Chapter 8
The Proofs of the PCP Theorems

Angsheng Li

Institute of Software
Chinese Academy of Sciences

Advanced Algorithms, U CAS
April, 2016

Outline

1. Backgrounds
2. CSP
3. Gap amplification
4. Hardness of $2\mathrm{CSP}_W$
5. Hastad's 3bit PCP

Three approaches

1. Local test approach (Arora, Sudan, 1992, full proof 1998)
2. Expander approach (Dinur, 06)
3. Fourier analysis approach (Hastad, 1998)

We introduce the two later approaches.
The first approach is a development of new ECC and new decoding algorithms of the ECC, based on the algebraic fundamental theorem.

CSP with non-binary alphabet

Definition

($q\mathrm{CSP}_W$) For $q, W \in \mathbb{N}$, $q\mathrm{CSP}$ with alphabet $[W] = \{0, 1, 2 \cdots, W - 1\}$.

For $\rho < 1$,
the $\rho - \mathrm{GAP}\ q\ \mathrm{CSP}_W$ problem.
Examples:
i) 3SAT: $q = 3$, $W = 2$, constraints are OR's of literals
ii) 3COL: $2\mathrm{CSP}_3$.

Overall ideas of Dinur's proof

We know
The PCP theorem $\Longleftrightarrow \rho - \mathrm{GAP}q\mathrm{CSP}$ is NP-hard for $\rho < 1$.
Let $\rho = 1 - \epsilon$.

Theorem

Given a 3CSP instance ϕ, if ϕ is satisfiable, $\mathrm{val}(\phi) = 1$, otherwise, then $\mathrm{val}(\phi) \leq 1 - \frac{1}{m}$.

Therefore, for $\rho = 1 - \frac{1}{m}$,
the $\rho - \mathrm{GAP3CSP}$ is NP-hard.
To prove the PCP theorem, it suffices to amplify the error from $\frac{1}{m}$ to a constant ϵ_0.

Reduction

The proof is a reduction R:

$$R : \; q\mathrm{CSP} \to q'\mathrm{CSP}$$

$$\phi \mapsto \psi$$

$$\mathrm{val}(\phi) \leq 1 - \epsilon \Rightarrow \mathrm{val}(\psi) \leq 1 - 2\epsilon.$$

Linear-blowup reduction

Definition

Let f be a function mapping CSP instances to CSP instances. We say that f is a complete linear-blowup reduction, written CL-reduction, if:

i) f is polynomial time computable
ii) (Completeness) If $\mathrm{val}(\phi) = 1$, then so is $\mathrm{val}(f(\phi))$.
iii) (Linear blowup) If ϕ has m constraints, then $f(\phi)$ has at most cm constraints and alphabet W, where C, W depend on only the arity and alphabet of ϕ.

The PCP main lemma

Lemma

There exist constants q_0, $\epsilon_0 > 0$ and a CL-reduction f:

- *If ϕ is q_0CSP, then so is $\psi = f(\phi)$,*
- *If $\epsilon < \epsilon_0$ and $\mathrm{val}(\phi) \leq 1 - \epsilon$, then*

$$\mathrm{val}(\psi) \leq 1 - 2\epsilon.$$

Consequently:
There exist constants q_0, ϵ_0 such that

$$(1 - 2\epsilon_0) - \mathrm{GAP}q_0\mathrm{CSP}$$

is NP-hard.

Gap amplification lemma

Lemma

For every $l, q \in \mathbb{N}$, there exist $W \in \mathbb{N}$, $\epsilon_0 > 0$, CL-reduction g:

- *If ϕ is q*CSP*, then $\psi = g(\phi)$ is $2\mathrm{CSP}_W$,*
- *for each $\epsilon < \epsilon_0$, if $\mathrm{val}(\phi) \leq 1 - \epsilon$, then*

$$\mathrm{val}(\psi) \leq 1 - l \cdot \epsilon.$$

Arity:

$$q \Rightarrow 2$$

Alphabet:

$$2 \Rightarrow W$$

Error:

$$\epsilon \Rightarrow l\epsilon$$

Alphabet reduction lemma

Lemma

There exist q_0, CL-reduction h:

1) *If ϕ is $2\mathrm{CSP}_W$, then $\psi - h(\phi)$ is $q_0\mathrm{CSP}$*
2) *If $\mathrm{val}(\phi) \le 1 - \epsilon$, then*

$$\mathrm{val}(\psi) \le 1 - \frac{\epsilon}{3}.$$

- Arity: $2 \Rightarrow q_0$
- Alphabet: $W \Rightarrow 2$
- Error: $\epsilon \Rightarrow \frac{\epsilon}{3}$.
- Combining the gap amplification and the alphabet reduction lemmas with $l = 6$, $q = q_0$.

Intuition

- Parallel repetition
- To reduce the size, we use random walks in expanders

Basic tools

1) For a regular graph $G = (V, E)$, $S \subseteq V$, $|S| \leq \frac{n}{2}$, $|V| = n$,

$$\Pr_{(u,v)\in_{\mathrm{R}} E}[u \in S \,\&\, v \in S] \leq \frac{|S|}{n}\left(\frac{1}{2} + \frac{\lambda(G)}{2}\right).$$

2)

$$\lambda(G^l) = (\lambda(G))^l.$$

For $T = \bar{S}$,

$$e(S, T) \geq (1 - \lambda(G))\frac{d|S| \cdot |T|}{n} \geq \frac{1 - \lambda(G)}{2} \cdot d|S|$$

The probability that $v \in T$ under the condition of $u \in S$ is at least $\frac{1-\lambda(G)}{2}$.
The probability that $v \in S$ under the condition of $u \in S$ is $\frac{1}{2} + \frac{\lambda(G)}{2}$.
This gives 1). 2) as before.

Notation

Definition

We say that a $q\mathrm{CSP}_W$ instance ϕ is “nice", if:

P1 The arity q of ϕ is 2.

P2 ϕ has a constraint graph G satisfying:

- 0.1 for a constraint with variables u_i, u_j, there is an edge (i, j)
- 0.2 G has parallel edges and self-loops
- 0.3 G is d-regular, and half the edges are self-loops

P3 G is an expander with $\lambda(G) \leq 0.9$, say.

Convention: Assume all CSP instances are nice.

Powering

Lemma

There is an algorithm that given any $2\mathrm{CSP}_W$ instance ψ satisfying P1 - P3, and an integer $t \geq 1$, produces an instance ψ^t satisfying:

1. ψ^t *is a* $2\mathrm{CSP}_{W'}$ *instance,* $W' < W^{d^{5t}}$, ψ^t *has* $d^{t+\sqrt{t}+1} \cdot n$ *constraints.*
2. *If* ψ *is satisfied, then so is* ψ^t.
3. *For every* $\epsilon < \frac{1}{d\sqrt{t}}$, *if* $\mathrm{val}(\psi) \leq 1 - \epsilon$, *then* $\mathrm{val}(\psi^t) \leq 1 - \epsilon'$, *for* $\epsilon' = \frac{\sqrt{t}}{10^5 d W^4}\epsilon$.
4. ψ^t *is produced from* ψ *in time polynomial in m and* W^{d^t}.

Proof - I

Outline of the reduction:

$$\psi \Rightarrow \psi^t$$

Variables y – the same y's

$$y \in W \Rightarrow y \in W^{d^{5t}}$$

Consider the constraint graph G of ψ.
Let y be a variable of ψ^t, the assignment of y in ψ^t defines the codes for all old variables of ψ in a ball of radius $t + \sqrt{t}$.
For every path P in G of length $2t + 1$, define a constraint for ψ^t as follows:

Defining constraints for ψ^t

Suppose that

$$P = i_1, i_2, \cdots, i_{2t+1}.$$

Define the constraint c_P for ψ^t:
c_P is false, if there is a $j \in [2t+1]$ satisfying:

(i) i_j is in the $(t+\sqrt{t})$-radius ball around i_1,

(ii) I_{j+1} is in the $(t+\sqrt{t})$-radius ball of i_{2t+1},

(iii) Let w be the value of i_j defined by i_1, w' be the value of I_{j+1} defined by i_{2t+1}, and

(iv) (w, w') fails to satisfy the constraint associated with i_j and i_{j+1} in ψ.

Lifting assignment for ψ^t

For every variable u in ψ^t, u defines a value $f_u(v)$ for every v in G such that $\mathrm{dist}(u, v) \leq t + \sqrt{t}$ in G.
For every assignment to the variables $u_1, u_2, \cdots, u_n$ in ψ, we lift it to a canonical assignment to the variables $y_1, y_2, \cdots, y)n$ in ψ^t as follows:
For each y_i, define

$$f_i(y_j) = f(u_j)$$

for each y_j in the $t + \sqrt{t}$-radius ball of u_i.
Completeness:
If $(u_1), \cdots, f(u_n)$ satisfy ψ, then the assignment defined above for ψ^t satisfies all the constraints of ψ^t.

Soundness

$$\mathrm{val}(\psi) \le \epsilon \Rightarrow \mathrm{val}(\psi^t) \le 1 - \epsilon',$$

for $\epsilon' = \frac{\sqrt{t}}{10^5 d W^4}\epsilon$.
Given an assignment $f_1, f_2, \cdots, f_n$ to the new variables $y_1, y_2, \cdots, y_n$ for ψ^t. Note that $f_i(j)$ is the value of y_j defined by y_i.
For a fixed j, define $f(j)$ to be the majority $f_i(j)$ for all possible i's, and define $f(j)$ to be the value of u_j for ψ.

Plurality assignment

Idea: Fix an assignment $\mathbf{y} = y_1, y_2, \cdots, y_n$ to ψ^t, define an assignment **u** for ψ by plurality. Then:
If **u** violates a few (ϵ) constraints of ψ, then **y** violates many ($\epsilon' = \Omega(\sqrt{t}\epsilon)$) constraints of ψ^t.

Definition

(Plurality assignment) For every variable u_i of ψ, we define the random variable Z_i over $\{0, 1 \cdots, W-1\}$ as follows:

(i) start from vertex i,

(ii) take t step random walk in G to reach vertex k,

(iii) let z_i be the most likely value of $y_k(i)$.

(iv) let

$$\mathbf{z} = z_1, z_2, \cdots, z_n$$

be the plurality assignment.

Failure set

Note

$$\Pr[Z_i = z_i] \geq \frac{1}{W}.$$

Assume $\mathrm{val}(\psi) \leq 1 - \epsilon$.
For the plurality assignment $\mathbf{z} = z_1, z_2, \cdots, z_n$, let F be the set of constraints of ψ that are not satisfied by $\mathbf{z}$.
Then:

$$|F| \geq \epsilon m = \epsilon d \frac{n}{2}.$$

We call F the *failure set* of ψ. We will use the failure set F to show that $\mathbf{y}$ fails to satisfy ϵ' fraction of the constraints of ψ^t.

Probability space

1) Pick a $(2t+1)$ step path $i_1, i_2, \cdots i_{2t+2}$ in G, i.e., a random constraint of ψ^t.
2) For each j, $1 \leq j \leq 2t+1$, we say that the j-th edge in the path, i.e., (i_j, i_{j+1}), is *truthful* if:
   – y_{i_j} gives the plurality value of i_j, and
   – $y_{i_{2t+2}}$ gives the plurality value for i_{j+1}.

Fact: If there is an edge (i_j, i_{j+1}) which is both truthful and in F, then the constraint defined by the path is unsatisfied.
What we will prove is: there are ϵ' fraction of the paths that contain the edges as above.

The probability that an edge is chosen

Lemma

(Property 1) For each edge e of G and each $j \in [2t+1]$,

$$\Pr[e \text{ is the } j\text{th edge of the path}] = \frac{1}{|E|} = \frac{2}{dn}.$$

The proof is by observation.

The probability that a chosen edge is truthful

Lemma

(Property 2) Let $\delta < \frac{1}{100W}$. For each edge e of G and j with $t \leq j \leq t + \delta\sqrt{t}$,

$$\Pr[e \text{ is truthful} \mid e \text{ is the jth edge}] \geq \frac{1}{2W^2}.$$

Intuition: The edges in the middle of the paths are truthful with high probability.

Proof of Property 2 - I

By property 1, the set of walks of length $2t+1$ that contain $e=(i_j, i_{j+1})$ at the jth step can be generated by concatenating a random walk of length j from i_j, and a random walk of length $2t-j$ from i_{j+1}.
To property Property 2, it suffices to prove:
The probability that:
– y_{i_j} gives the plurality value of i_j, and
– $y_{i_{2t+2}}$ gives the plurality value for i_{j+1}
is at least $\frac{1}{2W^2}$.

Proof of Property 2 - II

Assume $j \in \{t, t+1, \cdots, t+\delta\sqrt{t}\}$.
Recall that at each vertex of G, half edges are self-loops.
For a random walk of l steps, we define a distribution S_l:
1) the number of the random coins that come up “heads",
2) take S_l “real" steps on the graph.
Then:

$$\Pr[S_l = k] = \binom{l}{k} 2^{-t}.$$

Proof of Property 2 - III

This gives

$$\frac{1}{2}\sum_m |\Pr[S_t = m] - \Pr[S_{t+\delta\sqrt{t}} = m]| \leq 10\delta.$$

Therefore, for each $j \in \{t, t+1, \cdots, t+\delta\sqrt{t}\}$,

$$\begin{aligned} &\Pr[y_{i_1} \text{ gives the plurality value for } i_j \text{ and} \\ &\quad y_{i_{2t+1}} \text{ gives the pluraity value for} i_{j+1}] \\ &\geq (\frac{1}{W} - 10\delta)(\frac{1}{W} - 10\delta) \geq \frac{1}{2W^2}. \end{aligned} \qquad (1)$$

Proof

Let V be the random variable denoting the number of edges among the middle $\delta\sqrt{t}$ edges that are truthful and in F. According to properties 1 and 2,

$$E[V] \geq \delta\sqrt{t} \times \frac{|F|}{|E|} \times \frac{1}{2W^2}.$$

Property 3

First,

$$E[V^2] \le 30\epsilon\delta\sqrt{t}d.$$

Let V': the number of edges in the middle that are in F.
Then $V \le V'$.
We prove

$$E[V'^2] \le 30\epsilon\delta\sqrt{t}d.$$

For $j \in \{t, t+1, \cdots, t+\delta\sqrt{t}\}$,

$$I_j = \begin{cases} 1, & \text{if the } j\text{th edge is in } F, \\ 0, & \text{o.w.} \end{cases} \tag{2}$$

Then

$$V' = \sum_{j \in \{t, t+1, \cdots, t+\delta\sqrt{t}\}} I_j.$$

Proof of property 3 - II

$$
\begin{aligned}
E[V'^2] &= E[\sum_{j,j'} I_j I_{j'}] \\
&= E[\sum_{j} I_j^2] + E[\sum_{j\neq j'} I_j I_{j'}] \\
&= \epsilon\delta\sqrt{t} + E[\sum_{j\neq j'} I_j I_{j'}] \\
&= \epsilon\delta\sqrt{t} + 2\sum_{j<j'} \Pr[(j\text{th edge is in } F \ \wedge\ (j'\text{th edge is in } F)] \\
&\leq \epsilon\delta\sqrt{t} + 2\sum_{j<j'} \Pr[(j\text{th vertex in } S) \wedge (j'\text{th vertex in } S)]
\end{aligned}
$$

$$
\begin{aligned}
&\leq \epsilon\delta\sqrt{t} + 2\sum_{j<j'} \epsilon d(\epsilon d + (\lambda(G))^{j'-j}) \\
&\leq \epsilon\delta\sqrt{t} + 2\epsilon^2\delta\sqrt{t}d^2 + 2\epsilon\delta\sqrt{t}d\sum_{k\geq 1}\lambda^k(G) \\
&\leq \epsilon\delta\sqrt{t} + 2\epsilon^2\delta\sqrt{t}d^2 + 20\epsilon\delta\sqrt{t}d \\
&\leq 30\epsilon\delta\sqrt{t}d.(\epsilon < \frac{1}{d\sqrt{t}}).
\end{aligned} \tag{3}
$$

Finally,

$$
\Pr[V > 0] \geq \frac{(E[V])^2}{E[V^2]} \geq \frac{(\delta\sqrt{t}\epsilon)^2}{30\epsilon\delta\sqrt{t}d} = \frac{\sqrt{t}}{10^5 dW^4}\epsilon = \epsilon'.
$$

Proof of reducing alphabet size - I

Let ϕ be a 2CSP instance with:
(i) n variables $u_1, u_2, \cdots, u_n$,
(ii) alphabet $\{0, 1, \cdots W - 1\}$, and
(iii) constraints $C_1, C_2, \cdots, C_m$.
Each variable takes value in $[W]$, that is interpreted as a string in $\{0, 1\}^{\log W}$.
Each constraint C_k involves variables u_i and u_j is regarded as a circuit $\widehat{C}_k$ applied to the bit strings.
Let l be an upper bound of all the circuits size.
Then,

$$l \leq 2^{2^{\log W}} < W^4.$$

Now each $\widehat{C}_k$ is a new constraint with binary variables.

Project property

For each constraint $C(y_1, y_2)$, for each value of y_1, there is a unique y_2 such that $C(y_1, y_2)$ is satisfied.

A $2\mathrm{CSP}$ instance ϕ is called *regular*, if every variable appears in the same number of constraints.

Raz's repetition Theorem

Theorem

There is a $c > 1$ such that for every $t > 1$, $\epsilon - \mathrm{GAP2CSP}_W$ is NP-hard for $\epsilon = 2^{-t}$, $W = 2^{ct}$, and the result holds for $2\mathrm{CSP}$ instances that are regular and have the projection property.

Intuition

Assume ϕ is a $2\mathrm{CSP}_W$ instance such that either $\mathrm{val}(\phi) = 1$ or $\mathrm{val}(\phi) = \rho < 1$, and its is NP-hard to distinct the two cases.
Construct ϕ^{*t} as follows.
For every t-tuple of constraints of ϕ:

$$\phi_1(y_1, z_1), \phi_2(y_2, z_2), \cdots, \phi_t(y_t, z_t)$$

ϕ^{*t} has the constraint of the form:

$$\wedge_{i=1}^{t} \phi_i(y_i, z_i)$$

between variables $(y_1, y_2, \cdots, y_t)$ and $(z_1, z_2, \cdots, z_t)$.
Running the verifier for ϕ in parallel t times gives the theorem.

3-bit PCP Theorem

Theorem

For every $\delta > 0$ and every language $L \in \mathrm{NP}$, there is a PCP verifier V for L making three binary queries haing completeness $1 - \delta$ and soundness at most $\frac{1}{2} + \delta$.
Moreover the tests used by V are linear. That is, given a proof $\pi \in \{0, 1\}^m$, V chooses a triple $(i_1, i_2, i_3) \in [m]^3$ and $b \in \{0, 1\}$ according to some distribution and accepts if and only if

$$\pi_{i_1} + \pi_{i_2} + \pi_{i_3} = b \pmod 2.$$

Long code

Definition

The long code for $[W]$ encodes each $w \in [W]$ by a table of all values of the function $\chi_{\{w\}} : \{\pm 1\}^{[W]} \to \{\pm 1\}$.
Let $W \in \mathbb{N}$. For $w \in [W]$,

$$\chi_{\{w\}}(x_1, x_2, \cdots, x_W) = \prod_{i \in \{w\}} x_i = \prod_{i=w} x_i = x_w.$$

The long code or codeword defined by w is the table of the function $\chi_{\{w\}}$.
Given a function $f : \{\pm 1\}^W \to \{\pm 1\}$, we need to test if f is a long code $\chi_{\{w\}}$ for some $w \in [W]$.

Local test of long code

The local tester for long code $\mathcal{T}$:

(1) Pick two uniformly random vectors x, y from $\{\pm 1\}^W$.

(2) Pick a *noisy* $z \in \{\pm 1\}^W$ as follows: For each i
– with probability $1 - \rho$, define $z)i = +1$,
– o.w., then $z_i = -1$.

(3) Accepts if:

$$f(x)f(y) = f(xyz).$$

Completeness

If $f = \chi_{\{w\}}$ for some $w \in [W]$, then

- $f(x)f(y) = x_w y_w$
- $f(xyz) = x_w y_w z_w$
- $f(x)f(y) = f(xyz) \iff x_w = 1$, which holds with probability $1 - \rho$.

Soundness - I

Lemma

If the tester accepts with probability $\frac{1}{2} + \delta$, then

$$\sum_{\alpha} \widehat{f}_{\alpha}^{3}(1-2\rho)^{|\alpha|} \geq 2\delta.$$

Suppose the lemma holds.
If $|\alpha|$ is large, $(1-2\rho)^{|\alpha|}$ is negligible. Therefore, there are small α such that $\widehat{f}_{\alpha}$ is large, so f is close to χ_{α}.
For $k = \frac{1}{2\rho}\log\frac{1}{\epsilon}$, if $|\alpha| > k$, then

$$\begin{aligned}(1-2\rho)^{|\alpha|} &< (1-2\rho)^{\frac{1}{2\rho}\log\epsilon^{-1}} \\ &= ((1-2\rho)^{\frac{1}{2\rho}})^{\log\frac{1}{\epsilon}} < (\frac{1}{e})^{\log\frac{1}{\epsilon}} < \epsilon.\end{aligned} \tag{4}$$

Soundness - II

By the lemma,

$$\begin{aligned} 2\delta &\leq \sum_{\alpha} \widehat{f}_{\alpha}^{3}(1-2\rho)^{|\alpha|} \\ &= \sum_{|\alpha|\leq k} \widehat{f}_{\alpha}^{3}(1-2\rho)^{|\alpha|} + \sum_{|\alpha|>k} \widehat{f}_{\alpha}^{3}(1-2\rho)^{|\alpha|} \\ &\leq \max_{|\alpha|\leq k} \widehat{f}_{\alpha} \sum_{\alpha,|\alpha|\leq k} \widehat{f}_{\alpha}^{2}(1-2\rho)^{|\alpha|} + \epsilon \\ &\leq \max_{\alpha,|\alpha|\leq k} \widehat{f}_{\alpha} + \epsilon. \end{aligned} \tag{5}$$

Therefore, there is an α such that $|\alpha| \leq k$, $\widehat{f}_{\alpha} \geq 2\delta - \epsilon$.
f is close to χ_{α}.

Proof of the lemma - I

If the tester accepts with prob $\frac{1}{2} + \delta$, then

$$E[f(x)f(y)f(xyz)] = 2\delta.$$

Let $f = \sum_\alpha \widehat{f}_\alpha \chi_\alpha$.

$$\begin{aligned} 2\delta \leq E_{x,y,z}[(\sum_\alpha \widehat{f}_\alpha \chi_\alpha(x))(\sum_\beta \widehat{f}_\beta \chi_\beta(y))(\sum_\gamma \widehat{f}_\gamma \chi_\gamma(xyz))] \\ = \sum_\alpha \widehat{f}_\alpha^3 E_z[\chi_\alpha(z)]. \qquad (6) \end{aligned}$$

By the choice of z,

$$E_z[\chi_\alpha(z)] = E_z[\prod_{i \in \alpha} z_i].$$

Proof of the lemma - II

By the independence, the later is

$$\prod_{i \in \alpha} E[z_i] = (1 - 2\rho)^{|\alpha|},$$

since $E[z_i] = 1 - 2\rho$. Therefore,

$$2\delta \leq \sum_{\alpha} \widehat{f}_{\alpha}^{3} (1 - 2\rho)^{|\alpha|}.$$

Recall the instance

Assume: For a $2\mathrm{CSP}_W$ instance ϕ, either $\mathrm{val}(\phi) = 1$ or $\mathrm{val}(\phi) \leq 1 - \epsilon$.
Suppose that
(i) ϕ has n variables $x_1, x_2, \cdots, x_n$, taking values in $[W]$,
(ii) for each constraint $\phi_r(x_i, x_j)$, there is a function $h : [W] \to [W]$ such that ϕ_r is satisfied by π if and only if $\pi(j) = h(\pi(i))$.

Bifolded

Observation For $v = (v_1, v_2, \cdots, v_W)$,

$$\chi_{\{w\}}(-v) = -\chi_{\{w\}}(v) = -v_w$$

.

Definition

We say that a function is biofolded, if for all $v \in \{\pm 1\}^W$, $f(-v) = -f(v)$.

Bifolded lemma

Lemma

If $f : \{\pm 1\}^W \to \{\pm 1\}$ is bifolded and $\widehat{f}_\alpha \neq 0$, then $|\alpha|$ is odd. In particular, $|\alpha| \geq 1$.

By definition,

$$\widehat{f}_\alpha = \langle f, \chi_\alpha \rangle = E_v[f(v)\chi_\alpha(v)] = E_v[f(v)\prod_{i\in\alpha} v_i]$$

If $|\alpha|$ is even, then $\chi_\alpha(-v) = \chi_\alpha(v)$, in which case, if f is bifolded, $f(-v) = -f(v)$. Therefore,
$\widehat{f}_\alpha = E_v[f(v)\chi_\alpha(v)] = 0$.
Assume the functions are bifolded.

Hastad's verifier V_H

Assumptions:
1) The proof π is expected to be the assignment $w_1, w_2 \cdots, w_n$ to the variables $v_1, v_2, \cdots, v_n$ such that each w_i is encoded by a bifolded long code.
V_H assumes each $w)i$ is treated as a function $f_i : \{\pm 1\}^W \to \{\pm 1\}$.
2) Randomly picks a constraint $\phi_r(i, j)$ in the $2\mathrm{CSP}_W$ instance.
3) V_H checks:
- f_i, f_j encode two values in $[W]$ that satisfy ϕ_r, i.e., if $f)i$, f_j are the long codes of w, w', then $h(w) = w'$.

V_H - II

For $u \in [W]$, let $h^{-1}(u) = \{w \mid h(w) = u\}$.
For $y \in \{\pm 1\}^W$, $\mathcal{H}^{-1}(y)$ is the string z in $\{\pm 1\}^W$ such that for each $w \in [W]$, the wth bit of the z is $y_{h(w)}$.
V_H proceeds as follows:

1. Pick random v, y from $\{\pm 1\}^W$,
2. Pick a noisy $z \in \{\pm 1\}^W$ by
   – with prob $1 - \rho$, $z_i = +1$,
   – $z_i = -1$, otherwise.
3. Accepts, if

$$f(v)g(y) = f(\mathcal{H}^{-1}(y)vz).$$

Completeness

If ϕ is satisfied, take a satisfying assignment and form a proof for V_H.
Suppose f, g are long codes of w, u with $h(u) = w$. Then

$$f(v)g(y)f(\mathcal{H}^{-1}(y)vz) = v_w y_u y_{h(w)} v_w z_w = z_w \tag{7}$$

V_H accepts with prob $1 - \rho$.

Soundness- I

For $\alpha \subseteq [W]$,

$$h_2(\alpha) = \{u \in [W] \mid |h^{-1}(t) \cap \alpha| \geq 1.$$

Lemma

Let $f, g : \{\pm 1\}^W \to \{\pm 1\}$ be bifolded functions and $h : [W] \to [W]$ such that they pass the test by V_H with prob $\geq \frac{1}{2} + \delta$. Then:

$$\sum_{\alpha \neq \emptyset} \widehat{f}_\alpha^2 \widehat{g}_{h_2(\alpha)} (1 - 2\rho)^{|\alpha|} \geq 2\delta.$$

Soundness - II

Lemma

Suppose that ϕ is a $2\mathrm{CSP}_W$ instance with $\mathrm{val}(\phi) < \epsilon$. If $\rho\delta^2 > \epsilon$, then V_H accepts with prob $< \frac{1}{2} + \delta$.