This semester's topic: TFNP $\cap$ cryptography

cryptography:
- OWF one-way functions
- public key crypto
- IO

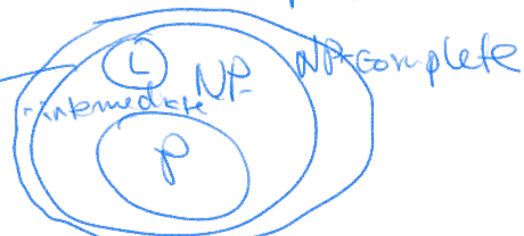
$P \neq NP$. assuming very hard (average-case) problems in NP

???

Dream: show OWF exist based off "normal" complexity assumptions

maybe?

Ladner's theorem if $P \neq NP$
there are "intermediate languages": $L \notin P$, $L \in NP$
but not NP-complete.



assume this is hard

Good candidate for intermediate (not NP-complete) problems: TFNP
T = total

---

overview of crypto

Impagliazzo 1995 "a personal view of ..."

- Algorithmica – $P = NP^{av}$
- Heuristica – $P \neq NP$, but NP is easy-on-average
- Pessiland – NP is not easy-on-average, yet no OWF exist.
- Minicrypt – OWF exist but no PKE
- Cryptomania – PKC exists.
- "obfustopia" – iO + ~~PKE~~ OWF exists.

CRHF

($\Leftrightarrow$ PRG $\Leftrightarrow$ PRF
$\Leftrightarrow$ MAC $\Leftrightarrow$ private key enc
$\Leftrightarrow$ sig schemes)

Def: $f: \{0,1\}^* \to \{0,1\}^*$ is a one-way function (owF)
if:
- f is poly time computable
- $\forall$ ppt A $\exists$ neg $\varepsilon(\cdot)$ s.t.

$$\Pr_{x \leftarrow_u \{0,1\}^n}\left[f(A(1^n, f(x))) = f(x) \right] \leq \varepsilon(n)$$

$$x \underset{\text{hard}}{\overset{\text{easy}}{\rightleftarrows}} f(x)$$

Note: owF exist $\Rightarrow$ NP is not easy-on-average.

Def:
- f is an injective owF if $\forall n$ $f_n := \underbrace{f|_{\{0,1\}^n}}_{f \text{ restricted to } \{0,1\}^n}$ is an injective function, and f is a owf.
- f is an onto owf if $\forall n$ f_n is onto owF
- f is a one-way permutation (owP) if f is an injective + onto owf, ie. $\forall n$ $f_n: \{0,1\}^n \to \{0,1\}^n$ is a bijection (and f is a owF)

owP exists $\Rightarrow$ iowF exists $\Rightarrow$ owF exists

other directions not known in fact separation.

Def: A collision resistant hash function (CRHF) is a pair of alg. (GEN, H) s.t:
- Gen is a ppt alg, that on input 1^n outputs a key s $|s| \geq n$ $\quad Gen(1^n) \to s$ (assume s includes info on n, e.g. $s = 1^n, \ldots$)
- H is a $\underset{\text{poly time computable}}{\text{det.}}$ function, s.t $H^s(x) \in \{0,1\}^{\ell(n)}$

[Note: if H^s is only defined on inputs $\in \{0,1\}^{L(n)}$,
i.e. $H^s: \{0,1\}^{L(n)} \to \{0,1\}^{\ell(n)}$, $L(n) > \ell(n)$,
this is called fixed-length CRHF]

- (Gen, H) satisfies collision-resistance:

$\forall$ ppt A $\exists$ neg $\varepsilon()$ s.t.:

$$\Pr_{s \leftarrow Gen(1^n)}[A(s) \to (x_1, x_2) : x_1 \neq x_2 \text{ and } H^s(x_1) = H^s(x_2)] \leq \varepsilon(n)$$

Note: CRHF exist $\Rightarrow$ OWF exist

proof sketch: $f(x,r)$: run $Gen(1^n; r) \to s$
output $(s, H^s(x))$
this is a OWF $\blacksquare$

"everything else" (CRHF $\overset{??}{\Rightarrow}$ OWP
PKE $\overset{??}{\Rightarrow}$ CRHF
$\overset{??}{\Leftarrow}$)
is not known,
evidence that it's false

$\to$ does not fit neatly within 5 worlds.

Def: $\mathcal{O}$ is an indistinguishability obfuscator ($i\mathcal{O}$)
for a class of circuits $\mathcal{C}$, if:

- $\mathcal{O}$ is a ppt algorithm
- $\forall C \in \mathcal{C}$, $\mathcal{O}(C) \equiv C$ (i.e., computes the same function)
- $\forall C_1, C_2 \in \mathcal{C}$ where $|C_1| = |C_2|$, and $C_1 \equiv C_2$,

$\forall$ ppt D $\exists$ neg $\varepsilon(\cdot)$ s.t.

$$\left| \Pr_{\mathcal{O},D}[D(\mathcal{O}(c_1))=1] - \Pr[D(\mathcal{O}(c_2))=1] \right| \le \varepsilon(n)$$

Note: • "iO exists in algorithmica"
(i.e, if P=NP then iO exists:
$\mathcal{O}(C)$: "output lexicog. first C' such that $C \equiv C'$ "

• OWF + iO is very powerful!
e.g. OWF + iO $\Rightarrow$ PKE
⋮

Total complexity

Def A relation R is a subset of $\{0,1\}^* \times \{0,1\}^*$

we are going to think of relations & search problems interchangeably.

Terminology
For $(x,y) \in R$
- y is an image of x under R (relation / set-theory view)
- y is a solution to x under R (search problem view)

Notation $(x,y) \in R \iff xRy$ (logic notation)
$R(x) = \{y : (x,y) \in R\}$ = set of solutions to x

Def a rel. R is polynomial if $\exists$ poly $p(\cdot)$ st
$\forall (x,y) \in R,\ |y| \le p(|x|)$

Def FP is the class of poly-relations R st there exists a poly time algo M st $M(x)$ outputs y st xRy.

functional

eg of a relation: FSAT : for formula φ, $(\varphi, x) \in$ FSAT iff $\varphi(x) = 1$.

<u>Claim</u> $\text{FSAT} \in \text{FP} \iff \text{P} = \text{NP}$

exercise (uses search-to-decision reduction)

<u>Def</u> FNP is the class of poly. relations st $\exists$ poly time M st $M(x, y) = 1 \iff xRy$

<u>Claim</u> $\text{FNP} = \text{FP} \iff \text{P} = \text{NP}$

<u>Def</u> A relation R is total iff $\forall x \in \{0,1\}^*$, $R(x) \neq \emptyset$

total

(search problems)

<u>Def</u> <u>TFNP</u> is the class of relations in <u>FNP</u> that are <u>total</u>.

eg. $\text{FSAT} \notin \text{TFNP}$. $\exists \varphi \notin \text{SAT}$

$\nexists y$ st $(\varphi, y) \in \text{FSAT}$

About TFNP itself ...

languages st $\exists$ certificates for non-membership in language.

$x \notin L \iff \exists y$ certificate $(M(x,y) = 1)$

<u>Prop</u> If $L \in \text{NP} \cap \text{coNP}$, then the associated search problem (for x, find a certificate that $x \in L$ or that $x \notin L$) is in TFNP.

TFNP is sort of the search problem analogue of $\text{NP} \cap \text{coNP}$.

<u>Thm</u> If a problem in TFNP is <u>NP-hard</u>, then the polynomial hierarchy collapses to the second level

$$PH = \underline{NP = co\text{-}NP}$$

Not believed to be true!

<u>Pf</u> Let $R \in \text{TFNP}$ be NP-hard :

for any NP decision problem (language L) can reduce deciding $x \overset{?}{\in} L$ to solving an instance of R (+ maybe some poly time overhead)

Let V be the verifier R $((x,y) \in R \iff V(x,y)=1)$

$L \in NP$, let f be its reduction to R.

- Exists poly time M such that given $\underline{x}$; $f(x)$, and a solution y to $f(x)$, M outputs $x \overset{?}{\in} L$.

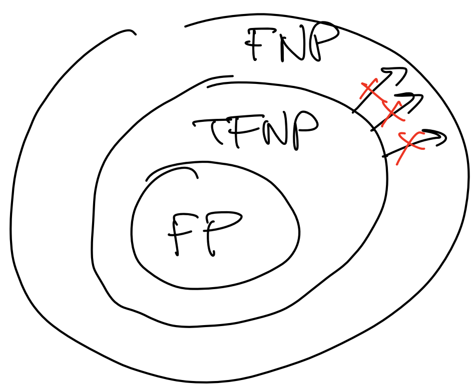
R instance

$\forall y$ st $V(f(x),y)=1$, $x \in L \iff M(x,f(x),y)=1$

But R is total! So a y necessarily exists.

$$\underbrace{x \notin L \iff \exists y \text{ st } V(f(x),y)=1 \wedge M(x,f(x),y)=0}$$

this is a certificate for non-membership in L, so $L \in coNP$ ▨



Other reason we like TFNP: has beautiful + interesting mathematical structure.

What kind of problems in TFNP?

- eg. FACTORING: given integer N, either output "prime" if N is prime, or output a non-trivial factor of N.

$\in$ TFNP

How do we get more TFNP problems...

Suppose you have an "existence theorem":

for any instance of a type t, there exists an efficiently verifiable property y of t.

t: could be circuits, graphs, integers, finite group elements, etc

Each existence thm gives a problem in TFNP:
given instance of t, find y.

If the proof of ex. thm. is constructive and efficiently so,
then problem is in FP.

Very important / famous example:

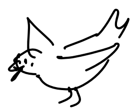
Pigeonhole principle!

Let $M: X \to Y$ be a mapping s.t. $|Y| < |X|$.
Then there exist $x_1, x_2 \in X$ st $M(x_1) = M(x_2)$
and $x_1 \neq x_2$.

$\Rightarrow$ gives a TFNP problem! Given M, find such a collision.

But how to represent M?

Most general way to represent the "type" in ex. thms:
as a circuit.



Def (search problem / relation) PIGEON: Given a circuit

$C: \{0,1\}^n \to \{0,1\}^n$ find x s.t. $C(x) = 0^n$

or $x_1, x_2 \in \{0,1\}^n$ st $x_1 \neq x_2$ and $C(x_1) = C(x_2)$.

forces co-domain of C be smaller than domain.

Minor modifications / other ways to force smaller co-domain
don't make a difference.

eg $C: \{0,1\}^n \to \{0,1\}^n$, modify $C': \{0,1\}^n \to \{0,1\}^n \setminus 0^n$

by mapping any x $C(x) = 0^n$ to 1^n

Now find a collision of C'.

PIGEON & this variant are equiv. to each other. (exercise)

PIGEON $\in$ TFNP

Def PPP is the class of relations in TFNP that are poly-time reducible to PIGEON.

Def WEAK-PIGEON Given $C: \{0,1\}^n \to \{0,1\}^{n-1}$ find $x \neq x'$ st $C(x) = C(x')$

Substantially "easier" than pigeon problem.

PIGEON: ≥ 1 collision

WEAK-PIGEON $\geq 2^{n-1}$ solutions

Def PWPP: relations in TFNP that are pt reducible to WEAK-PIGEON.

What about ... p-WEAKPIGEON $C: \{0,1\}^{n+p} \to \{0,1\}^n$

$\Downarrow$

- reduces to WEAK-PIGEON $C': \{0,1\}^{n+1} \to \{0,1\}^n$

$$C'(x) = C(x \| 0^{p-1})$$

Prop WEAK-PIGEON reduces to p-WEAK-PIGEON.

Pf $C: \{0,1\}^{n+1} \to \{0,1\}^n$ construct

$$C^p(x_1, \dots, x_p) = C(x_1) \| \cdots \| C(x_p)$$

$$C^p: \{0,1\}^{p \times n + p} \to \{0,1\}^{pn} \leftarrow \text{p-WEAK PIGEON instance}$$

oracle solves it.

$$C^p(x_1, \dots, x_p) = C^p(x_1', \dots, x_p')$$

$\exists i$ st $x_i \neq x_i'$ and $C(x_i) = C(x_i')$

This red. worked $P \leq P(n)$

WEAK-PIGEON is "robust" up to either 1 bit shrinkage, up to poly bits shrinkage

picture so far:

Existence theorem: Given an finite acyclic graph G, and a vertex of degree 1, there exists another vertex of deg. 1.

Pf: follow the path from deg-1 vertex.

How to define a comp. problem based on this?

Idea 1: input an adjacency matrix.

This problem $\in$ FP .

Idea 2: represent exponential size graph using circuits.

Fix d.

G a graph on $V = \{0,1\}^n$ represented by

$C : \{0,1\}^n \times \{0,1\}^{\log d} \to \{0,1\}^n$

where $C(u,i)$ for $i \in [d]$ gives the i-th neighbour of u.

If $C(u,i) = u$ represents no i-th neighbour.

Actually ... this defines a directed graph.

To represent undirected graphs, (u,v) have an edge if $C(u,i) = v$ and $C(v,j) = u$ for $i,j \in [d]$

<u>Def</u> (attempt) Given $d \le poly(n)$, G rep. by circuit C, and vertex v of deg 1, find another $u \ne v$ of deg 1.

Q: why $d \le poly(n)$?

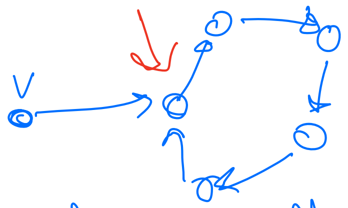
if $d = \Omega(poly(n))$, then ✓ search problem

✗ FNP

✓ yes in FNP.

As written, not in TFNP .... :(

Doesn't enforce acyclicity !!!



(would have another existence thm... a vertex of odd degree)

Let's think of syntactic ways to enforce acyclicity.

1 → PPA

2 → PPAD

3 → PLS

4 → PPP

} we'll see next week