3$ we get:

$$\mathbb{E}_{S^\perp}[1_{\alpha \in S^\perp}] \geq \mathbb{P}_{C \in \mathcal{C}}[\alpha \in C, C \in \mathcal{C}_3].$$

- Now $|\mathcal{C}| = \binom{k}{d}_2$.

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- Formally, let $\mathcal{C}$ be d dimension codes and $\mathcal{C}_3$ be d dimension codes of distance (at least) 3.
- Chosing $S^\perp$ to be a random code in $\mathcal{C}_3$ we get:

$$\mathbb{E}_{S^\perp}[1_{\alpha \in S^\perp}] \geq \mathbb{P}_{C \in \mathcal{C}}[\alpha \in C, C \in \mathcal{C}_3].$$

- Now $|\mathcal{C}| = \binom{k}{d}_2$.
- The number of codes in $\mathcal{C}$ containing $\alpha \in \mathbb{F}_2^k$ is $\binom{k-1}{d-1}_2$.

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- The number of codes containing $\alpha \in \mathbb{F}_2^k$ and distance at most 2 is $k^2 \binom{k-2}{d-2}_2$.

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- The number of codes containing $\alpha \in \mathbb{F}_2^k$ and distance at most 2 is $k^2 \binom{k-2}{d-2}_2$.
- So,

$$\mathbb{P}_{C \in \mathcal{C}}[\alpha \in C, C \in \mathcal{C}_3] \geq \frac{\binom{k-1}{d-1}_2 - k^2 \binom{k-2}{d-2}_2}{\binom{k}{d}_2}.$$

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- The number of codes containing $\alpha \in \mathbb{F}_2^k$ and distance at most 2 is $k^2 \binom{k-2}{d-2}_2$.
- So,

$$\mathbb{P}_{C \in \mathcal{C}}[\alpha \in C, C \in \mathcal{C}_3] \geq \frac{\binom{k-1}{d-1}_2 - k^2 \binom{k-2}{d-2}_2}{\binom{k}{d}_2}.$$

- Simplifying the above we get:

$$\mathbb{E}_{S^\perp}[1_{\alpha \in S^\perp}] \geq \frac{1}{100k^2}.$$

$\gamma_3(f)$ and $\tau(f)$ (contd.)

- The number of codes containing $\alpha \in \mathbb{F}_2^k$ and distance at most 2 is $k^2 \binom{k-2}{d-2}_2$.
- So,

$$\mathbb{P}_{C \in \mathcal{C}}[\alpha \in C, C \in \mathcal{C}_3] \geq \frac{\binom{k-1}{d-1}_2 - k^2 \binom{k-2}{d-2}_2}{\binom{k}{d}_2}.$$

- Simplifying the above we get:

$$\mathbb{E}_{S^\perp}[1_{\alpha \in S^\perp}] \geq \frac{1}{100k^2}.$$

- This proves our claim.

Thank You.

Thank You.