BILL START RECORDING

HW 11 Solutions

Problem 1

Describe the reduction of 3SAT to IND SET.

Problem 1

Describe the reduction of 3SAT to IND SET.
1) Input $(L_{11} \vee L_{12} \vee L_{13}) \wedge \cdots \wedge (L_{k1} \vee L_{k2} \vee L_{k3})$

Problem 1

Describe the reduction of 3SAT to IND SET.

1) Input $(L_{11} \vee L_{12} \vee L_{13}) \wedge \cdots \wedge (L_{k1} \vee L_{k2} \vee L_{k3})$

2)

$$V = \{(i, L_{ij})\colon 1 \leq i \leq k, 1 \leq j \leq 3\}$$

Problem 1

Describe the reduction of 3SAT to IND SET.

1) Input $(L_{11} \vee L_{12} \vee L_{13}) \wedge \cdots \wedge (L_{k1} \vee L_{k2} \vee L_{k3})$

2)

$$V = \{(i, L_{ij}) \colon 1 \leq i \leq k, 1 \leq j \leq 3\}$$

3) E is

Problem 1

Describe the reduction of 3SAT to IND SET.

1) Input $(L_{11} \vee L_{12} \vee L_{13}) \wedge \cdots \wedge (L_{k1} \vee L_{k2} \vee L_{k3})$

2)

$$V = \{(i, L_{ij}) \colon 1 \le i \le k, 1 \le j \le 3\}$$

3) E is

$$\{(i, L_{i1}, (i, L_{i2}), (i, L_{i2}, (i, L_{i3}), (i, L_{i3}, (i, L_{i1}) \colon 1 \le i \le k\}$$

Problem 1

Describe the reduction of 3SAT to IND SET.

1) Input $(L_{11} \vee L_{12} \vee L_{13}) \wedge \cdots \wedge (L_{k1} \vee L_{k2} \vee L_{k3})$

2)

$$V = \{(i, L_{ij}) \colon 1 \leq i \leq k, 1 \leq j \leq 3\}$$

3) E is

$$\{(i, L_{i1}, (i, L_{i2}), (i, L_{i2}, (i, L_{i3}), (i, L_{i3}, (i, L_{i1}) \colon 1 \leq i \leq k\}$$

$$\bigcup \{(i, L_{ij}), (i', L_{i',j'}) \colon i \neq i' \wedge L_{ij} = \neg L_{i',j'}\}.$$

Problem 1. Think About

Come up with a 3-CNF formula that is NOT in 3-SAT. Apply your algorithm to it. What does the graph look like?

$$(x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge$$

Problem 1. Think About

Come up with a 3-CNF formula that is NOT in 3-SAT. Apply your algorithm to it. What does the graph look like?

$$(x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge$$

$$(x \vee y \neg \vee \neg z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee y \vee \neg z) \wedge$$

Problem 1. Think About

Come up with a 3-CNF formula that is NOT in 3-SAT. Apply your algorithm to it. What does the graph look like?

$$(x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge$$

$$(x \vee y \neg \vee \neg z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee y \vee \neg z) \wedge$$

$$(\neg x \vee \neg y \vee z) \wedge (\neg x \vee y \neg \vee \neg z)$$

Problem 1. Think About

Come up with a 3-CNF formula that is NOT in 3-SAT. Apply your algorithm to it. What does the graph look like?

$$(x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge$$

$$(x \vee y \neg \vee \neg z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee y \vee \neg z) \wedge$$

$$(\neg x \vee \neg y \vee z) \wedge (\neg x \vee y \neg \vee \neg z)$$

The graph would be a mess!

Problem 1. Think About

Come up with a 3-CNF formula that is NOT in 3-SAT. Apply your algorithm to it. What does the graph look like?

$$(x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge$$

$$(x \vee y \neg \vee \neg z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee y \vee \neg z) \wedge$$

$$(\neg x \vee \neg y \vee z) \wedge (\neg x \vee y \neg \vee \neg z)$$

The graph would be a mess!

Most formulas are satisfiable.

Problem 1. Think About

Come up with a 3-CNF formula that is NOT in 3-SAT. Apply your algorithm to it. What does the graph look like?

$$(x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge$$

$$(x \vee y \neg \vee \neg z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee y \vee \neg z) \wedge$$

$$(\neg x \vee \neg y \vee z) \wedge (\neg x \vee y \neg \vee \neg z)$$

The graph would be a mess!

Most formulas are satisfiable.

Thats why SAT Solvers work so well.

Problem 2a

$$\mathrm{SQ}_k = \{x \colon (\exists y_1, \ldots, y_k)[x = y_1^2 + \cdots + y_k^2]\}.$$

Problem 2a

$\mathrm{SQ}_k = \{x \colon (\exists y_1, \ldots, y_k)[x = y_1^2 + \cdots + y_k^2]\}$.

a) Show that, for all k, SQ_k is in NP.

Problem 2a

$\mathrm{SQ}_k = \{x\colon (\exists y_1, \ldots, y_k)[x = y_1^2 + \cdots + y_k^2]\}$.

a) Show that, for all k, SQ_k is in NP.

$\mathrm{SQ}_k = \{x\colon (\exists y_1, \ldots, y_k)[x = y_1^2 + \cdots + y_k^2]\}$.

Problem 2a

$\mathrm{SQ}_k = \{x \colon (\exists y_1, \ldots, y_k)[x = y_1^2 + \cdots + y_k^2]\}$.

a) Show that, for all k, SQ_k is in NP.

$\mathrm{SQ}_k = \{x \colon (\exists y_1, \ldots, y_k)[x = y_1^2 + \cdots + y_k^2]\}$.

Since $y_i \le x$, $|y_i| < |x|$ (thats length not abs val.)

Problem 2a

$\mathrm{SQ}_k = \{x : (\exists y_1, \ldots, y_k)[x = y_1^2 + \cdots + y_k^2]\}$.

a) Show that, for all k, SQ_k is in NP.

$\mathrm{SQ}_k = \{x : (\exists y_1, \ldots, y_k)[x = y_1^2 + \cdots + y_k^2]\}$.

Since $y_i \le x$, $|y_i| < |x|$ (thats length not abs val.)

Addition and mult are easy, so verification is easy.

Problem 2b

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

where $(\forall i)[p_i \equiv 1 \pmod 4]$ and $(\forall i)[q_i \equiv 3 \pmod 4]$.

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

where $(\forall i)[p_i \equiv 1 \pmod 4]$ and $(\forall i)[q_i \equiv 3 \pmod 4]$.

x **is the sum of two squares iff** $(\forall i)[s_i \equiv 1 \pmod 2]$**.**

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

where $(\forall i)[p_i \equiv 1 \pmod 4]$ and $(\forall i)[q_i \equiv 3 \pmod 4]$.

x **is the sum of two squares iff** $(\forall i)[s_i \equiv 1 \pmod 2]$**.**

Not known to be in P.

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

where $(\forall i)[p_i \equiv 1 \pmod 4]$ and $(\forall i)[q_i \equiv 3 \pmod 4]$.

x **is the sum of two squares iff** $(\forall i)[s_i \equiv 1 \pmod 2]$**.**

Not known to be in P.

SQ_2 can be computed IF you could factor.

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

where $(\forall i)[p_i \equiv 1 \pmod 4]$ and $(\forall i)[q_i \equiv 3 \pmod 4]$.

x **is the sum of two squares iff** $(\forall i)[s_i \equiv 1 \pmod 2]$.

Not known to be in P.

SQ_2 can be computed IF you could factor.

$$\mathrm{SQ}_2 \le_T \mathrm{FACT}$$

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

where $(\forall i)[p_i \equiv 1 \pmod 4]$ and $(\forall i)[q_i \equiv 3 \pmod 4]$.

x **is the sum of two squares iff** $(\forall i)[s_i \equiv 1 \pmod 2]$**.**

Not known to be in P.

SQ_2 can be computed IF you could factor.

$$\mathrm{SQ}_2 \le_T \mathrm{FACT}$$

which means SQ_2 can be solved by making queries to FACT.

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

where $(\forall i)[p_i \equiv 1 \pmod 4]$ and $(\forall i)[q_i \equiv 3 \pmod 4]$.

x **is the sum of two squares iff** $(\forall i)[s_i \equiv 1 \pmod 2]$**.**

Not known to be in P.

SQ_2 can be computed IF you could factor.

$$\mathrm{SQ}_2 \le_T \mathrm{FACT}$$

which means SQ_2 can be solved by making queries to FACT.

If SQ_2 is NP-complete then $\mathrm{SAT} \le \mathrm{SQ}_2 \le_T \mathrm{FACT}$.

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

where $(\forall i)[p_i \equiv 1 \pmod 4]$ and $(\forall i)[q_i \equiv 3 \pmod 4]$.

x **is the sum of two squares iff** $(\forall i)[s_i \equiv 1 \pmod 2]$**.**

Not known to be in P.

SQ_2 can be computed IF you could factor.

$$\mathrm{SQ}_2 \le_T \mathrm{FACT}$$

which means SQ_2 can be solved by making queries to FACT.

If SQ_2 is NP-complete then $\mathrm{SAT} \le \mathrm{SQ}_2 \le_T \mathrm{FACT}$.

Recall $\mathrm{SAT} \le \mathrm{FACT} \rightarrow \mathrm{TAUT} \in \mathrm{NP}$ which is unlikely.

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

where $(\forall i)[p_i \equiv 1 \pmod 4]$ and $(\forall i)[q_i \equiv 3 \pmod 4]$.

x **is the sum of two squares iff** $(\forall i)[s_i \equiv 1 \pmod 2]$**.**

Not known to be in P.

SQ_2 can be computed IF you could factor.

$$\mathrm{SQ}_2 \le_T \mathrm{FACT}$$

which means SQ_2 can be solved by making queries to FACT.

If SQ_2 is NP-complete then $\mathrm{SAT} \le \mathrm{SQ}_2 \le_T \mathrm{FACT}$.

Recall $\mathrm{SAT} \le \mathrm{FACT} \rightarrow \mathrm{TAUT} \in \mathrm{NP}$ which is unlikely.

$\mathrm{SAT} \le_T \mathrm{FACT}$ doesn't imply $\mathrm{TAUT} \in \mathrm{NP}$ but it implies other things unlikely.

Problem 2b

b) Is $\mathrm{SQ}_2 \in \mathrm{P}$? Is SQ_2 NP-Complete?

The 2-Square Theorem

Let $x = 2^a p_1^{r_1} \cdots p_b^{r_b} q_1^{s_1} \cdots q_d^{s_d}$

where $(\forall i)[p_i \equiv 1 \pmod 4]$ and $(\forall i)[q_i \equiv 3 \pmod 4]$.

x **is the sum of two squares iff** $(\forall i)[s_i \equiv 1 \pmod 2]$**.**

Not known to be in P.

SQ_2 can be computed IF you could factor.

$$\mathrm{SQ}_2 \le_T \mathrm{FACT}$$

which means SQ_2 can be solved by making queries to FACT.

If SQ_2 is NP-complete then $\mathrm{SAT} \le \mathrm{SQ}_2 \le_T \mathrm{FACT}$.

Recall $\mathrm{SAT} \le \mathrm{FACT} \to \mathrm{TAUT} \in \mathrm{NP}$ which is unlikely.

$\mathrm{SAT} \le_T \mathrm{FACT}$ doesn't imply $\mathrm{TAUT} \in \mathrm{NP}$ but it implies other things unlikely.

We do not think SQ_2 is NP-complete.

Problem 2c

Problem 2c

c) Is $\mathrm{SQ}_3 \in \mathrm{P}$? Is SQ_3 NP-Complete?

Problem 2c

c) Is $\mathrm{SQ}_3 \in \mathrm{P}$? Is SQ_3 NP-Complete?

Legendre's 3-square theorem: $x \in \mathrm{SQ}_3$ iff $x \neq 4^a(8b+7)$.

Problem 2c

c) Is $\mathrm{SQ}_3 \in \mathrm{P}$? Is SQ_3 NP-Complete?

Legendre's 3-square theorem: $x \in \mathrm{SQ}_3$ iff $x \neq 4^a(8b+7)$.

$\mathrm{SQ}_3 \in \mathrm{P}$:

Problem 2c

c) Is $\mathrm{SQ}_3 \in \mathrm{P}$? Is SQ_3 NP-Complete?

Legendre's 3-square theorem: $x \in \mathrm{SQ}_3$ iff $x \neq 4^a(8b+7)$.

$\mathrm{SQ}_3 \in \mathrm{P}$:
1) Input x.

Problem 2c

c) Is $\mathrm{SQ}_3 \in \mathrm{P}$? Is SQ_3 NP-Complete?

Legendre's 3-square theorem: $x \in \mathrm{SQ}_3$ iff $x \neq 4^a(8b+7)$.

$\mathrm{SQ}_3 \in \mathrm{P}$:
1) Input x.
2) Keep dividing 4 into it until you get
$x = 4^a c$ where 4 does not divide c.

Problem 2c

c) Is $\mathrm{SQ}_3 \in \mathrm{P}$? Is SQ_3 NP-Complete?

Legendre's 3-square theorem: $x \in \mathrm{SQ}_3$ iff $x \neq 4^a(8b+7)$.

$\mathrm{SQ}_3 \in \mathrm{P}$:
1) Input x.
2) Keep dividing 4 into it until you get
$x = 4^a c$ where 4 does not divide c.
3) If $c \not\equiv 7 \pmod 8$ then $x \in \mathrm{SQ}_3$, else $x \notin \mathrm{SQ}_3$.

Problem 2d

Problem 2d

d) Is $\mathrm{SQ}_4 \in \mathrm{P}$? Is SQ_4 NP-Complete?
It is know that **every** number is the sum of 4 squares.
So $\mathrm{SQ}_4 = \mathsf{N} \in \mathrm{P}$.

Problem 2d

d) Is $\mathrm{SQ}_4 \in \mathrm{P}$? Is SQ_4 NP-Complete?
It is know that **every** number is the sum of 4 squares.
So $\mathrm{SQ}_4 = \mathsf{N} \in \mathrm{P}$.

e) Is $\mathrm{SQ}_5 \in \mathrm{P}$? Is SQ_5 NP-Complete?
It is know that **every** number is the sum of 4 squares.
So $\mathrm{SQ}_5 = \mathsf{N} \in \mathrm{P}$.

Problem 3a

$$A_k = \{G : \ G \text{ is Planar and } G \text{ is } k\text{-colorable } \}.$$

Problem 3a

$A_k = \{G\colon\ G \text{ is Planar and } G \text{ is } k\text{-colorable }\}$.
Show that, for all k, the set A_k is in NP.
$A_k = \{G = (V, E)\colon (\exists f)$

$$[f\colon V \to [k] \wedge (\forall (a, b) \in E[f(a) \neq f(b)] \wedge G \text{ Planar}].$$

Problem 3b,3c,3d

Problem 3b,3c,3d

b) Is $A_2 \in \mathrm{P}$? YES Is A_2 NP-complete? PROB NOT.

Problem 3b,3c,3d

b) Is $A_2 \in \mathrm{P}$? YES Is A_2 NP-complete? PROB NOT.

c) Is $A_3 \in \mathrm{P}$? Is A_3 NP-complete?

Problem 3b,3c,3d

b) Is $A_2 \in \mathrm{P}$? YES Is A_2 NP-complete? PROB NOT.

c) Is $A_3 \in \mathrm{P}$? Is A_3 NP-complete?
A_3 is NP-complete so prob not in P.

Problem 3b,3c,3d

b) Is $A_2 \in \mathrm{P}$? YES Is A_2 NP-complete? PROB NOT.

c) Is $A_3 \in \mathrm{P}$? Is A_3 NP-complete?
A_3 is NP-complete so prob not in P.

Problem 3b,3c,3d

b) Is $A_2 \in \mathrm{P}$? YES Is A_2 NP-complete? PROB NOT.

c) Is $A_3 \in \mathrm{P}$? Is A_3 NP-complete?
A_3 is NP-complete so prob not in P.

d) Is $A_4 \in \mathrm{P}$? Is A_4 NP-complete?

Problem 3b,3c,3d

b) Is $A_2 \in \mathrm{P}$? YES Is A_2 NP-complete? PROB NOT.

c) Is $A_3 \in \mathrm{P}$? Is A_3 NP-complete?
A_3 is NP-complete so prob not in P.

d) Is $A_4 \in \mathrm{P}$? Is A_4 NP-complete?
All planar graphs are 4-colorable.
Hence A_4 is the set of all planar graphs, $A_4 \in \mathrm{P}$.

Problem 3b,3c,3d

b) Is $A_2 \in \mathrm{P}$? YES Is A_2 NP-complete? PROB NOT.

c) Is $A_3 \in \mathrm{P}$? Is A_3 NP-complete?
A_3 is NP-complete so prob not in P.

d) Is $A_4 \in \mathrm{P}$? Is A_4 NP-complete?
All planar graphs are 4-colorable.
Hence A_4 is the set of all planar graphs, $A_4 \in \mathrm{P}$.

e) Is $A_5 \in \mathrm{P}$? Is A_5 NP-complete?

Problem 3b,3c,3d

b) Is $A_2 \in \mathrm{P}$? YES Is A_2 NP-complete? PROB NOT.

c) Is $A_3 \in \mathrm{P}$? Is A_3 NP-complete?
A_3 is NP-complete so prob not in P.

d) Is $A_4 \in \mathrm{P}$? Is A_4 NP-complete?
All planar graphs are 4-colorable.
Hence A_4 is the set of all planar graphs, $A_4 \in \mathrm{P}$.

e) Is $A_5 \in \mathrm{P}$? Is A_5 NP-complete?
All planar graphs are 4-colorable.
Hence A_5 is the set of all planar graphs, $A_5 \in \mathrm{P}$.

Point of Problems 2 and 3

Point of Problems 2 and 3

For problems 2 and 3 a theorem in MATH enabled us to show that some problems were in P.

Point of Problems 2 and 3

For problems 2 and 3 a theorem in MATH enabled us to show that some problems were in P.

To show $\mathrm{P} \neq \mathrm{NP}$ we have to prove that no (perhaps hard) theorem in math will show SAT is in P

Point of Problems 2 and 3

For problems 2 and 3 a theorem in MATH enabled us to show that some problems were in P.

To show $\mathrm{P} \neq \mathrm{NP}$ we have to prove that no (perhaps hard) theorem in math will show SAT is in P

Respect Lower Bounds!