PCP and Approximation

Thursday, May 31, 2018 9:10 AM

More formally on the relationship between hardness of approximation and PCP.

Constraint Satisfaction Problem (generalization of SAT)

q is a natural number

An instance of qCSP is a collection of functions $\varphi_1 \dots \varphi_m$ (called constraints)

$\varphi_i : \{0,1\}^n \to \{0,1\}$ each φ_i depends on at most q of the inputs

$\forall i \in [m] \quad \exists j_1 \cdots j_q \in [n] \quad f : \{0,1\}^q \to \{0,1\}$

$\varphi_i(\vec{u}) = f(u_{j_1}, \dots u_{j_q})$ for every $\vec{u} \in \{0,1\}^n$

$\vec{u}$ satisfies the i^{th} constraint if $\varphi_i(\vec{u}) = 1$

The fraction of constraints satisfied in $\dfrac{\sum_{i=1}^{m} \varphi_i(\vec{u})}{m}$

$$\mathrm{val}(\varphi) = \max_{\vec{u}} \left[\frac{\sum_{i=1}^{m} \varphi_i(\vec{u})}{m} \right]$$

φ is satisfiable iff $\mathrm{val}(\varphi) = 1$.

q is the "arity" of φ.

PCP and Approximation

Thursday, May 31, 2018 9:10 AM

Gap CSP: $\forall\, q \in \mathbb{N}$, $\rho \le 1$ define ρ-GAP q CSP to be the problem of determining for φ instance of q-CSP:

1) $val(\varphi) = 1$ "YES" instance.
2) $val(\varphi) < \rho$ "NO" instance.

ρ-GAP q CSP is NP hard if for every $L \in NP$ $\exists$ poly-time function f:

Completeness $x \in L \Rightarrow val(f(x)) = 1$
Soundness $x \notin L \Rightarrow val(f(x)) < \rho$.

Theorem 1: $\exists\, q \in \mathbb{N}$, $\rho \in (0,1)$ such that ρ-GAP-q-CSP is NP-hard.

Theorem 2: $NP \overset{?}{=} PCP(\log n, 1)$

Theorem 2 $\Rightarrow$ Theorem 1 Assume $NP \subseteq PCP(\log n, 1)$

Will show $1/2$-GAP-q-CSP is NP-hard for some q

$\Rightarrow$ SAT has a PCP system in which the verifier uses $c \cdot \log n$ bits and queries q locations.

$V_{x,r}$ is the function that on input $\pi \in \{0,1\}^q$ is 1 iff the verifier accepts.

PCP and Approximation

Thursday, May 31, 2018 9:10 AM

$\varphi_x = \{ V_{x,r} \}_{r \in \{0,1\}^{c \log n}}$ is an instance of CSP with $2^{c \log n} = \text{poly}(n)$ constraints.

Each r gives a different constraint.

Note: at most $q \cdot 2^{c \log n}$ bits of the proof are ever consulted, so Prover only needs to commit to those bits. (This forms the "proof" $\vec{u}$).

Random string r: determines which q bits are sent to the verifier.

Since $V_{x,r}$ runs in poly-time, the transformation of x to φ_x is also poly time.

if $x \in SAT \Rightarrow \text{val}(\varphi) = 1$. (V accepts w/ prob 1)

if $x \notin SAT \Rightarrow \text{val}(\varphi) \leq 1/2$ (V accepts w/ prob $\leq 1/2$).

Theorem 1 $\Rightarrow$ Theorem 2

ρ-GAP-qCSP is NP hard for some $q \in \mathbb{N}$, $\rho < 1$.

$\Rightarrow$ translates to a PCP system w/ q queries, ρ soundness and log randomness, for any $L \in NP$.

PCP and Approximation

$x \in L \qquad Val(f(x)) = 1$

$x \notin L \qquad Val(f(x)) \le \rho.$

Thursday, May 31, 2018 9:10 AM

Run reduction of L to ρ-GAP-q-CSP to get $\varphi_x = f(x)$.

Suppose $\varphi_x = \{\varphi_i\}_{1 \le i \le m}$.

The verifier will expect the proof to be an assignment to the variables.

Verifier selects random $i \in [m]$ and asks to see the variables involved in φ_i. (There are q)

if $x \in L \Rightarrow Val(\varphi_x) = 1$ and verifier accepts w.p. $= 1$.

if $\cancel{x \notin L} \Rightarrow Val(\varphi_x) \le \rho$ and verifier accepts w.p. $\le \rho$

$\hookrightarrow$ Can be boosted to $1/2$ at the expense of a constant factor in q & randomness.

What about hardness of approximation for other problems?

We already showed a $1/2$-approx for Vertex cover.

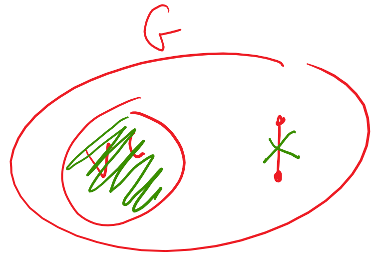
Is it possible to do better?

We will show that for VC there is a γ s.t. approximating VC to within γ is NP-hard.

Also for any $\gamma < 1$ approximating Indep Set to within γ is NP hard. $\hookrightarrow$ since VC has $1/2$-approx the approximability of VC & IS is very different.

PCP and Approximation

Thursday, May 31, 2018 9:10 AM



Note: the complement of a vertex cover is an independent set.

VC = size of smallest vertex cover.

IS = size of largest independent set.

$VC = n - IS$

In terms of exact solutions, these two problems have the same complexity.

A ρ-approx for Independent Set produces an independent set of size at least $\rho \cdot IS$. What kind of approx does this give for VC?

$$\frac{n - IS}{n - \rho \cdot IS}$$

this could be very small if IS is close to n.

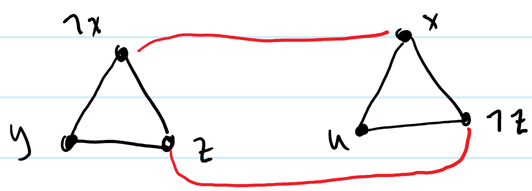
First we will show that each problem has a ρ s.t. it can not be ρ-approximated (unless P=NP).

Then we will show how to amplify this factor for Independent Set.

Lemma: $\exists$ poly-time reduction from 3CNF $\to$ graphs s.t. $\forall \phi$ $f(\phi)$ is an n vertex graph whose largest indep set has size $\frac{val(\phi)\, n}{3}$

$VC = n - \frac{val(\phi) n}{3}$

This is the reduction we saw at the beginning of the quarter:



#vertices = 3m.

PCP and Approximation

Thursday, May 31, 2018 9:10 AM

<u>Corollary</u>: $\exists \rho < 1$ $\rho' < 1$

Independent Set can not be ρ-approximated in poly time.
Vertex Cover can not be ρ'-approximated in poly time

<u>Proof</u>: $L \in NP$ $\exists f$ f'

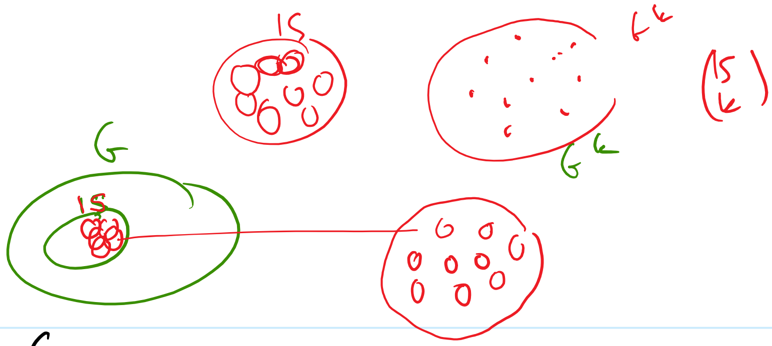
$x \in L \longrightarrow \varphi$ satisfiable $\longrightarrow G$ has indep set of size $\frac{n}{3}$.
$x \notin L \longrightarrow \leq \rho m$ clauses in φ can be satisfied $\rightarrow$ Indep set in G has size $< \rho \frac{n}{3}$

$x \in L \rightarrow \varphi$ satisfiable $\rightarrow G$ has vertex cover of size $\frac{2n}{3}$
$x \notin L \rightarrow \leq \rho m$ clauses in φ can be satisfied $\rightarrow$ Vertex Cover in G has size $\geq n - \frac{\rho n}{3}$
$\geq (1-\rho/3)n.$

Approx to within $\frac{2/3}{(1-\rho/3)} = \frac{2}{3-\rho}$
not possible unless $P = NP$.

PCP and Approximation

Thursday, May 31, 2018 9:10 AM



Boosting for Independent Set:

Graph $G \longrightarrow G^k$

$G=(V,E)$
$|V|=n$.

Every vertex in G^k represents a size-k subset in G.

$\#$ vertices in $G^k = \binom{n}{k}$

$x \longrightarrow \binom{x}{k}$

$\rho \cdot x \longrightarrow \binom{\rho x}{k}$

Two vertices S_1 + S_2 are not adjacent iff $S_1 \cup S_2$ is an independent set in G.

$\geq IS \longrightarrow \geq \binom{IS}{k}$

$IS \longleftarrow \binom{IS}{k}$

Indep Set in G^k $S_1 \cdots S_r$

$S_1 \cup S_2 \cdots \cup S_r$ is independent in G.

$|S_1 \cup S_2 \cdots \cup S_r| \geq t$ s.t. $r \leq \binom{t}{k}$

Gap of ρ in G becomes a gap of $\dfrac{\binom{\rho \cdot IS}{k}}{\binom{IS}{k}} \approx \rho^k$. in G^k

For any constant γ, can select k s.t. $\rho^k < \gamma$

k is a constant + running time of reduction is $O(n^k)$.