Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

### Course "Proofs and Computers", JASS'06

## PCP-Theorem by Gap Amplification

Bernhard Vesenmayer

Faculty of Mathematics TU Munich

March 29, 2006

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

### Preprocessing

Constant degree Expanderizing Preprocessing

### Powering

Assignments N(e) Two Cases

## Composition

Preparation Composition Properties

## Main Theorem Proof of the Main Theorem Proof of PCP Theorem

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

# Preprocessing

In this step we want to transform a given constraint graph into a 'nice' one. That means for the resulting graph G' should hold:

- 1. G' is of constant degree d, i.e. independent of the input graph G,
- 2. G' is d-regular with self-loops, and  $\lambda(G') \leq \lambda < d$ ,
- 3.  $\beta_1 \cdot \text{UNSAT}(G) \leq \text{UNSAT}(G') \leq \text{UNSAT}(G).$

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	00000	0	0	0	
	000	0000000	0		
	0	00	0		
Constant de	gree				

## Constant degree

## Proposition 1 (Constant degree)

Any constraint graph  $G = \langle (V, E), \Sigma, \mathscr{C} \rangle$  can be transformed into a  $(d_0 + 1)$ -regular graph  $G' = \langle (V', E'), \Sigma, \mathscr{C}' \rangle$  such that |V'| = 2|E| and

## cUNSAT(G) $\leq$ UNSAT(G') $\leq$ UNSAT(G)

for some global constants  $d_0, c > 0$ .

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	00000 000 0	0 0000000 00	0 0	0	
Constant de	gree				

1. Let  $X_n$  be a  $d_0$ -regular expander on n vertices with  $h(X_0) > h_0$ .

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	00000 000 0	0 0000000 00	0	0	
Constant deg	gree				

- 1. Let  $X_n$  be a  $d_0$ -regular expander on n vertices with  $h(X_0) > h_0$ .
- 2. Let  $d_v$  be the degree of v. Replace v by  $X_{d_v}$ , equipped with equality constraints, denoted by [v]. Let  $E_1$  be the set of such edges.

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	00000 000 0	0 0000000 00	0 0	0	
Constant de	gree				

- 1. Let  $X_n$  be a  $d_0$ -regular expander on n vertices with  $h(X_0) > h_0$ .
- 2. Let  $d_v$  be the degree of v. Replace v by  $X_{d_v}$ , equipped with equality constraints, denoted by [v]. Let  $E_1$  be the set of such edges.
- For every (u, v) ∈ E put an edge between one vertice of [u] and [v], such that each vertice only sees one such 'external' edge. Let E<sub>2</sub> be the set of those edges.

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
		0 0000000 00	0 0	0	
Constant deg	gree				

- 1. Let  $X_n$  be a  $d_0$ -regular expander on n vertices with  $h(X_0) > h_0$ .
- 2. Let  $d_v$  be the degree of v. Replace v by  $X_{d_v}$ , equipped with equality constraints, denoted by [v]. Let  $E_1$  be the set of such edges.
- For every (u, v) ∈ E put an edge between one vertice of [u] and [v], such that each vertice only sees one such 'external' edge. Let E<sub>2</sub> be the set of those edges.
- 4. Define  $G' := ([V], \mathbf{E} = E_1 \cup E_2)$ , where  $[V] := \cup_{v \in V} [v]$ .

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	00000	0	0	0	
	000	0000000	0		
	0	00	0		
Constant de	gree				

## Properties: Upper bound

- 1. Let  $\sigma: V \to \Sigma$  be a best assignment of G.
- 2. Define  $\sigma' : [V] \to \Sigma$  by:  $\forall v \in V, x \in [v] : \sigma'(x) = \sigma(v)$

 $\Rightarrow \mathrm{UNSAT}(\mathcal{G}) = \mathrm{UNSAT}_{\sigma}(\mathcal{G}) \geq \mathrm{UNSAT}_{\sigma'}(\mathcal{G}') \geq \mathrm{UNSAT}(\mathcal{G}')$ 

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
		0 0000000 00	0 0	0	

### Constant degree

## Properties: Lower bound

- 1. Let  $\sigma': [V] \to \Sigma$  be a best assignment.
- 2. Define  $\sigma: V \to \Sigma$  by:  $\sigma(v) := \max_{a \in \Sigma} (P_{x \in [v]}(\sigma'(x) = a))$
- 3. Let  $F \subset E$ ,  $\mathbf{F} \subset \mathbf{E}$  be the set of edges that reject  $\sigma, \sigma'$ .
- 4. Let  $S := \bigcup_{v \in V} \{x \in [v]; \sigma'(x) \neq \sigma(v)\}.$

$$\Rightarrow |\mathbf{F}| + |S| \ge |F| = \alpha \cdot |E|, \text{ where } \alpha := \frac{|F|}{|E|}.$$

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000	0	0	0	
	000	0000000	0		
	0	00	0		
Constant de	gree				

## Properties: Lower bound - Two cases

We have to distinguish between two cases:

- 1.  $|\mathbf{F}| \ge \frac{\alpha}{2} |E|$
- 2.  $|\mathbf{F}| < \frac{\alpha}{2}|E|$

The first case is simple:

$$\begin{aligned} |\mathbf{F}| &\geq \frac{\alpha}{2} |E| = \frac{\alpha}{2d} |\mathbf{E}| \\ \Rightarrow \text{UNSAT}(G') &= \text{UNSAT}_{\sigma'}(G') \\ &\geq \frac{1}{2d} \text{UNSAT}_{\sigma}(G) \\ &\geq \frac{1}{2d} \text{UNSAT}(G). \end{aligned}$$

Outline	Preprocessing 00000 000	Powering 0 0000000	Composition 0 0	Main Theorem 0	Proof of PCP Theorem
	0	00	0		
Constant dee	ree				

## Properties: Lower bound - Two cases

Second case:  $|\mathbf{F}| < \frac{\alpha}{2} |E| \Rightarrow |S| \ge \frac{\alpha}{2} |E|$ . Define the following: 1.  $S^{v} := [v] \cap S$ 2.  $S_{a}^{v} := \{x \in S^{v}; \sigma'(x) = a\}$ 3.  $|S_{a}^{v}| \le \frac{|[v]|}{2} \Rightarrow |E(S_{a}^{v}, [v] \setminus S_{a}^{v})| \ge h_{0} \cdot |S_{a}^{v}|$ 4.  $|\mathbf{F}| \ge \sum_{v \in V} \sum_{a \in \Sigma} h_{0} |S_{a}^{v}| = h_{0} |S| \ge h_{0} \frac{\alpha}{2} |E| = \frac{h_{0}\alpha}{2d} |\mathbf{E}|$ 

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000	0	0	0	
	000	0000000	0		
	0	00	0		

# Expanderizing

## Proposition 2 (Expanderizing)

Let  $d_0, h_0 > 0$  be some global constants. Any d-regular constraint graph G can be transformed into G' such that

1. 
$$G'$$
 is  $(d + d_0 + 1)$ -regular, has self-loops, and  
 $\lambda(G') \le d + d_0 + 1 - \frac{h_0^2}{d + d_0 + 1} < \deg(G')$ ,  
2.  $\operatorname{size}(G') = O(\operatorname{size}(G))$  and

2. 
$$size(G') = O(size(G))$$
, and

3. 
$$\frac{d}{d+d_0+1}$$
 · UNSAT(G)  $\leq$  UNSAT(G')  $\leq$  UNSAT(G).

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000	0 0000000 00	0	0	

1. Let 
$$E_{loop} := \{(v, v); v \in V\}.$$

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
		0 0000000 00	0	0	

## Construction of G'

1. Let 
$$E_{loop} := \{(v, v); v \in V\}.$$

2. Let X = (V, E') be a  $d_0$ -regular expander on |V| vertices with  $h(X) \ge h_0$ .

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000	0	0	0	
	000	0000000	0		
	0	00	0		

- 1. Let  $E_{loop} := \{(v, v); v \in V\}.$
- 2. Let X = (V, E') be a  $d_0$ -regular expander on |V| vertices with  $h(X) \ge h_0$ .
- 3. Define  $G' = (V, E \cup E' \cup E_{loop})$  with trivial constraints on the new edges.

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

## Properties

1. G' is  $(d + d_0 + 1)$ -regular and of the same size as G.

2. 
$$\lambda(G') \leq d + d_0 + 1 - \frac{h(G')^2}{d(G')} \leq d + d_0 + 1 - \frac{h_0^2}{d + d_0 + 1} < d + d_0 + 1$$

3. The fraction of unsatisfied edges drops at most by  $\frac{d}{d+d_0+1}$ .  $\Box$ 

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 •	0 0000000 00	0 0	0	

#### Preprocessing



## Lemma 1 (Preprocessing)

There exist constants  $0 < \lambda < d$  and  $\beta_1 > 0$  such that any constraint graph G can be transformed into a constraint graph G', denoted G' = prep(G), such that

- 1. G' is d-regular with self-loops, and  $\lambda(G') \leq \lambda < d$ .
- 2. G' has the same alphabet as G, and size(G') = O(size(G)).
- 3.  $\beta_1 \cdot \text{UNSAT}(G) \leq \text{UNSAT}(G') \leq \text{UNSAT}(G)$ .

*Proof.* Consecutively apply the previous two propositions.

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0	0	

In this step we amplify the satisfiability gap. Let G be a given constraint graph. Consider the graph  $G^t$  which is defined as follows:

1. The vertices of  $G^t$  are the same as the vertices of G

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0	0	

In this step we amplify the satisfiability gap. Let G be a given constraint graph. Consider the graph  $G^t$  which is defined as follows:

- 1. The vertices of  $G^t$  are the same as the vertices of G
- 2. *u* and *v* are connected by *k* edges in **E** iff the number of *t*-step paths from *u* to *v* in *G* is exactly *k*.

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0	0	

In this step we amplify the satisfiability gap. Let G be a given constraint graph. Consider the graph  $G^t$  which is defined as follows:

- 1. The vertices of  $G^t$  are the same as the vertices of G
- 2. *u* and *v* are connected by *k* edges in **E** iff the number of *t*-step paths from *u* to *v* in *G* is exactly *k*.
- 3. The alphabet of  $G^t$  is  $\Sigma^{d^t}$ , where every vertex specifies values for all its neighbours reachable in t steps.

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

In this step we amplify the satisfiability gap. Let G be a given constraint graph. Consider the graph  $G^t$  which is defined as follows:

- 1. The vertices of  $G^t$  are the same as the vertices of G
- 2. *u* and *v* are connected by *k* edges in **E** iff the number of *t*-step paths from *u* to *v* in *G* is exactly *k*.
- 3. The alphabet of  $G^t$  is  $\Sigma^{d^t}$ , where every vertex specifies values for all its neighbours reachable in t steps.
- 4. The constraint associated with an edge  $\mathbf{e} = (u, v) \in \mathbf{E}$  is satisfied iff the assignments for u and v are consistent with an assignment that satisfies all of the constraints induced by the t neighbourhoods of u and v.

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

## Lemma 2 (Powering)

Let  $\lambda < d$ , and  $|\Sigma|$  be arbitrary constants. 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  $G = \langle (V, E), \Sigma, \mathscr{C} \rangle$  with self-loops and  $\lambda(G) \leq \lambda$ 

UNSAT
$$(G^t) \geq \beta_2 \sqrt{t} \cdot \min\left(UNSAT(G), \frac{1}{t}\right)$$

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	• 0000000 00	0 0 0	0	
A					

# Assignments

- 1. Let  $\tilde{\sigma}$  be a best assignment for  $G^t$ , i.e. UNSAT $_{\tilde{\sigma}}(G^t) = \text{UNSAT}(G^t)$ .
- 2. Let  $\tilde{\sigma}(v)_w$  denote the value that is specified for w by v.
- 3. For every  $1 \le j \le t$  and  $v \in V$  let  $X_{v,j}$  be a random variable with distribution

$$P(X_{v,j} = a) := \frac{\# \text{ j-step from } v \text{ to some } w \text{ with } \tilde{\sigma}(w)_v = a}{\# \text{ j-step paths starting at } v}$$

4. Now define  $\sigma: V \to \Sigma$  as follows:

$$\sigma(\mathbf{v}) := \operatorname{maxarg}_{\mathbf{a} \in \boldsymbol{\Sigma}}(P(X_{\mathbf{v}, \frac{t}{2}} = \mathbf{a}))$$

Outline	Preprocessing 000000 000 0	Powering ○ ●○○○○○○○	Composition 0 0	Main Theorem O	Proof of PCP Theorem
N(e)					

# $N(\mathbf{e})$

- 1. Let  $F \subset E$  be a subset of the edges that reject  $\sigma$ , such that  $\text{UNSAT}(G) = \frac{|F|}{|E|}$ .
- 2. Let  $I_r := \{\frac{t}{2} r < i \le \frac{t}{2} + r\}.$
- 3. For each  $\mathbf{e} = (v_0, \dots, v_t) \in \mathbf{E}$  define the following random variable

$$N_{i}(\mathbf{e}) := \begin{cases} 1 & \text{if } (v_{i-1}, v_{i}) \in F \land \tilde{\sigma}(v_{0})_{v_{i-1}} = \sigma(v_{i-1}) \\ & \land \tilde{\sigma}(v_{t})_{v_{i}} = \sigma(v_{i}) \\ 0 & \text{otherwise} \end{cases}$$
$$N(\mathbf{e}) := \sum_{i \in I_{r}} N_{i}$$

Then  $\text{UNSAT}_{\tilde{\sigma}}(G^t) \geq P(N > 0) \geq \frac{E^2(N)}{E(N^2)}$ .

Outline	Preprocessing 000000 000 0	Powering ○ ○●○○○○○○ ○○	Composition 0 0	Main Theorem O	Proof of PCP Theorem
N(e)					

1. By definition we have:  $E(N) = \sum_{i \in I_r} E(N_i) = \sum_{i \in I_r} P(N_i > 0).$ 2. We can gain the probability of  $P(N_i > 0)$  as follows:  $P(N_i > 0) = P((u, v) \in F)P(X_{u,i-1} = \sigma(u))P(X_{v,t-i} = \sigma(v))$ 

$$= \frac{|F|}{|E|} P(X_{u,i-1} = \sigma(u)) P(X_{v,t-i} = \sigma(v))$$

3. For any  $l \in I_r$  we can decompose as follows  $(B_{l,p})$  is binomially distributed with  $p = 1 - \frac{1}{d}$  and  $X'_{u,k}$  is defined like  $X_{u,k}$  but without loops):

$$P(X_{u,l} = \sigma(u)) = \sum_{k=0}^{l} P(B_{l,p} = k) P(X'_{u,k} = \sigma(u)),$$

Outline	Preprocessing 000000 000 0	O ○ ○ ○ ○ ○ ○ ○ ○	Composition 0 0	Main Theorem O	Proof of PCP Theorem
N(e)					

Now we need the following technical proposition, stating the distribution of  $B_{l_1}$  and  $B_{l_2}$  are quite similar:

## Proposition 3

For every  $p \in [0,1]$  and c > 0 there exists some  $0 < \tau \le 1$  such that if  $|l_1 - l_2| \le (\sqrt{l_1} \land \sqrt{l_2})$ , then

$$\tau \leq \frac{P(B_{l_1,p}=k)}{P(B_{l_2,p}=k)} \leq \frac{1}{\tau} \quad \forall k, |k-pl_1| \vee |k-pl_2| \leq c(\sqrt{l_1} \wedge \sqrt{l_2})$$

1. Define 
$$J := \{k \in \mathbb{N}; |k - pl| \lor |k - p\frac{t}{2}| \le c(\sqrt{\frac{t}{2}} \land \sqrt{l})\}.$$

2. Choose c such that  $P(B_{\frac{t}{2},p} \notin J) \leq \frac{1}{2|\Sigma|}$ .

Outline	Preprocessing 000000 000 0	O ○ ○ ○ ○ ○ ○ ○ ○	Composition 0 0	Main Theorem O	Proof of PCP Theorem
N(e)					

- 1. By construction of  $\sigma$  we have  $P(X_{u,\frac{t}{2}} = \sigma(u)) \geq \frac{1}{|\Sigma|}$ .
- 2. Apply the proposition with  $r := -\frac{3}{2} + \frac{1}{2}\sqrt{1+2t}$  (then the condition  $|l_1 l_2| \le \sqrt{l_1} \land \sqrt{l_2}$  is met) and with  $l_1 = \frac{t}{2}, l_2 = i 1$ :

$$P(X_{u,i-1} = \sigma(u)) \geq \sum_{k \in J} P(B_{i-1,p} = k) P(X'_{u,k} = \sigma(u))$$
  
$$\geq \tau \cdot \sum_{k \in J} P(B_{\frac{t}{2},p} = k) P(X'_{u,k} = \sigma(u))$$
  
$$\geq \tau (P(X_{u,\frac{t}{2}} = \sigma(u)) - \frac{1}{2|\Sigma|})$$
  
$$\geq \frac{\tau}{2|\Sigma|}$$

Outline	Preprocessing 000000 000 0	Powering ○ ○○○○●○○ ○○	Composition 0 0	Main Theorem O	Proof of PCP Theorem
N(e)					

Therefore we finally have:

$$E(N) = \sum_{i \in I_r} E(N_i) = \sum_{i \in I_r} P(N_i > 0)$$
  
$$= \sum_{i \in I_r} \frac{|F|}{|E|} P(X_{u,i-1} = \sigma(u)) P(X_{v,t-i} = \sigma(v))$$
  
$$\geq |I_r| \frac{\tau^2}{4|\Sigma|^2} \frac{|F|}{|E|}$$
  
$$\geq \Omega(\sqrt{t}) \cdot \frac{|F|}{|E|}$$

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 00000●0 00	0 0	0	
N(e)					

 $E(N^2)$ 

Define  $Z_i(\mathbf{e}) = 1$  iff  $e_i \in F$ , else  $Z_i(\mathbf{e}) = 0$ ,  $Z(\mathbf{e}) := \sum_{i \in I_r} Z_i(\mathbf{e})$ .

$$\begin{split} E(Z^2) &= \sum_{i \in I_r} E(Z_i^2) + 2 \sum_{i < j; i, j \in I_r} E(Z_i Z_j) \\ &= |I_r| \frac{|F|}{|E|} + 2 \sum_{i < j; i, j \in I_r} E(Z_i Z_j) \\ E(Z_i Z_j) &= P(Z_i Z_j > 0) = P(Z_i > 0) P(Z_j > 0 | Z_i > 0) \\ &= \frac{|F|}{|E|} P(Z_j > 0 | Z_i > 0) \\ P_{|\mathbf{e}|=t}(Z_j (\mathbf{e}) > 0 | Z_i(\mathbf{e}) > 0) \\ &= P_{|\mathbf{e}'|=t-i+1}(Z_{j-i+1}(\mathbf{e}') > 0 | Z_1(\mathbf{e}') > 0) \le \frac{|F|}{|E|} + \left(\frac{\lambda}{d}\right)^{j-i} \end{split}$$

N(e)	Outline	Preprocessing 000000 000 0	O ○ ○ ○ ○ ○ ○ ○	Composition 0 0	Main Theorem O	Proof of PCP Theorem
	N(e)					

# $E(N^2)$

Having that  $\lambda < d$ , we know that  $\sum_{i=0}^{\infty} \left(\frac{\lambda}{d}\right)^i = K < \infty$ . Gathering all those results, we can estimate  $E(N^2)$ :

$$E(N^{2}) \leq E(Z^{2}) \leq |I_{r}| \frac{|F|}{|E|} + 2\frac{|F|}{|E|} \sum_{i < j; i, j \in I_{r}} \left( \frac{|F|}{|E|} + \left(\frac{\lambda}{d}\right)^{j-i} \right)$$

$$\leq O(\sqrt{t}) \frac{|F|}{|E|} + 2\left(|I_{r}|^{2} \left(\frac{|F|}{|E|}\right)^{2} + |I_{r}| \frac{|F|}{|E|} K\right)$$

$$= O(\sqrt{t}) \frac{|F|}{|E|} + O(t) \left(\frac{|F|}{|E|}\right)^{2}$$

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 ●0	0 0 0	0	
Two Cases					

# Powering: Two Cases

Now we can show the amplification. However we have to distinguish between two cases:

- 1. UNSAT(**G**) >  $\frac{1}{\sqrt{t}}$
- 2. UNSAT(**G**)  $\leq \frac{1}{\sqrt{t}}$

The first case is simple:

$$\begin{aligned} \text{UNSAT}(G^t) &\geq P(N > 0) \geq \frac{\Omega(\sqrt{t})^2 \frac{|F|^2}{|E|^2}}{O(t) \frac{|F|}{|E|}} \geq \Omega(1) \frac{|F|}{|E|} \geq \Omega(1) \frac{1}{\sqrt{t}} \\ &= \Omega(\sqrt{t}) \frac{1}{t} \geq \Omega(\sqrt{t}) \min(\text{UNSAT}(G), \frac{1}{t}) \end{aligned}$$

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000	0	0	0	
	0000	00	õ		
Two Cases					

## Powering: Two Cases

Let  $\mathrm{UNSAT}(G) \leq \frac{1}{\sqrt{t}}$ , then we have:

$$E(N^2) \le O(\sqrt{t})\frac{|F|}{|E|} + O(t)\left(\frac{|F|}{|E|}\right)^2 \le O(\sqrt{t})\frac{|F|}{|E|}$$

$$\Rightarrow \text{UNSAT}(G^{t}) \geq P(N > 0) \geq \frac{\Omega(\sqrt{t})^{2} \frac{|F|^{2}}{|E|^{2}}}{O(\sqrt{t}) \frac{|F|}{|E|}} \\ \geq \Omega(\sqrt{t}) \frac{|F|}{|E|} \geq \Omega(\sqrt{t}) \min(\text{UNSAT}(G), \frac{1}{t})$$

outinite		0		
0000C 000 0	00000 00000 00		0	

# Composition

## Definition 4

[Assignment Tester] An Assignment Tester with alphabet  $\Sigma_0$ and rejection probability  $\varepsilon > 0$  is a polynomial-time transformation  $\mathscr{P}$  whose input is a circuit  $\Phi$  over Boolean variables X, and whose output is a constraint graph  $G = \langle (V, E), \Sigma_0, \mathscr{C} \rangle$  such that  $X \subset V$ , and such that the following holds. Let  $V' = V \setminus X$ , and let  $a : X \to \{0, 1\}$  be an assignment.

1. If  $a \in \text{SAT}(\Phi)$ , there exists  $b : V' \to \Sigma_0$  such that  $\text{UNSAT}_{a \cup b}(G) = 0$ .

2. If 
$$a \notin \text{SAT}(\Phi)$$
 then for all  $b : V' \to \Sigma_0$  holds  
 $\text{UNSAT}_{a \cup b}(G) \geq \varepsilon \cdot \text{dist}(a, \text{SAT}(\Phi)).$ 

	Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
0 00 0		000000 000 0	0 0000000 00	0 0 0	0	

# Composition

We this we can state the composition lemma:

## Lemma 3 (Composition)

Let  $\mathscr{P}$  an assignment tester with constant rejection probability  $\varepsilon > 0$ , and alphabet  $\Sigma_0, |\Sigma_0| = O(1)$ . There exists  $\beta_3 > 0$  that depends only on  $\mathscr{P}$ , such that any constraint graph  $G = \langle (V, E), \Sigma, \mathscr{C} \rangle$  can be transformed into a constraint graph  $G' = \langle (V', E'), \Sigma_0, \mathscr{C}' \rangle$ , denoted by  $G \circ \mathscr{P}$ , such that size $(G') = M(|\Sigma|) \cdot size(G)$ , and

## $\beta_3 \cdot \text{UNSAT}(G) \leq \text{UNSAT}(G') \leq \text{UNSAT}(G)$

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000	0	•	0	
	000	0000000	0		
Preparation					

## Composition: Preparation

The assignment tester needs input constraints defined over Boolean variables.

- 1. Let  $e: \Sigma \to \{0,1\}^{l}$  be an encoding with relative Hamming distance  $\varrho > 0, l = O(\log |\Sigma|)$ .
- 2. Replace each  $v \in V$  by I Boolean variables [v].
- Replace each constraint c over the two variables v, w by c̃ over [v] ∪ [w], such that c̃ is satisfied iff the assignment for [v] ∪ [w] is a legal encoding via e of an assignment for v and w that satisfies c.

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000	0	0	0	
	000	0000000	•		
	0	00	0		
Composition					

# Composition: Composition

- 1. Run  $\mathscr{P}$  on any such  $\tilde{c}$  and get constraint graphs  $G_c = \langle (V_c, E_c), \Sigma_0, \mathscr{C}_c \rangle.$
- 2. Without loss of generality we can assume  $|E_c| = |E_{c'}|$  for any constraints c, c'.
- 3. Define the resulting graph G' as follows:

$$G' = \left\langle (V', E'), \Sigma_0, \mathscr{C}' \right\rangle,$$

where  $V' = \cup_{c \in \mathscr{C}} V_c, E' = \cup_{c \in \mathscr{C}} E_c, \mathscr{C}' = \cup_{c \in \mathscr{C}} \mathscr{C}_c.$ 

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000	0000000	0	0	
Properties					

# Composition: Properties

- 1. Any c is transformed into a constraint  $\tilde{c}: \{0,1\}^{2l} \to \{T,F\}.$
- 2. Set *M* as the maximal size of the output graph of  $\mathscr{P}$  for an input  $\tilde{c}$ .

 $\Rightarrow M$  only depends on  $|\Sigma|$  and  $\mathscr{P}$ , and we have  $size(G') \leq M \cdot size(G)$ .

- 3. Let  $\sigma': V' \to \Sigma_0$  be a best assignment for G'.
- 4. Define  $\sigma: V \to \Sigma$  by: $\sigma(v) := \operatorname{minarg}_{a \in \Sigma}(\operatorname{dist}(e(a), \sigma'([v]))).$
- 5. Let c be a constraint over the variables u, v that rejects  $\sigma$ .
- 6. That means  $\operatorname{dist}(\sigma'|_{[u]\cup[v]}, \operatorname{SAT}(\tilde{c})) \geq \frac{\varrho}{4}$ .
- 7. By definition at least a fraction of  $\varepsilon \cdot \frac{\varrho}{4}$  of the constraints in  $\mathscr{C}_c$  reject  $\sigma'$ .

$$\Rightarrow \text{UNSAT}(G') \geq \frac{\varepsilon \varrho}{4} \cdot \text{UNSAT}(G).$$

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

## Main Theorem

Finally we can state the main amplification theorem:

## Theorem 4 (Main)

For any  $\Sigma$ ,  $|\Sigma| = O(1)$ , there exist constants C > 0 and  $0 < \alpha < 1$ , such that given a constraint graph  $G = \langle (V, E), \Sigma, \mathscr{C} \rangle$  one can construct, in polynomial time, a constraint graph  $G' = \langle (V', E'), \Sigma_0, \mathscr{C}' \rangle$  such that

- 1.  $size(G') \leq C \cdot size(G)$  and  $|\Sigma_0| = O(1)$ .
- 2. If UNSAT(G) = 0 then UNSAT(G') = 0
- 3. UNSAT(G')  $\geq \min(2 \cdot \text{UNSAT}(G), \alpha)$ .

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem	
	000000	0 0000000 00	0	•		
Proof of the Main Theorem						

1. Define  $G' = (prep(G))^t \circ \mathscr{P}$  using the previous lemmata.

2. Each lemma only incurs a linear blowup of the size.

3. Choose 
$$t = \left\lceil \left(\frac{2}{\beta_1 \beta_2 \beta_3}\right)^2 \right\rceil$$
 and  $\alpha = \frac{\beta_3 \beta_2}{\sqrt{t}}$ :

$$\begin{aligned} \text{JNSAT}(G') &\geq \beta_3 \cdot \text{UNSAT}((\textit{prep}(G))^t) \\ &\geq \beta_3 \cdot \beta_2 \sqrt{t} \cdot \min(\text{UNSAT}(\textit{prep}(G)), \frac{1}{t}) \\ &\geq \beta_3 \cdot \beta_2 \sqrt{t} \cdot \min(\beta_1 \text{UNSAT}(G), \frac{1}{t}) \\ &\geq \min(2 \cdot \text{UNSAT}(G), \alpha). \end{aligned}$$

J

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

1. It is NP-hard to decide if UNSAT(G) = 0 or not for a given constraint graph G with  $|\Sigma| = 7$ .

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

- 1. It is NP-hard to decide if UNSAT(G) = 0 or not for a given constraint graph G with  $|\Sigma| = 7$ .
- 2. Let  $G_0$  be such an instance and  $G_i$  be the the outcome after applying the main theorem on  $G_{i-1}$ .

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

- 1. It is NP-hard to decide if UNSAT(G) = 0 or not for a given constraint graph G with  $|\Sigma| = 7$ .
- 2. Let  $G_0$  be such an instance and  $G_i$  be the the outcome after applying the main theorem on  $G_{i-1}$ .
- 3. Set  $k := \lceil \log(\alpha |E_0|) \rceil = O(\log n) :\Rightarrow \forall i \le k : size(G_i) \le C^i \cdot size(G_0) = poly(n).$

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

- 1. It is NP-hard to decide if UNSAT(G) = 0 or not for a given constraint graph G with  $|\Sigma| = 7$ .
- 2. Let  $G_0$  be such an instance and  $G_i$  be the the outcome after applying the main theorem on  $G_{i-1}$ .
- 3. Set  $k := \lceil \log(\alpha |E_0|) \rceil = O(\log n) :\Rightarrow \forall i \le k : size(G_i) \le C^i \cdot size(G_0) = poly(n).$
- 4. If  $\text{UNSAT}(G_0) = 0$  then  $\text{UNSAT}(G_i) = 0$ .

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

- 1. It is NP-hard to decide if UNSAT(G) = 0 or not for a given constraint graph G with  $|\Sigma| = 7$ .
- 2. Let  $G_0$  be such an instance and  $G_i$  be the the outcome after applying the main theorem on  $G_{i-1}$ .
- 3. Set  $k := \lceil \log(\alpha | E_0|) \rceil = O(\log n) :\Rightarrow \forall i \le k : size(G_i) \le C^i \cdot size(G_0) = poly(n).$
- 4. If  $\text{UNSAT}(G_0) = 0$  then  $\text{UNSAT}(G_i) = 0$ .
- 5. If not, then we have by induction: UNSAT( $G_i$ )  $\geq \min(2^i \text{UNSAT}(G_0), \alpha)$ .

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

- 1. It is NP-hard to decide if UNSAT(G) = 0 or not for a given constraint graph G with  $|\Sigma| = 7$ .
- 2. Let  $G_0$  be such an instance and  $G_i$  be the the outcome after applying the main theorem on  $G_{i-1}$ .
- 3. Set  $k := \lceil \log(\alpha |E_0|) \rceil = O(\log n) :\Rightarrow \forall i \le k : size(G_i) \le C^i \cdot size(G_0) = poly(n).$
- 4. If  $\text{UNSAT}(G_0) = 0$  then  $\text{UNSAT}(G_i) = 0$ .
- 5. If not, then we have by induction: UNSAT( $G_i$ )  $\geq \min(2^i \text{UNSAT}(G_0), \alpha)$ .
- Therefore 2<sup>k</sup>UNSAT(G<sub>0</sub>) ≥ α and therefore UNSAT(G<sub>k</sub>) ≥ α.

Outline	Preprocessing	Powering	Composition	Main Theorem	Proof of PCP Theorem
	000000 000 0	0 0000000 00	0 0 0	0	

- 1. It is NP-hard to decide if UNSAT(G) = 0 or not for a given constraint graph G with  $|\Sigma| = 7$ .
- 2. Let  $G_0$  be such an instance and  $G_i$  be the the outcome after applying the main theorem on  $G_{i-1}$ .
- 3. Set  $k := \lceil \log(\alpha | E_0 |) \rceil = O(\log n) :\Rightarrow \forall i \le k : size(G_i) \le C^i \cdot size(G_0) = poly(n).$
- 4. If  $\text{UNSAT}(G_0) = 0$  then  $\text{UNSAT}(G_i) = 0$ .
- 5. If not, then we have by induction: UNSAT( $G_i$ )  $\geq \min(2^i \text{UNSAT}(G_0), \alpha)$ .
- 6. Therefore  $2^k \text{UNSAT}(G_0) \ge \alpha$  and therefore  $\text{UNSAT}(G_k) \ge \alpha$ .
- 7. Now a local gadget reduction takes  $G_k$  to 3SAT form, while maintaining the satisfiability gap up to some constant.