# Lecture 1

Lecturer: Irit Dinur
Preliminary Scriber: Karthik C. S.
Scribe Upgrader: Inbal Livni

We would like to address the bottleneck of constructing good PCPs using Expander graphs. We note at the high level, that we do not know how to randomly construct good PCPs, and similarly, we do not know how to randomly construct high dimensional expanders. We feel that this might not be a coincidence.

PCPs (Probabilistically Checkable Proofs), historically are related to **NP**(Needs Proof). We will illustrate the PCP theorem using the **NP**-hard problem, "3-coloring". Here, we are given a graph $G(V, E)$, and the task is to determine if there is a coloring assignment to the vertices of $V$ using three colors, so that no edge in $E$ is colored monochromatically (i.e., there is no edge both of whose vertices have the same color). It is clearly in **NP**. It is additionally, **NP**-hard. We can think of the requirement of the monochromaticity of the edge as a constraint over the two vertices. Therefore, we can think of the 3-coloring problem as a set of constraints over $\{1, 2, 3\}$ to pairs of vertices. The PCP theorem states that it is **NP**-hard to even find an assignment to the vertices that satisfy 99% of the constraints. In other words, if there was an *efficient* algorithm to find an assignment to the vertices such that at most 1% of the edges are monochromatically colored then, **P**=**NP**.

We are given a graph $G(V, E)$, and a proof $c : V \to \{1, 2, 3\}$ which is a coloring of the vertices, proving that $G$ is 3-colorable. Consider a verifier, who only reads a small part of the proof (chosen at random). Formally, we have the following verification procedure: pick an edge in the graph uniformly at random, and check if it is not monochromatic. We would like a result of the following type to hold: if $G$ is 3-colorable then the probability that the verifier says the graph is 3-colorable should be 1; on the other hand if $G$ was not 3-colorable then the verifier should say that the graph $G$ is not 3-colorable with some constant probability. However, a priori, if $G$ was not 3-colorable then the verifier can say that the graph $G$ is not 3-colorable with probability only equal to $1/|E|$ (in the worst-scenario). The PCP theorem says that there is a transformation such that in the PCP transformed proof, the former, stronger requirements hold.

Such a transformation can be seen as a gap amplification, wherein we start from a graph $G(V, E)$, with value 1 or value less than 1 (here value corresponds to the maximum fraction of non-monochromatic edges over all possible assignments). We would like to construct $H(V', E')$, such that the value is 1 or the value is less than 0.95.

This PCP transformation can be thought of as using an error-correcting code: a difference of even just 1 bit in the message space, translates to a non-trivial hamming distance in the encoded message space. For example let $G_0$ be a 3 colorable graph and then pick any 4 vertices in $G_0$ and add all the edges between the 4 picked vertices to obtain a new graph $G_1$ which is not 3-colorable. If we look locally at parts of $G$ and $G'$, in every place not containing these 4 vertices they look identical. However, the same PCP transformation on both these graphs

should amplify the non-3-colarability of $G_1$ where as preserve the 3-colorability in $G_0$. We hope that at this point the reader is convinced of the non-triviality of the existence of such a transformation.

A naive idea for constructing PCPs is to cover $G$ by many "small" subsets, and construct $H$ by having a vertex for each of the subsets. In this case $|V'| = \binom{n}{k}$, where $k$ is the cardinality of the subsets introduced. We introduce an edge in $H$ if the corresponding subsets in $G$ substantially overlap. However, the analysis of such a reduction is not clear. Instead, we consider a reduction from the graph 3-coloring problem $G$ to an agreement problem on the graph (i.e., complex) $H$. An assignment for $G$ is $c : V(G) \to \{1, 2, 3\}$. An assignment for $H$ is for all subsets $S$, a function $f(S) : S \to \{1, 2, 3\}$. In other words, an assignment for $H$ is $f : X(k-1) \to \{1, 2, 3\}^k$. The constraints in $H$ are that if $S_1, S_2 \in X(k-1)$, and $S_1$ and $S_2$ substantially overlap then the constraint on the edge is satisfied if their assignments to the vertices in the intersection are in agreement, and for every subset $S$ the coloring induced by $f(S)$ leads to no monochromatic edge.

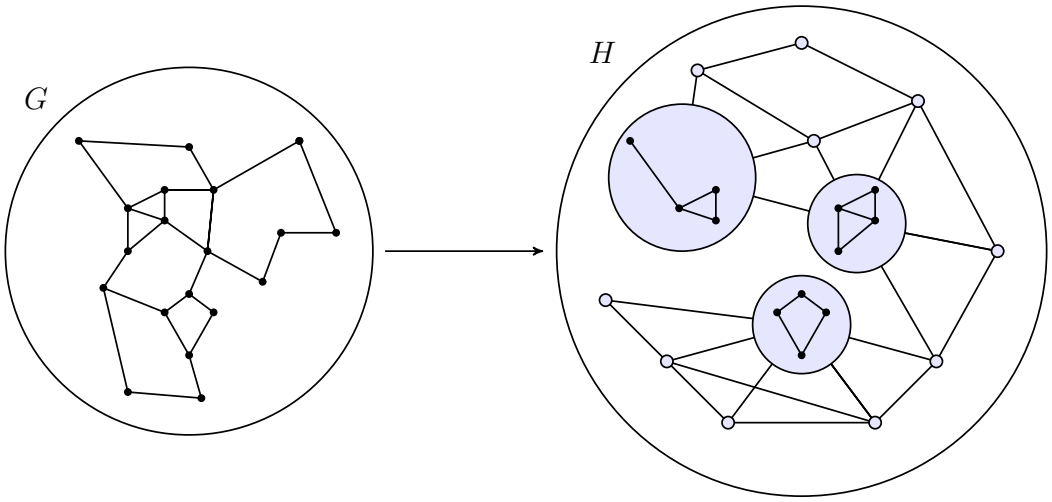


Figure 1: Each vertex in $H$ is a neighborhood of size $k$ of a vertex in $G$, as can be seen in the purple circles.

More formally, we defined the following,

**Definition 1.** *Let $\Sigma$ be the set $\{1, 2, 3\}$. Let $a_0(X, \Sigma) = \{c : X(0) \to \Sigma\}$ denote the assignment to the vertices. We generalize, and define:*

$$\mathfrak{a}_i(X, \Sigma) = \left\{ f : X(i) \to \Sigma^{i+1} \mid \forall S, f(S) : S \to \Sigma \right\}.$$

We can relate such assignments to the coboundary operator we had seen previously. More precisely we have the following,

**Definition 2.**

$$U : \mathfrak{a}_i(X, \Sigma) \to \mathfrak{a}_{i+1}(X, \Sigma),$$

*wherein $\forall S \in X(i)$, we have $Uf(S)$ is an assignment to the elements of $S$, i.e., $\forall u \in S$, $Uf(S)(u) = f(u)$.*

In other words, if we have a valid partial coloring for level $i$, then a coboundary operator is well defined to color the simplices at level $i + 1$. However, if the coloring at level $i$ is not valid,

then we are stuck. We will look at this more closely below:

Given $f \in \mathfrak{A}_{k-1}(X, \Sigma)$, we define an agreement parameter denoted by $\alpha_t(f)$, which is the probability that $f(S_1)$ and $f(S_2)$ agree on $T$, where we have selected $T \in X(t)$ uniformly at random, followed by the selection of $S_1$ and $S_2$ (both in $X(k-1)$) uniformly and independently at random, such that both of $S_1$ and $S_2$ contain $T$. We have the following claim.

**Claim 3.** *If $f \in \mathfrak{A}_i(X, \varepsilon)$ and $\alpha_{i-1}(f) = 1$ then,*

- *$Uf$ can be defined.*
- *$Df$ can be defined, whereas $D : \mathfrak{A}_i(X, \Sigma) \to \mathfrak{A}_{i-1}(X, \Sigma)$ is the partial assignment to the facets.*