Reading group: proof of the PCP theorem*

1 The PCP Theorem

The usual formulation of the PCP theorem is equivalent to:

**Theorem 1.** There exists a finite constraint language \( \mathcal{A} \) such that the following problem is NP-hard: given a CSP(\( \mathcal{A} \))-instance \( \Phi \) decide if \( \Phi \) is satisfiable or if every subset of the constraints of size \(|\Phi|/2\) is unsatisfiable.

The problem in the statement is also called GapCSP(\( \mathcal{A} \)).

2 The Label Cover Problem

Let \( \Sigma \) be a finite alphabet. An instance of the label cover problem for \( \Sigma \) is:

- a bipartite graph \((V_1, V_2, E)\),
- for every \((u, v) \in E\), a function \(\pi_{u,v} : \Sigma \rightarrow \Sigma\).

A solution to an instance is a pair of mappings \(s_1 : V_1 \rightarrow \Sigma\) and \(s_2 : V_2 \rightarrow \Sigma\) such that for all \((u, v) \in E\), \(\pi_{u,v}(s_1(u)) = s_2(v)\).

**Proposition 1.** Label cover over a 3-element alphabet is NP-hard.

**Definition 1.** A (strong) Mal’cev condition \((\mathcal{L}, \Sigma)\) where \(\mathcal{L}\) is a finite functional language and \(\Sigma\) is a finite set of identities over \(\mathcal{L}\).

**Example 1.** \(m(x,x,y) \approx m(y,x,x) \approx y\) with \(\mathcal{L} = \{m\}\).

**Definition 2.** A Mal’cev condition \((\mathcal{L}, \Sigma)\) is satisfied in a clone \(\mathcal{C}\) if there is a mapping \(\xi : \mathcal{L} \rightarrow \mathcal{C}\) such that \(\xi(\mathcal{L}) \models \Sigma\).

A Mal’cev condition is said to be trivial if one of the following equivalent statements hold:

1. it is satisfied in the clone of projections,
2. it is satisfied in every clone,

*Notes as of December 4, 2017. Report mistakes to antoine.mottet@tu-dresden.de.
3. it is satisfied in Pol(1-in-3-SAT).

A Mal'cev condition is said to be bipartite if there is a partition $L = L_1 \cup L_2$ such that every identity is of the form $f(\text{variables}) \approx g(\text{variables})$ with $f \in L_1$ and $g \in L_2$. It is special bipartite if it is of the form $f(\text{variables}) \approx g(x_1, \ldots, x_n)$ (all variables are different in the right-hand side).

**Proposition 2.** It is NP-hard to decide whether a height 1 special bipartite Mal'cev condition is trivial.

We first prove that the two problems are equivalent up to polytime reductions.

The translation from the Mal'cev problem to LC($\Sigma$) is as follows. The vertices $(V_1, V_2)$ correspond to $(L_1, L_2)$. A set of identities $E$ gives an edge relation on $V_1 \cup V_2$. Given an edge $f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) \approx g(x_1, \ldots, x_n)$, we take $\pi_{f,g}$ to be $\pi$.

Was the other reduction given?

**Proof of Proposition 2.** We even prove that the even more special case of height 1 bipartite special ternary in two variables is NP-hard.

We reduce 1-in-3-SAT to this problem. Let $V, C$ be an instance of 1-in-3-SAT. We take $L_2$ to be the set of variables. We take $L_1$ to contain one symbol $f_C$ for each constraint $C(x_{i_1}, x_{i_2}, x_{i_3})$ in $C$. We add the equalities $f_C(x, x, y) \approx g_{i_3}(x, y)$, $f_C(x, y, x) \approx g_{i_2}$, and $f_C(y, x, x) \approx g_{i_1}$. □

**Definition 3.** The GapLabelCover$_\epsilon$($\Sigma$) problem is as follows: given an LC($\Sigma$)-instance, decide if it is solvable, or if no $\epsilon$-part is solvable.

**Theorem 2.** For all $\epsilon > 0$, there exists $\Sigma$ such that GapLabelCover$_\epsilon$($\Sigma$) is NP-hard.

Be convinced that PCP implies that there exist $\epsilon \in (0, 1)$ and $\Sigma$ such that GapLabelCover$_\epsilon$($\Sigma$) is NP-hard. Parallel repetition (no time to formalize) gives a way to turn $\epsilon$ into any number in $(0, 1)$.

### 3 Expander graphs: Marcello Mamino

“I only have two hours to talk so let’s get on with it.”

Marcello Mamino

We want to prove: fix finite domain $\Sigma$ and let $\Gamma$ be the full binary constraint language on $\Sigma$. We prove: the classical problem CSP($\Gamma$) reduces in polynomial-time to GapCSP($\Gamma$).

More precisely. Let $\Phi$ be an instance of CSP($\Gamma$) that is unsatisfiable, but a big portion of the constraints are simultaneously satisfiable. We want to construct a new instance $\Psi$ such that at most half of the constraints are satisfiable. Let $n$ be the number of constraints of $\Phi$. The gap of $\Phi$ is the smallest number...
\[ \alpha \in [0,1] \] such that a part of \( \Phi \) of size \((1 - \alpha)n\) is satisfiable. If \( \Phi \) is not satisfiable, the gap is \( > 0 \). We amplify this gap by multiplying it repeatedly by a constant \( k \), which is meant to be independent of the size of \( \Phi \).

At each step, suppose that our instance grows by a factor of \( h \) (independent of \(|\Phi|\) as well). This means that the size of the instance grows as \( h^{\text{number of steps}} \sim n^{1 \log h(k)} \).

**Strategic goal:** \( \exists \Sigma, k > 1, h, \alpha \) such that we can effectively translate an instance of \( \text{CSP}(\Gamma) \) of gap \( x < \alpha \) to one of gap \( xk \) and size not larger than \( h \times \) original size.

We define the **product** of two instances \( \Phi_1(\pi) \) and \( \Phi_2(\eta) \). It contains as variables \( x_1, \ldots, x_n \) and \( y_1, \ldots, y_m \) and constraints \( R(\pi') \land S(\eta') \) (of arity \( \text{len}(\pi') + \text{len}(\eta') \)) for every pair of constraint \( R(\pi') \) and \( S(\eta') \) from \( \Phi_1 \) and \( \Phi_2 \).

**Claim.** If \( \alpha \) is the gap of \( \Phi_1 \) and \( \Phi_2 \), then gap of the product is \( 1 - (1 - \alpha)^2 \).

**Proof.** Easy, just project on each coordinate, this gives subsets of each instance with relative size at most \((1 - \alpha)\). 

This proves that once we manage to go from a gap that depends on \( \Phi \) to the \( \alpha \) from the statement (which is a constant), then we can also go to \( \frac{1}{2} \) by iterated squaring (a constant number of times).

Let’s now go back to the strategic goal. One step to reduce the gap is composed of the following substeps:

1. Regularize the graph (i.e., turn it into an **expander**).
2. Increase the gap (this causes the domain size of increase).
3. Shrink the domain.

Expanders are used at every step of this strategy.

**Definition 4** (Expansion ratio). Let \( G \) be a graph. The **edge expansion ratio** of \( G \), denoted by \( h(G) \), is defined as

\[
\min_{S \subseteq G, |S| \leq |V(G)|} \frac{|E(S, \overline{S})|}{|S|},
\]

where \( E(S, \overline{S}) \) is the set of edges with one endpoint in \( S \) and the other endpoint in \( \overline{S} \).

Little game of the expanders: find infinite families of \( d \)-regular graphs with \( h(G) \geq \alpha > 0 \). It’s easy to build such a family by a probabilistic argument, but we would like to compute them efficiently and deterministically.

Let \( M(G) \) be the adjacency matrix of a \( d \)-regular graph \( G \). This is a symmetric matrix with nonnegative integer entries, where the entry \((v, w)\) for \( v, w \in G \) counts the number of edges between \( v \) and \( w \). Take \( \frac{1}{d} M(G) \), which is a bistochastic matrix. Being a symmetric real matrix, it is diagonalisable as \( A \times \text{diag}(1, \lambda_2, \ldots, \lambda_{|G|}) \times A^{-1} \) with \( 1 \geq \lambda_2 \geq \cdots \geq \lambda_{|G|} \) being the eigenvalues of \( \frac{1}{d} M(G) \).
Exercise. Remember that the spectral radius of a stochastic matrix is precisely 1. Prove that \(-1\) is an eigenvalue iff the graph is bipartite.

Definition 5. The spectral gap of \(G\) is defined to be \(1 - \lambda_2\). We also also define it as \(\min(1 - |\lambda_2|, 1 - |\lambda_G|)\).

Remark: if \(v\) is a probability distribution on \(V(G)\), a random walk with \(n\) steps gives the distribution \((\frac{1}{2}M(G))^nv\), and the matrix \((\frac{1}{2}M(G))^n\) looks like \(A \text{ diag}(1, \lambda_2, \ldots, \lambda_{n_G}) A^{-1}\), where the diagonal converges quickly to \(\text{diag}(1, 0, \ldots, 0)\).

Theorem 3. For every \(d\)-regular finite graph \(G\) with second greatest associated eigenvalue \(\lambda_2\), we have

\[
d\frac{1 - \lambda_2}{2} \leq h(G) \leq d\sqrt{1 - \lambda_2}.
\]

Proof. Part 1: We prove the second inequality. Construct the matrix \(N\) with rows \(V\) and columns \(E\). Fix an arbitrary orientation on \(G\). For each edge \(e = (v, w)\), we put \(-1\) in \(N\) at position \(n_{v,e}\) and 1 at position \(n_{w,e}\).

Let \(f: V \to \mathbb{R}\) be a column vector. Then \(\|f^T N\|_2^2 = \sum_{(i,j) \in E(G)} |f(i) - f(j)|^2\). Define \(B_f := \sum_{(i,j) \in E(G)} |f(i) - f(j)|^2\). We prove that

\[
\|f\|_2^2 h(G) \leq B_f \leq \sqrt{2d} \|f^T N\|_2 \cdot \|f\|_2
\]

holds when the support of \(f\) has size at most \(\frac{n}{2}\) and is nonnegative. Then by choosing \(f\) appropriately, this proves the second inequality.

We prove \(\|f\|_2^2 h(G) \leq B_f\). Let \(\beta_0, \ldots, \beta_r\) be an enumeration of the image of \(f\) where \(\beta_0 < \cdots < \beta_r\). Note that \(\beta_0 = 0\), since the support of \(f\) is not the whole \(V\). Let \(V_i\) be the set of \(x \in V(G)\) such that \(f(x) \geq \beta_i\). We have \(V(G) = V_0 \supseteq V_1 \supseteq \cdots \supseteq V_r\).

Claim. \(B_f\) is equal to \(\sum_{i=1}^r \|E(V_i, \overline{V_i})\| \times (\beta_i^2 - \beta_{i-1}^2)\).

Proof. Quite clear. \(\Box\)

Now, \(\sum_{i=1}^r \|E(V_i, \overline{V_i})\| \times (\beta_i^2 - \beta_{i-1}^2) \geq h(G) \sum_{i=1}^r |V_i| \times (\beta_i^2 - \beta_{i-1}^2),\) where we use the fact that \(|V_i| \leq \frac{|V(G)|}{r}\). We can rewrite this as \(h(G) \sum_{i=1}^r \beta_i^2 (|V_i| - |V_{i+1}|),\) if we define \(V_{r+1} := \emptyset\). Finally, we note that this is simply equal to \(h(G)\) \(\|f\|_2\).

On to prove \(B_f \leq \sqrt{2d} \|f^T N\|_2 \cdot \|f\|_2\). But this is just stupid computations:

\[
B_f = \sum_{(x,y) \in E} |f(x) - f(y)| \cdot |f(x) + f(y)|
\]

\[
\leq \sqrt{\sum (f(x) - f(y))^2 \cdot \sum (f(x) + f(y))^2}
\]

\[
\leq \|f^T N\|_2 \cdot \sqrt{2} \sum f(x)^2 + f(y)^2
\]

\[
\leq \|f^T N\|_2 \cdot \sqrt{2d} \|f\|_2.
\]
What we just proved is that
\[ h(G) \leq \sqrt{2d} \frac{\|f^T N\|}{\|f\|} \]
holds for every nonnegative function \( f : V \to \mathbb{R} \) with support of size at most \(|V|/2\). Let \( g \) be an eigenvector associated with the eigenvalue \( \lambda_2 \). Define \( f := g^+ \), i.e., the vector that is like \( g \) when it is nonnegative and is 0 otherwise. If the support of \( f \) is too big, just pick \( g' := -g \) and do the same. Define another matrix \( L := N \times N^T \) of size \(|V(G)|^2\). The matrix \( L \) has \( d \)'s on the diagonal and at position \( i,j \) is \(-1\times\)number of edges connecting \( i \) and \( j = -dm_{i,j} \). Therefore, \( L = dI - dM \).

Let \( x \) be in the support of \( f \). We compute
\[
(Lf)(x) = d \cdot f(x) - \sum_{y \in V(G)} d \cdot M_{x,y} f(y)
= d \cdot g(x) - \sum_{y \in supp(f)} dM_{x,y} g(y)
\leq (Lg)(x)
= (dg - d\lambda_2 g)(x)
= d(1 - \lambda_2)g(x).
\]

This is amazing, because it gives \( \|f^T N\|^2 = f^T N N^T f = f^T L f = (f^T L|_{supp(f)}) \cdot f = \|f^T L|_{supp(f)}\| \cdot \|f\| \leq d(1 - \lambda_2)\|f\|^2 \). So, in the inequality at the top of the page, we obtain \( h(G) \leq \ldots \).

**Part 2:** let us now prove the first inequality. By rearranging, we want to prove \( d\lambda_2 \geq d - 2h(G) \). First, it suffices to prove that there exists \( f : V \to \mathbb{R} \) that is orthogonal to \( \left( \begin{array}{c} 1 \\ \vdots \\ 1 \end{array} \right) := 1_V \) and such that we have \( d\frac{f^T M f}{\|f\|^2} \geq d - 2h(G) \).

Indeed, suppose that we have such an \( f \) where the value of the fraction is \( \alpha \). Let \( A \) be orthogonal and such that \( A^T M A \) is diagonal. Let \( g := A^T f \). The first observation is that the first component of \( g \) is 0 (trivial). Then just compute.

Let \( S \) be a set witnessing the edge-expansion ratio. Define \( f := |S|1_S - |S|1_S \). It is indeed orthogonal to \( 1_V \) and then it is simple computation. The denominator of the fraction is \( \|f\| = |S|^3 \cdot |S| + |S|^2 \cdot |S| = (|S| + |S|) \times |S| = |n|S||\bar{S}| \). Note that \( f \) can be written as \( n1_S - |S|1_V \) and also as \(-n1_S + |S|1_V \). The numerator of the fraction is then
\[
f^T dM f = (n1_S - |S|1_V)^T M (-n1_S + |S|1_V)
= -n^21_S^T dM 1_S + n|S|1_S^T dM 1_V + n|S|1_V^T dM 1_S - |S||\bar{S}|1_S^T dM 1_V
= -n^2 |E(S, S)| + nd|\bar{S}| |S| + nd|S| |\bar{S}| - |S||\bar{S}|n \cdot d
= nd|S||\bar{S}| - n^2 h(G)|S|.
\]
The fraction is then
\[ \frac{dT\| f \|_2}{\| f \|_2} = \frac{nd\|S\| \|S\| - n^2|E(S, S)|}{n\|S\| \|S\|} \]
\[ = d - \frac{nh(G)}{|S|} \]
\[ \geq d - 2h(G). \]

This concludes the proof.

Let us now see a construction of an infinite family of expanders!

**Definition 6.** A graph \( G = (V, E) \) is an \((n, d, \alpha)\)-expander if it is \( d \)-regular, \(|V| = n\) and all the associated eigenvalues, except for 1 are bounded above in absolute value by \( \alpha \).

We define the zigzag product of two graphs. Let \( G \) be an orange graph that is \((n, m, \alpha)\) and \( H \) be a blue graph that is \((m, d, \beta)\). We build \( G \otimes H \) by first exploding every orange vertex by \( m \) vertices and then pasting arbitrarily a copy of \( H \) inside. The zigzag product is then the graph on this vertex set and where there is an edge \((x, y)\) if there is a blue edge from \( x \) to \( z \), an orange edge from \( z \) to \( w \), and a blue edge from \( w \) to \( y \).

**Theorem 4.** \((n, m, \alpha) \otimes (m, d, \beta) = (n \cdot m, d^2, f(\alpha, \beta))\), where \( f(\alpha, \beta) \leq \alpha + \beta + \beta^2 \). Moreover, if \( \alpha, \beta < 1 \), then \( f(\alpha, \beta) < 1 \).

**Proof.**

How to use this. Let \( H \) be a \((d^4, d^2, 1/2)\) expander. Let \( G_1 := H^2 \), where \( H^2 \) is the graph definable in \( H \) by \( E \circ E \). \( G_1 \) is a \((d^4, d^2, \leq 1/2)\) expander. Now define \( G_{n+1} := (G_n)^2 \otimes H \).

Claim: \( G_{n+1} \) is a \((d^{4n}, d^4, 1/2)\) expander. Indeed, \( (G_n)^2 \) is \((d^{4n}, d^4, 1/4)\). Then by the property of the zigzag, we obtain a \((d^{4(n+1)}, d^4, 1/4 + 1/4 + 1/4 \leq 1/2)\) expander.

End of the proof, followed by a philosophical discussion about the degree of a vertex that has a loop.