Expander Graphs and Their Applications (XVII)

Yijia Chen
Shanghai Jiaotong University

Review of the Previous Lecture

Amplification Lemma (stronger version)

Lemma

Let $0 < \lambda < d$ and $|\Sigma|$ be constants. Then there exists a constant $\beta_2 = \beta_2(\lambda, d, |\Sigma|) > 0$ such that for every $t \in \mathbb{N}$ and for every d-regular constraint graph G with a selfloop on each vertex and $\lambda(G) \leq \lambda$, the following hold.

For every $\vec{\sigma} : V \to \Sigma^{d^{\lceil t/2 \rceil}}$ let $\sigma : V \to \Sigma$ be defined according to "popular opinion" by setting, for each $v \in V$, $\sigma(v) := a$ such that

$$\Pr[\text{a random } \lceil t/2 \rceil\text{-step walk in } G \text{ from } v \text{ reaches a vertex } w \text{ with } \vec{\sigma}(w)_v = a],$$

where $\vec{\sigma}(w)_v \in \Sigma$ denotes the restriction of $\vec{\sigma}(w)$ to v, is maximized over all $a \in \Sigma$.

Then

$$\mathrm{unsat}_{\vec{\sigma}}(G^t) \geq \beta_2 \cdot \sqrt{t} \cdot \min\left(\mathrm{unsat}_{\sigma}(G), \frac{1}{t}\right).$$

Assignment Tester

Long Code

Long Code

Let $s \in \mathbb{N}$ and

$$\underline{L} := \left\{ f \mid f : \{0,1\}^s \to \{0,1\} \right\}.$$

Long Code

Let $s \in \mathbb{N}$ and

$$\underline{L} := \left\{ f \mid f : \{0,1\}^s \to \{0,1\} \right\}.$$

For every string $a = (a_1, \ldots, a_s) \in \{0,1\}^s$ we define $\underline{A_a} : L \to \{0,1\}$ in such a way that for every $f \in L$

$$A_a(f) = f(a).$$

Long Code

Let $s \in \mathbb{N}$ and

$$L := \left\{ f \mid f : \{0,1\}^s \to \{0,1\} \right\}.$$

For every string $a = (a_1, \ldots, a_s) \in \{0,1\}^s$ we define $A_a : L \to \{0,1\}$ in such a way that for every $f \in L$

$$A_a(f) = f(a).$$

Each A_a itself can be viewed as a string of $|L|$ bits, and the set

$$\left\{ A_a \mid a \in \{0,1\}^s \right\}$$

is an error-correcting code called the Long-Code.

Long Code

Let $s \in \mathbb{N}$ and

$$L := \left\{ f \mid f : \{0,1\}^s \to \{0,1\} \right\}.$$

For every string $a = (a_1, \ldots, a_s) \in \{0,1\}^s$ we define $A_a : L \to \{0,1\}$ in such a way that for every $f \in L$

$$A_a(f) = f(a).$$

Each A_a itself can be viewed as a string of $|L|$ bits, and the set

$$\left\{ A_a \mid a \in \{0,1\}^s \right\}$$

is an error-correcting code called the Long-Code.

Let $\ell \in \mathbb{N}$.

Long Code

Let $s \in \mathbb{N}$ and

$$L := \left\{ f \mid f : \{0,1\}^s \to \{0,1\} \right\}.$$

For every string $a = (a_1, \ldots, a_s) \in \{0,1\}^s$ we define $A_a : L \to \{0,1\}$ in such a way that for every $f \in L$

$$A_a(f) = f(a).$$

Each A_a itself can be viewed as a string of $|L|$ bits, and the set

$$\left\{ A_a \mid a \in \{0,1\}^s \right\}$$

is an error-correcting code called the Long-Code.

Let $\ell \in \mathbb{N}$. $s_1, s_2 \in \{0,1\}^\ell$ are δ-far (resp. δ-close) from one another is $\mathrm{dist}(s_1, s_2) \geq \delta \cdot \ell$ (resp. if $\mathrm{dist}(s_1, s_2) \leq \delta \cdot \ell$).

Long Code

Let $s \in \mathbb{N}$ and

$$L := \left\{ f \mid f : \{0,1\}^s \to \{0,1\} \right\}.$$

For every string $a = (a_1, \ldots, a_s) \in \{0,1\}^s$ we define $A_a : L \to \{0,1\}$ in such a way that for every $f \in L$

$$A_a(f) = f(a).$$

Each A_a itself can be viewed as a string of $|L|$ bits, and the set

$$\left\{ A_a \mid a \in \{0,1\}^s \right\}$$

is an error-correcting code called the Long-Code.

Let $\ell \in \mathbb{N}$. $s_1, s_2 \in \{0,1\}^\ell$ are δ-far (resp. δ-close) from one another is $\mathrm{dist}(s_1, s_2) \geq \delta \cdot \ell$ (resp. if $\mathrm{dist}(s_1, s_2) \leq \delta \cdot \ell$). Recall

$$\mathrm{dist}(s_1, s_2) := \left| \left\{ i \in [\ell] \mid s_1(i) \neq s_2(i) \right\} \right|.$$

Long Code

Let $s \in \mathbb{N}$ and

$$L := \left\{ f \mid f : \{0,1\}^s \to \{0,1\} \right\}.$$

For every string $a = (a_1, \ldots, a_s) \in \{0,1\}^s$ we define $A_a : L \to \{0,1\}$ in such a way that for every $f \in L$

$$A_a(f) = f(a).$$

Each A_a itself can be viewed as a string of $|L|$ bits, and the set

$$\left\{ A_a \mid a \in \{0,1\}^s \right\}$$

is an error-correcting code called the Long-Code.

Let $\ell \in \mathbb{N}$. $s_1, s_2 \in \{0,1\}^\ell$ are δ-far (resp. δ-close) from one another is $\mathrm{dist}(s_1, s_2) \geq \delta \cdot \ell$ (resp. if $\mathrm{dist}(s_1, s_2) \leq \delta \cdot \ell$). Recall

$$\mathrm{dist}(s_1, s_2) := \left| \left\{ i \in [\ell] \mid s_1(i) \neq s_2(i) \right\} \right|.$$

and

$$\mathrm{rdist}(s_1, s_2) := \frac{\mathrm{dist}(s_1, s_2)}{\ell}.$$

Long Code (cont'd)

Long Code (cont'd)

Lemma

For $a \neq a' \in \{0,1\}^s$

$$\mathrm{rdist}(A_a, A_{a'}) = \frac{1}{2}.$$

Folded Strings

Folded Strings

Let A be a string of length $|L|$, which we also viewed as a function

$$A : L \to \{0, 1\}.$$

Folded Strings

Let A be a string of length $|L|$, which we also viewed as a function

$$A : L \to \{0, 1\}.$$

A is *folded over true* if for every $f \in L$

$$A(-f) = -A(f)$$

where $-$ is the Boolean negation.

Folded Strings

Let A be a string of length $|L|$, which we also viewed as a function

$$A : L \to \{0,1\}.$$

A is *folded over true* if for every $f \in L$

$$A(-f) = -A(f)$$

where $-$ is the Boolean negation.

For a function $\psi : \{0,1\}^s \to \{0,1\}$ the string A is *folded over* ψ if for every $f \in L$

$$A(f) = A(f \wedge \psi).$$

Folded Strings (cont'd)

Folded Strings (cont'd)

First, let

$$\underline{L_\psi} := \{f \in L \mid f = f \wedge \psi\}$$

Folded Strings (cont'd)

First, let

$$L_\psi := \{f \in L \mid f = f \wedge \psi\}$$

Then we choose some $L'_\psi \subseteq L_\psi$ such that for every $f \in L_\psi$

- if $-f \in L_\psi$ too, then L'_ψ contains exactly one of f and $-f$;
- otherwise, L'_ψ contains f.

Folded Strings (cont'd)

First, let

$$\underline{L_\psi} := \{f \in L \mid f = f \wedge \psi\}$$

Then we choose some $L'_\psi \subseteq L_\psi$ such that for every $f \in L_\psi$

- if $-f \in L_\psi$ too, then L'_ψ contains exactly one of f and $-f$;
- otherwise, L'_ψ contains f.

Lemma

If $A : L \to \{0,1\}$ is folded over true and over ψ, then A is uniquely determined by $A \restriction L'_\psi$.

Long-Code Theorem

Long-Code Theorem

There exists a *Long-Code Test* $\mathbb{T}$ which is a randomized algorithm that has input a function $\psi : \{0,1\}^s \to \{0,1\}$, and also oracle access to a string $A : L \to \{0,1\}$ *folded over true and over* ψ. $\mathbb{T}$ reads the input ψ and tosses some random coins. Based on these it computes a three-bit predicate

$$w : \{0,1\}^3 \to \{0,1\}$$

and three locations $f_1, f_2, f_3 \in L$ in which it queries the string A. It then outputs $w(A(f_1), A(f_2), A(f_3))$. Denote an execution of $\mathbb{T}$ with access to input ψ and string A by $\mathbb{T}^A(\psi)$. Then the following hold.

Long-Code Theorem

There exists a *Long-Code Test* $\mathbb{T}$ which is a randomized algorithm that has input a function $\psi : \{0,1\}^s \to \{0,1\}$, and also oracle access to a string $A : L \to \{0,1\}$ *folded over true and over* ψ. $\mathbb{T}$ reads the input ψ and tosses some random coins. Based on these it computes a three-bit predicate

$$w : \{0,1\}^3 \to \{0,1\}$$

and three locations $f_1, f_2, f_3 \in L$ in which it queries the string A. It then outputs $w(A(f_1), A(f_2), A(f_3))$. Denote an execution of $\mathbb{T}$ with access to input ψ and string A by $\mathbb{T}^A(\psi)$. Then the following hold.

- (**Perfect Completeness**): If $a \in \{0,1\}^s$ with $\psi(a) = 1$, then

$$\Pr\left[\mathbb{T}^{A_a}(\psi) \text{ accepts}\right] = 1.$$

Long-Code Theorem

There exists a *Long-Code Test* $\mathbb{T}$ which is a randomized algorithm that has input a function $\psi : \{0,1\}^s \to \{0,1\}$, and also oracle access to a string $A : L \to \{0,1\}$ *folded over true and over* ψ. $\mathbb{T}$ reads the input ψ and tosses some random coins. Based on these it computes a three-bit predicate

$$w : \{0,1\}^3 \to \{0,1\}$$

and three locations $f_1, f_2, f_3 \in L$ in which it queries the string A. It then outputs $w(A(f_1), A(f_2), A(f_3))$. Denote an execution of $\mathbb{T}$ with access to input ψ and string A by $\mathbb{T}^A(\psi)$. Then the following hold.

- (**Perfect Completeness**): If $a \in \{0,1\}^s$ with $\psi(a) = 1$, then

$$\Pr\left[\mathbb{T}^{A_a}(\psi) \text{ accepts}\right] = 1.$$

- (**Strong Soundness**): For every $\delta \in [0,1]$ if $A : L \to \{0,1\}$ is folded over true and over ψ and at least δ-far from A_a for all $a \in \{0,1\}^s$ with $\psi(a) = 1$, then

$$\Pr\left[\mathbb{T}^{A}(\psi) \text{ rejects}\right] \geq \Omega(\delta).$$

Proof of the Long-Code Theorem

Some Technical Changes

Some Technical Changes

Let $s \in \mathbb{N}$.

Some Technical Changes

Let $s \in \mathbb{N}$. We will identify $\{0,1\}^s$ with $[n]$ for $n := 2^s$.

Some Technical Changes

Let $s \in \mathbb{N}$. We will identify $\{0,1\}^s$ with $[n]$ for $n := 2^s$.

We consider Boolean functions $\psi : [n] \to \{-1,1\}$ by changing 1 (i.e., true) to -1, and 0 (i.e., false) to 1.

Long-Code Theorem (restated)

Long-Code Theorem (restated)

There exists a *Long-Code Test* $\mathbb{T}$ which is a randomized algorithm that has input a function $\psi : [n] \to \{-1, 1\}$, and also oracle access to a string $A : L \to \{-1, 1\}$ *folded over true and over* ψ. $\mathbb{T}$ reads the input ψ and tosses some random coins. Based on these it computes a three-bit predicate $w : \{0, 1\}^3 \to \{-1, 1\}$ and three locations $f_1, f_2, f_3 \in L$ in which it queries the string A. It then outputs $w(A(f_1), A(f_2), A(f_3))$ such that

Long-Code Theorem (restated)

There exists a *Long-Code Test* $\mathbb{T}$ which is a randomized algorithm that has input a function $\psi : [n] \to \{-1, 1\}$, and also oracle access to a string $A : L \to \{-1, 1\}$ *folded over true and over* ψ. $\mathbb{T}$ reads the input ψ and tosses some random coins. Based on these it computes a three-bit predicate $w : \{0, 1\}^3 \to \{-1, 1\}$ and three locations $f_1, f_2, f_3 \in L$ in which it queries the string A. It then outputs $w(A(f_1), A(f_2), A(f_3))$ such that

- (**Perfect Completeness**): If $a \in [n]$ with $\psi(a) = -1$, then

$$\Pr\left[\mathbb{T}^{A_a}(\psi) \text{ accepts}\right] = 1.$$

Long-Code Theorem (restated)

There exists a *Long-Code Test* $\mathbb{T}$ which is a randomized algorithm that has input a function $\psi : [n] \to \{-1, 1\}$, and also oracle access to a string $A : L \to \{-1, 1\}$ *folded over true and over* ψ. $\mathbb{T}$ reads the input ψ and tosses some random coins. Based on these it computes a three-bit predicate $w : \{0, 1\}^3 \to \{-1, 1\}$ and three locations $f_1, f_2, f_3 \in L$ in which it queries the string A. It then outputs $w(A(f_1), A(f_2), A(f_3))$ such that

- (**Perfect Completeness**): If $a \in [n]$ with $\psi(a) = -1$, then

$$\Pr\left[\mathbb{T}^{A_a}(\psi) \text{ accepts}\right] = 1.$$

- (**Strong Soundness**): For every $\delta \in [0, 1]$ if $A : L \to \{-1, 1\}$ is folded over true and over ψ and at least δ-far from A_a for all $a \in \{0, 1\}^s$ with $\psi(a) = -1$, then

$$\Pr\left[\mathbb{T}^{A}(\psi) \text{ rejects}\right] \geq \Omega(\delta).$$

Standard Definition

Standard Definition

We identify $L = \{f \mid [n] \to \{-1, 1\}\}$ with the Boolean hypercube $\{-1, 1\}^n$, and use f, g for the points in the hypercube.

Standard Definition

We identify $L = \{f \mid [n] \to \{-1, 1\}\}$ with the Boolean hypercube $\{-1, 1\}^n$, and use f, g for the points in the hypercube.

We use letters A, B, or χ to denote functions whose domain is the hypercube.

Standard Definition (cont'd)

Standard Definition (cont'd)

For every $A, B : \{-1,1\}^n \to \{-1,1\}$ let

$$\underline{\langle A, B \rangle} := \mathbb{E}_{f \in L}\big[A(f) \cdot B(f)\big] = \frac{\sum_f A(f) \cdot B(f)}{2^n}.$$

Standard Definition (cont'd)

For every $A, B : \{-1,1\}^n \to \{-1,1\}$ let

$$\underline{\langle A, B \rangle} := \mathbb{E}_{f \in L}\big[A(f) \cdot B(f)\big] = \frac{\sum_f A(f) \cdot B(f)}{2^n}.$$

For every $\alpha \subseteq [n]$ let

$$\chi_\alpha : \{-1,1\}^n \to \{-1,1\} \quad \text{with} \quad \chi_\alpha(f) := \prod_{i \in \alpha} f(i).$$

Recall $\alpha = \emptyset$ we assume $\prod_{i \in \alpha} f(i) = 1$ for every $f \in L$.

Standard Definition (cont'd)

For every $A, B : \{-1,1\}^n \to \{-1,1\}$ let

$$\underline{\langle A, B \rangle} := \mathbb{E}_{f \in L}\left[A(f) \cdot B(f)\right] = \frac{\sum_f A(f) \cdot B(f)}{2^n}.$$

For every $\alpha \subseteq [n]$ let

$$\chi_\alpha : \{-1,1\}^n \to \{-1,1\} \quad \text{with} \quad \chi_\alpha(f) := \prod_{i \in \alpha} f(i).$$

Recall $\alpha = \emptyset$ we assume $\prod_{i \in \alpha} f(i) = 1$ for every $f \in L$.

For every $i \in [n]$

$$\chi_{\{i\}} = A_i.$$

Standard Definition (cont'd)

Standard Definition (cont'd)

Lemma

For every $\alpha, \beta \subseteq [n]$

Standard Definition (cont'd)

Lemma

For every $\alpha, \beta \subseteq [n]$

- *if* $\alpha = \beta$ *then* $\langle \chi_\alpha, \chi_\beta \rangle = 1$;

Standard Definition (cont'd)

Lemma

For every $\alpha, \beta \subseteq [n]$

- *if* $\alpha = \beta$ *then* $\langle \chi_\alpha, \chi_\beta \rangle = 1$;
- *if* $\alpha \neq \beta$ *then* $\langle \chi_\alpha, \chi_\beta \rangle = 0$.

Standard Definition (cont'd)

Standard Definition (cont'd)

Theorem

The characters $\{\chi_\alpha\}$ *form an orthogonal basis for the space of functions*

$$\{A \mid \{-1,1\}^n \to \mathbb{R}\}$$

using the inner product defined above.

Standard Definition (cont'd)

Theorem

The characters $\{\chi_\alpha\}$ *form an orthogonal basis for the space of functions*

$$\{A \mid \{-1,1\}^n \to \mathbb{R}\}$$

using the inner product defined above.

Therefore, every function $A : \{-1,1\}^n \to \{-1,1\}$ can be written as

$$A = \sum_{\alpha \subseteq [n]} \hat{A}_\alpha \cdot \chi_\alpha \quad \text{where} \quad \hat{A}_\alpha := \langle A, \chi_\alpha \rangle$$

Standard Definition (cont'd)

Theorem

The characters $\{\chi_\alpha\}$ *form an orthogonal basis for the space of functions*

$$\{A \mid \{-1,1\}^n \to \mathbb{R}\}$$

using the inner product defined above.

Therefore, every function $A : \{-1,1\}^n \to \{-1,1\}$ can be written as

$$A = \sum_{\alpha \subseteq [n]} \hat{A}_\alpha \cdot \chi_\alpha \quad \text{where} \quad \hat{A}_\alpha := \langle A, \chi_\alpha \rangle$$

We also have **Parseval's Identity**

$$\sum_{\alpha \subseteq [n]} \hat{A}_\alpha^2 = \langle A, A \rangle = 1.$$

Recall $A : \{-1,1\}^n \to \{-1,1\}$, hence the range of A is a subset of $\{-1,1\}$.

The Test

The Test

Let $\psi : [n] \to \{-1, 1\}$ be some predicate and

$$\tau := \frac{1}{100}.$$

The Test

Let $\psi : [n] \to \{-1, 1\}$ be some predicate and

$$\tau := \frac{1}{100}.$$

Let $A : \{-1, 1\}^n \to \{-1, 1\}$ be a string folded over true and over ψ, i.e., for every $f \in L = \{-1, 1\}^n$

$$A(-f) = -A(f) \quad \text{and} \quad A(f) = A(f \wedge \psi).$$

The Test

Let $\psi : [n] \to \{-1, 1\}$ be some predicate and

$$\tau := \frac{1}{100}.$$

Let $A : \{-1, 1\}^n \to \{-1, 1\}$ be a string folded over true and over ψ, i.e., for every $f \in L = \{-1, 1\}^n$

$$A(-f) = -A(f) \quad \text{and} \quad A(f) = A(f \wedge \psi).$$

Note, here $f \wedge \psi$ is defined by

$$(f \wedge \psi)(a) = \begin{cases} -1, & \text{if } f(a) = \psi(a) = -1 \\ 1, & \text{otherwise.} \end{cases}$$

for every $a \in [n]$.

The Test (cont'd)

The Test (cont'd)

A function $A : \{-1, 1\}^n \to \{-1, 1\}$ is the *legal encoding* of the value $a \in [n]$ if $A(f) = f(a)$ for all $f \in L$.

The Test (cont'd)

A function $A : \{-1, 1\}^n \to \{-1, 1\}$ is the *legal encoding* of the value $a \in [n]$ if $A(f) = f(a)$ for all $f \in L$.

The following procedure tests whether A is close to the legal encoding of some value $a \in [n]$ that satisfies ψ.

The Test (cont'd)

A function $A : \{-1, 1\}^n \to \{-1, 1\}$ is the *legal encoding* of the value $a \in [n]$ if $A(f) = f(a)$ for all $f \in L$.

The following procedure tests whether A is close to the legal encoding of some value $a \in [n]$ that satisfies ψ.

1. Select $f, g \in L$ uniformly at random.

The Test (cont'd)

A function $A : \{-1,1\}^n \to \{-1,1\}$ is the *legal encoding* of the value $a \in [n]$ if $A(f) = f(a)$ for all $f \in L$.

The following procedure tests whether A is close to the legal encoding of some value $a \in [n]$ that satisfies ψ.

1. Select $f, g \in L$ uniformly at random.
2. Set $h := g \cdot \mu$ where $\mu \in L$ is selected by doing the following independently for every $y \in [n]$. If $f(y) = 1$, then set $\mu(y) := -1$. If $f(y) = -1$, then set

$$\mu(y) := \begin{cases} 1 & \text{with probability } 1 - \tau \\ -1 & \text{with probability } \tau. \end{cases}$$

The Test (cont'd)

A function $A : \{-1,1\}^n \to \{-1,1\}$ is the *legal encoding* of the value $a \in [n]$ if $A(f) = f(a)$ for all $f \in L$.

The following procedure tests whether A is close to the legal encoding of some value $a \in [n]$ that satisfies ψ.

1. Select $f, g \in L$ uniformly at random.
2. Set $h := g \cdot \mu$ where $\mu \in L$ is selected by doing the following independently for every $y \in [n]$. If $f(y) = 1$, then set $\mu(y) := -1$. If $f(y) = -1$, then set

$$\mu(y) := \begin{cases} 1 & \text{with probability } 1 - \tau \\ -1 & \text{with probability } \tau. \end{cases}$$

3. Accept unless $A(g) = A(f) = A(h) = 1$.

Proof of the Long-Code Theorem

Proof of the Long-Code Theorem

Theorem (**Completeness**)

If $\alpha \in [n]$ *such that* $\psi(a) = -1$, *then* $\Pr\left[\mathbb{T}^{A_a}(\psi) \text{ accepts}\right] = 1$.

Proof of the Long-Code Theorem

Theorem (**Completeness**)

If $\alpha \in [n]$ *such that* $\psi(a) = -1$, *then* $\Pr\left[\mathbb{T}^{A_a}(\psi) \text{ accepts}\right] = 1$.

Proof.

We fix some $a \in [n]$ for which $\psi(a) = -1$.

Proof of the Long-Code Theorem

Theorem (**Completeness**)

If $\alpha \in [n]$ *such that* $\psi(a) = -1$, *then* $\Pr\left[\mathbb{T}^{A_a}(\psi) \text{ accepts}\right] = 1$.

Proof.

We fix some $a \in [n]$ for which $\psi(a) = -1$.

Now let $A : \{-1,1\}^n \to \{-1,1\}$ be the string with $A(f) = f(a)$ for all $f \in L$.

Proof of the Long-Code Theorem

Theorem (**Completeness**)

If $\alpha \in [n]$ *such that* $\psi(a) = -1$, *then* $\Pr\left[\mathbb{T}^{A_a}(\psi) \text{ accepts}\right] = 1$.

Proof.

We fix some $a \in [n]$ for which $\psi(a) = -1$.

Now let $A : \{-1,1\}^n \to \{-1,1\}$ be the string with $A(f) = f(a)$ for all $f \in L$.

Clearly A is folded over true and over ψ.

Proof of the Long-Code Theorem

Theorem (**Completeness**)

If $\alpha \in [n]$ *such that* $\psi(a) = -1$, *then* $\Pr\left[\mathbb{T}^{A_a}(\psi) \text{ accepts}\right] = 1$.

Proof.

We fix some $a \in [n]$ for which $\psi(a) = -1$.

Now let $A : \{-1,1\}^n \to \{-1,1\}$ be the string with $A(f) = f(a)$ for all $f \in L$.

Clearly A is folded over true and over ψ.

If $A(f) = f(a) = -1$ then the test accepts.

Proof of the Long-Code Theorem

Theorem (**Completeness**)

If $\alpha \in [n]$ *such that* $\psi(a) = -1$, *then* $\Pr\left[\mathbb{T}^{A_a}(\psi) \text{ accepts}\right] = 1$.

Proof.

We fix some $a \in [n]$ for which $\psi(a) = -1$.

Now let $A : \{-1,1\}^n \to \{-1,1\}$ be the string with $A(f) = f(a)$ for all $f \in L$.

Clearly A is folded over true and over ψ.

If $A(f) = f(a) = -1$ then the test accepts.

If $A(f) = f(a) = 1$, then $A(h) = h(a) = -g(a) = -A(g) \neq A(g)$, and again the test accepts.

□

Proof of the Long-Code Theorem (cont'd)

Proof of the Long-Code Theorem (cont'd)

Theorem (**Soundness**)

There exists a constant $c > 0$ *such that for every* $\delta \in [0,1]$, *if* $A : \{-1,1\}^n \to \{-1,1\}$ *is folded over true and over* ψ *and at least* δ*-far from* A_a *for all* $a \in [n]$ *with* $\psi(a) = -1$, *then* $\Pr\left[\mathbb{T}^A(\psi) \text{ rejects}\right] \geq c \cdot \delta$.

Proof of the Soundness

Proof of the Soundness

Let us fix some $\delta \in (0, 1]$ and assume that A is δ-far from every A_α for every $a \in [n]$ with $\psi(a) = -1$.

Proof of the Soundness

Let us fix some $\delta \in (0, 1]$ and assume that A is δ-far from every A_α for every $a \in [n]$ with $\psi(a) = -1$.

We let

$$\underline{\varepsilon} := Pr\left[\mathbb{T}^A(\psi) \text{ rejects}\right].$$

Proof of the Soundness

Let us fix some $\delta \in (0, 1]$ and assume that A is δ-far from every A_α for every $a \in [n]$ with $\psi(a) = -1$.

We let

$$\varepsilon := Pr\left[\mathbb{T}^A(\psi) \text{ rejects}\right].$$

We aim to show that

for some appropriate constant c we have $\varepsilon \geq c \cdot \delta$.

Proof of the Soundness (cont'd)

Proof of the Soundness (cont'd)

We will prove later:

Proposition. *There exists a constant $C > 0$ such that if $\mathbb{T}$ rejects with probability ε then*

$$\sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2 \leq C \cdot \varepsilon$$

Proof of the Soundness (cont'd)

We will prove later:

Proposition. *There exists a constant $C > 0$ such that if $\mathbb{T}$ rejects with probability ε then*

$$\sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2 \leq C \cdot \varepsilon$$

We will also need:

Theorem (**Friedgut, Kalai, and Naor**, 2002)

There is a constant $C' > 0$ such that the following holds. Let $n \in \mathbb{N}$, $\rho > 0$, and $A : \{-1,1\}^n \to \{-1,1\}$ with

$$\sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2 \leq \rho.$$

Then either

$$\left|\hat{A}_\emptyset\right|^2 \geq 1 - C' \cdot \rho \quad \text{or} \quad \left|\hat{A}_{\{i\}}\right|^2 \geq 1 - C' \cdot \rho \text{ for some } i \in [n].$$

Proof of the Soundness (cont'd)

Proof of the Soundness (cont'd)

Lemma

1. *If A is folded over true, then $\hat{A}_\alpha = 0$ for every $\alpha \subseteq [n]$ with even $|\alpha|$.*

Proof of the Soundness (cont'd)

Lemma

1. *If A is folded over true, then $\hat{A}_\alpha = 0$ for every $\alpha \subseteq [n]$ with even $|\alpha|$.*
2. *If A is folded over ψ and for some $i \in \alpha \subseteq [n]$ we have $\psi(i) = 1$, then $\hat{A}_\alpha = 0$.*

Proof of the Soundness (cont'd)

Lemma

1. *If A is folded over true, then $\hat{A}_\alpha = 0$ for every $\alpha \subseteq [n]$ with even $|\alpha|$.*
2. *If A is folded over ψ and for some $i \in \alpha \subseteq [n]$ we have $\psi(i) = 1$, then $\hat{A}_\alpha = 0$.*

Proof.

Recall

$$\hat{A}_\alpha = \langle A, \chi_\alpha \rangle = \frac{\sum_f A(f) \cdot \chi_\alpha(f)}{2^n} = \frac{\sum_f (A(f) \cdot \Pi_{a \in \alpha} f(a))}{2^n}$$

□

Proof of the Soundness (cont'd)

Proof of the Soundness (cont'd)

Then by the previous proposition (yet to be proved) and the theorem of **Friedgut, Kalai, and Naor**, we have some $i \in [n]$ such that

$$\psi(i) = -1 \quad \text{and} \quad \left|\hat{A}_{\{i\}}\right|^2 \geq 1 - C' \cdot C \cdot \varepsilon.$$

Proof of the Soundness (cont'd)

Then by the previous proposition (yet to be proved) and the theorem of **Friedgut, Kalai, and Naor**, we have some $i \in [n]$ such that

$$\psi(i) = -1 \quad \text{and} \quad \left|\hat{A}_{\{i\}}\right|^2 \geq 1 - C' \cdot C \cdot \varepsilon.$$

Therefore one of the following holds.

Proof of the Soundness (cont'd)

Then by the previous proposition (yet to be proved) and the theorem of **Friedgut, Kalai, and Naor**, we have some $i \in [n]$ such that

$$\psi(i) = -1 \quad \text{and} \quad \left|\hat{A}_{\{i\}}\right|^2 \geq 1 - C' \cdot C \cdot \varepsilon.$$

Therefore one of the following holds.

(i) $\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$, or

Proof of the Soundness (cont'd)

Then by the previous proposition (yet to be proved) and the theorem of **Friedgut, Kalai, and Naor**, we have some $i \in [n]$ such that

$$\psi(i) = -1 \quad \text{and} \quad \left|\hat{A}_{\{i\}}\right|^2 \geq 1 - C' \cdot C \cdot \varepsilon.$$

Therefore one of the following holds.

(i) $\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$, or

(ii) $-\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$

Proof of the Soundness (cont'd)

Then by the previous proposition (yet to be proved) and the theorem of **Friedgut, Kalai, and Naor**, we have some $i \in [n]$ such that

$$\psi(i) = -1 \quad \text{and} \quad \left|\hat{A}_{\{i\}}\right|^2 \geq 1 - C' \cdot C \cdot \varepsilon.$$

Therefore one of the following holds.

(i) $\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$, or

(ii) $-\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$

By definition

$$\hat{A}_\alpha = \mathbb{E}_f \left[A(f) \cdot \chi_\alpha(f)\right] = 1 - 2 \cdot \mathrm{rdist}(A, \chi_\alpha),$$

so if (i) holds, then

$$\delta \leq \mathrm{rdist}(A, \chi_{\{i\}}) \leq \frac{C \cdot C' \cdot \varepsilon}{2}.$$

Proof of the Soundness (cont'd)

Then by the previous proposition (yet to be proved) and the theorem of **Friedgut, Kalai, and Naor**, we have some $i \in [n]$ such that

$$\psi(i) = -1 \quad \text{and} \quad \left|\hat{A}_{\{i\}}\right|^2 \geq 1 - C' \cdot C \cdot \varepsilon.$$

Therefore one of the following holds.

(i) $\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$, or

(ii) $-\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$

By definition

$$\hat{A}_\alpha = \mathbb{E}_f\left[A(f) \cdot \chi_\alpha(f)\right] = 1 - 2 \cdot \mathrm{rdist}(A, \chi_\alpha),$$

so if (i) holds, then

$$\delta \leq \mathrm{rdist}(A, \chi_{\{i\}}) \leq \frac{C \cdot C' \cdot \varepsilon}{2}.$$

We are done.

Proof of the Soundness (cont'd)

Now assume (ii), i.e., $-\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$ holds.

Proof of the Soundness (cont'd)

Now assume (ii), i.e., $-\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$ holds.
Imagine first that

$$-\hat{A}_{\{i\}} = 1, \quad \text{i.e.,} \quad A = -\chi_{\{i\}} \quad \text{(why?)}.$$

Proof of the Soundness (cont'd)

Now assume (ii), i.e., $-\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$ holds.
Imagine first that

$$-\hat{A}_{\{i\}} = 1, \quad \text{i.e.,} \quad A = -\chi_{\{i\}} \quad \text{(why?)}.$$

Then the probability (over the choice of f, g, and h) that

$$f(i) = g(i) = h(i) = -1$$

is at least $(1 - \tau)/4$.

Proof of the Soundness (cont'd)

Now assume (ii), i.e., $-\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$ holds. Imagine first that

$$-\hat{A}_{\{i\}} = 1, \quad \text{i.e.,} \quad A = -\chi_{\{i\}} \quad \text{(why?)}.$$

Then the probability (over the choice of f, g, and h) that

$$f(i) = g(i) = h(i) = -1$$

is at least $(1 - \tau)/4$. In that case, $A(f) = A(g) = A(h) = 1$ by our tentative assumption $A = -\chi_{\{i\}}$. Then the test $\mathbb{T}$ rejects (so $\varepsilon \geq (1 - \tau)/4 > 1/8$ by $\tau = 1/100$).

Proof of the Soundness (cont'd)

Now assume (ii), i.e., $-\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$ holds.
Imagine first that

$$-\hat{A}_{\{i\}} = 1, \quad \text{i.e.,} \quad A = -\chi_{\{i\}} \quad \text{(why?)}.$$

Then the probability (over the choice of f, g, and h) that

$$f(i) = g(i) = h(i) = -1$$

is at least $(1 - \tau)/4$. In that case, $A(f) = A(g) = A(h) = 1$ by our tentative assumption $A = -\chi_{\{i\}}$. Then the test $\mathbb{T}$ rejects (so $\varepsilon \geq (1 - \tau)/4 > 1/8$ by $\tau = 1/100$).
This probability can go down by at most $3 \cdot \mathrm{rdist}(A, -\chi_{\{i\}})$*, which is an upper bound on the probability that at least one of* f, g, h *is a point of disagreement between* A *and* $-\chi_{\{i\}}$.

Proof of the Soundness (cont'd)

Now assume (ii), i.e., $-\hat{A}_{\{i\}} \geq \sqrt{1 - C' \cdot C \cdot \varepsilon} \geq 1 - C' \cdot C \cdot \varepsilon$ holds.
Imagine first that

$$-\hat{A}_{\{i\}} = 1, \quad \text{i.e.,} \quad A = -\chi_{\{i\}} \quad \text{(why?)}.$$

Then the probability (over the choice of f, g, and h) that

$$f(i) = g(i) = h(i) = -1$$

is at least $(1 - \tau)/4$. In that case, $A(f) = A(g) = A(h) = 1$ by our tentative assumption $A = -\chi_{\{i\}}$. Then the test $\mathbb{T}$ rejects (so $\varepsilon \geq (1 - \tau)/4 > 1/8$ by $\tau = 1/100$).
This probability can go down by at most $3 \cdot \mathrm{rdist}(A, -\chi_{\{i\}})$*, which is an upper bound on the probability that at least one of* f, g, h *is a point of disagreement between* A *and* $-\chi_{\{i\}}$. Then

$$\varepsilon \geq \frac{1 - \tau}{4} - 3 \cdot \mathrm{rdist}(A, -\chi_{\{i\}}) > \frac{1}{8} - \frac{3}{2} \cdot C \cdot C' \cdot \varepsilon,$$

i.e., $\varepsilon > 1/8 \cdot (1 + 3 \cdot C \cdot C'/2)$.

Proposition. *There exists a constant $C > 0$ such that if $\mathbb{T}$ rejects with probability ε then*

$$\sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2 \leq C \cdot \varepsilon$$

Proposition. *There exists a constant $C > 0$ such that if $\mathbb{T}$ rejects with probability ε then*

$$\sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2 \leq C \cdot \varepsilon$$

Proof.

Proposition. *There exists a constant $C > 0$ such that if $\mathbb{T}$ rejects with probability ε then*

$$\sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2 \leq C \cdot \varepsilon$$

Proof.

$$\begin{aligned} 1 - \varepsilon &= \Pr[\mathbb{T}^A(\psi) \text{ accepts}] \\ &= \mathbb{E}_{f,g,h}\left[1 - \frac{(1 + A(f))(1 + A(g))(1 + A(h))}{8}\right]. \end{aligned}$$

Proposition. *There exists a constant $C > 0$ such that if $\mathbb{T}$ rejects with probability ε then*

$$\sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2 \leq C \cdot \varepsilon$$

Proof.

$$\begin{aligned} 1 - \varepsilon &= \Pr[\mathbb{T}^A(\psi) \text{ accepts}] \\ &= \mathbb{E}_{f,g,h}\left[1 - \frac{(1 + A(f))(1 + A(g))(1 + A(h))}{8}\right]. \end{aligned}$$

Since (f, g) and (f, h) are pairs of random independent functions, and $\mathbb{E}[A] = \hat{A}_\emptyset = 0$ by A being folded over true, we have

$$1 - \varepsilon = \frac{7}{8} - \frac{\mathbb{E}_{g,h}\left[A(g)A(h)\right]}{8} - \frac{\mathbb{E}_{f,g,h}\left[A(f)A(g)A(h)\right]}{8}.$$

Proof. (cont'd)

Proof. (cont'd)

Using the Fourier Expansion $A(g) = \sum_\alpha \hat{A}_\alpha \chi_\alpha(g)$

$$\mathbb{E}_{g,h}\big[A(g)A(h)\big] = \mathbb{E}_{g,h}\left[\sum_{\alpha,\beta\subseteq[n]} \hat{A}_\alpha \hat{A}_\beta \chi_\alpha(g)\chi_\beta(h)\right] = \sum_{\alpha\subseteq[n]} \hat{A}_\alpha^2 \cdot (-\tau)^{|\alpha|}$$

which is bounded *by τ in absolute value*, since $\hat{A}_\emptyset = 0$.

Proof. (cont'd)

Using the Fourier Expansion $A(g) = \sum_\alpha \hat{A}_\alpha \chi_\alpha(g)$

$$\mathbb{E}_{g,h}\big[A(g)A(h)\big] = \mathbb{E}_{g,h}\left[\sum_{\alpha,\beta\subseteq[n]} \hat{A}_\alpha \hat{A}_\beta \chi_\alpha(g)\chi_\beta(h)\right] = \sum_{\alpha\subseteq[n]} \hat{A}_\alpha^2 \cdot (-\tau)^{|\alpha|}$$

which is bounded *by τ in absolute value*, since $\hat{A}_\emptyset = 0$.

Let $W := \mathbb{E}_{f,g,h}\big[A(f)A(g)A(h)\big]$.

Proof. (cont'd)

Using the Fourier Expansion $A(g) = \sum_\alpha \hat{A}_\alpha \chi_\alpha(g)$

$$\mathbb{E}_{g,h}\big[A(g)A(h)\big] = \mathbb{E}_{g,h}\left[\sum_{\alpha,\beta\subseteq[n]} \hat{A}_\alpha \hat{A}_\beta \chi_\alpha(g)\chi_\beta(h)\right] = \sum_{\alpha\subseteq[n]} \hat{A}_\alpha^2 \cdot (-\tau)^{|\alpha|}$$

which is bounded *by τ in absolute value*, since $\hat{A}_\emptyset = 0$.

Let $W := \mathbb{E}_{f,g,h}\big[A(f)A(g)A(h)\big]$.

$$\begin{aligned} -1 + \tau + 8\cdot\varepsilon \geq W &= \mathbb{E}_{g,f,\mu}\left[\sum_{\alpha,\beta,\gamma\subseteq[n]} \hat{A}_\alpha \hat{A}_\beta \hat{A}_\gamma \chi_\alpha(g)\chi_\beta(g\mu)\chi_\gamma(f)\right] \\ &= \sum_{\alpha,\gamma\subseteq[n]} \hat{A}_\gamma \hat{A}_\alpha^2 \mathbb{E}_{f,\mu}\big[\chi_\alpha(\mu)\chi_\gamma(f)\big] \\ &= \sum_{\gamma\subseteq\alpha\subseteq[n]} \hat{A}_\gamma \hat{A}_\alpha^2 \cdot (-1+\tau)^{|\gamma|}(-\tau)^{|\alpha\setminus\gamma|}, \end{aligned}$$

the last equality holds by the correlation of μ and f:

Proof. (cont'd)

Using the Fourier Expansion $A(g) = \sum_\alpha \hat{A}_\alpha \chi_\alpha(g)$

$$\mathbb{E}_{g,h}\big[A(g)A(h)\big] = \mathbb{E}_{g,h}\left[\sum_{\alpha,\beta\subseteq[n]} \hat{A}_\alpha \hat{A}_\beta \chi_\alpha(g)\chi_\beta(h)\right] = \sum_{\alpha\subseteq[n]} \hat{A}_\alpha^2 \cdot (-\tau)^{|\alpha|}$$

which is bounded *by τ in absolute value*, since $\hat{A}_\emptyset = 0$.

Let $W := \mathbb{E}_{f,g,h}\big[A(f)A(g)A(h)\big]$.

$$\begin{aligned} -1+\tau+8\cdot\varepsilon \geq W &= \mathbb{E}_{g,f,\mu}\left[\sum_{\alpha,\beta,\gamma\subseteq[n]} \hat{A}_\alpha \hat{A}_\beta \hat{A}_\gamma \chi_\alpha(g)\chi_\beta(g\mu)\chi_\gamma(f)\right] \\ &= \sum_{\alpha,\gamma\subseteq[n]} \hat{A}_\gamma \hat{A}_\alpha^2 \mathbb{E}_{f,\mu}\big[\chi_\alpha(\mu)\chi_\gamma(f)\big] \\ &= \sum_{\gamma\subseteq\alpha\subseteq[n]} \hat{A}_\gamma \hat{A}_\alpha^2 \cdot (-1+\tau)^{|\gamma|}(-\tau)^{|\alpha\setminus\gamma|}, \end{aligned}$$

the last equality holds by the correlation of μ and f: (i) if $\gamma \not\subseteq \alpha$ then $\mathbb{E}_{f,\mu}\big[\chi_\alpha(\mu)\chi_\gamma(f)\big] = 0$; (ii) $\mathbb{E}[\mu(i)] = \tau$ and $\mathbb{E}[f(i)\mu(i)] = -1+\tau$ for all $i \in [n]$.

Proof. (cont'd)

We now bound the absolute value of the above term.

Proof. (cont'd)

We now bound the absolute value of the above term. We claim that

$$\sum_{\gamma \subseteq \alpha} \left((1-\tau)^{|\gamma|} \tau^{|\alpha \setminus \gamma|} \right)^2 \leq (1-\tau)^{|\alpha|}.$$

Proof. (cont'd)

We now bound the absolute value of the above term. We claim that

$$\sum_{\gamma \subseteq \alpha} \left((1-\tau)^{|\gamma|} \tau^{|\alpha \setminus \gamma|} \right)^2 \leq (1-\tau)^{|\alpha|}.$$

The left hand side is the probability that *tossing* $2|\alpha|$ *independent* τ*-biased coins results in a pattern* $\gamma\gamma$ *where* $\gamma \in \{0,1\}^{|\alpha|}$.

Proof. (cont'd)

We now bound the absolute value of the above term. We claim that

$$\sum_{\gamma \subseteq \alpha} \left((1-\tau)^{|\gamma|} \tau^{|\alpha \setminus \gamma|} \right)^2 \leq (1-\tau)^{|\alpha|}.$$

The left hand side is the probability that *tossing* $2|\alpha|$ *independent* τ*-biased coins results in a pattern* $\gamma\gamma$ *where* $\gamma \in \{0,1\}^{|\alpha|}$. This probability is $\left(\tau^2 + (1-\tau)^2\right)^{|\alpha|} \leq (1-\tau)^{|\alpha|}$ since $\tau < 1-\tau$.

Proof. (cont'd)

We now bound the absolute value of the above term. We claim that

$$\sum_{\gamma \subseteq \alpha} \left((1-\tau)^{|\gamma|} \tau^{|\alpha \setminus \gamma|} \right)^2 \leq (1-\tau)^{|\alpha|}.$$

The left hand side is the probability that *tossing* $2|\alpha|$ *independent* τ*-biased coins results in a pattern* $\gamma\gamma$ *where* $\gamma \in \{0,1\}^{|\alpha|}$. This probability is $\left(\tau^2 + (1-\tau)^2\right)^{|\alpha|} \leq (1-\tau)^{|\alpha|}$ since $\tau < 1-\tau$. By the Cauchy-Schwarz inequality,

$$\begin{aligned} \sum_{\gamma \subseteq \alpha} \left| \hat{A}_\gamma \right| (1-\tau)^{|\gamma|} \tau^{|\alpha \setminus \gamma|} &\leq \sqrt{\sum_{\gamma \subseteq \alpha} \left| \hat{A}_\gamma \right|^2} \cdot \sqrt{\sum_{\gamma \subseteq \alpha} \left((1-\tau)^{|\gamma|} \tau^{|\alpha \setminus \gamma|} \right)^2} \\ &\leq (1-\tau)^{|\alpha|/2}. \end{aligned}$$

Proof. (cont'd)

We now bound the absolute value of the above term. We claim that

$$\sum_{\gamma \subseteq \alpha} \left((1-\tau)^{|\gamma|} \tau^{|\alpha \setminus \gamma|} \right)^2 \leq (1-\tau)^{|\alpha|}.$$

The left hand side is the probability that *tossing* $2|\alpha|$ *independent* τ*-biased coins results in a pattern* $\gamma\gamma$ *where* $\gamma \in \{0,1\}^{|\alpha|}$. This probability is $\left(\tau^2 + (1-\tau)^2\right)^{|\alpha|} \leq (1-\tau)^{|\alpha|}$ since $\tau < 1-\tau$. By the Cauchy-Schwarz inequality,

$$\begin{aligned} \sum_{\gamma \subseteq \alpha} \left| \hat{A}_\gamma \right| (1-\tau)^{|\gamma|} \tau^{|\alpha \setminus \gamma|} &\leq \sqrt{\sum_{\gamma \subseteq \alpha} \left| \hat{A}_\gamma \right|^2} \cdot \sqrt{\sum_{\gamma \subseteq \alpha} \left((1-\tau)^{|\gamma|} \tau^{|\alpha \setminus \gamma|} \right)^2} \\ &\leq (1-\tau)^{|\alpha|/2}. \end{aligned}$$

Splitting the sum into $|\alpha| = 1$ and $|\alpha| > 1$,

$$|W| \leq \sum_{|\alpha|=1} \left| \hat{A}_\alpha \right|^2 (1-\tau) + \sum_{|\alpha|>1} \left| \hat{A}_\alpha \right|^2 (1-\tau)^{|\alpha|/2}.$$

Proof. (cont'd)

Let $\rho := \sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2$.

Proof. (cont'd)

Let $\rho := \sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2$. We have $|W| \leq (1-\rho)(1-\tau) + \rho(1-\tau)^{3/2}$, since $\hat{A}_\alpha = 0$ for even $|\alpha|$.

Proof. (cont'd)

Let $\rho := \sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2$. We have $|W| \leq (1-\rho)(1-\tau) + \rho(1-\tau)^{3/2}$, since $\hat{A}_\alpha = 0$ for even $|\alpha|$. Thus

$$1 - \tau - 8\varepsilon \leq |W| \leq (1-\tau)\big((1-\rho) + \rho\sqrt{1-\tau}\big)$$

$$\implies \quad \rho \leq \frac{8\varepsilon}{(1-\tau)(1-\sqrt{1-\tau})}.$$

Proof. (cont'd)

Let $\rho := \sum_{|\alpha|>1} \left|\hat{A}_\alpha\right|^2$. We have $|W| \leq (1-\rho)(1-\tau) + \rho(1-\tau)^{3/2}$, since $\hat{A}_\alpha = 0$ for even $|\alpha|$. Thus

$$1 - \tau - 8\varepsilon \leq |W| \leq (1-\tau)\big((1-\rho) + \rho\sqrt{1-\tau}\big)$$

$$\implies \quad \rho \leq \frac{8\varepsilon}{(1-\tau)(1-\sqrt{1-\tau})}.$$

We are done since τ is a fixed constant.

□