Today

- Complete proof of a DNP-complete problem (under random reductions).
- Ajtai's reduction from worst-case to average-case for some lattice problems.

Recall from last time

- DNP problem given by (R, D); where $R \subseteq \{0,1\}^* \times \{0,1\}^*$ is a polytime-computable relation; and $D : \{0,1\}^* \to \{0,1\}^*$ is a polytime-computable function.
- Algorithm A is δ-good for (R, D) if it can solve R for all but δ fraction of instances drawn from $\{D(z)\}$, where z is uniform, in poly-time. (To solve R means to find the relative y such that $R(x, y)$ if one exists.)
- (R, D) in Avg-P if there exists $B(x, \delta)$ such that $B_\delta(\cdot) = B(\cdot, \delta)$ is δ-good for (R, D) and B runs in time poly in $|x|, 1/\delta$.

Last time (contd.)

- For $\alpha \geq 1$, D_1 α-dominates D_2 if for every x $\Pr_{D_1}[x] \geq \Pr_{D_2}[x]/\alpha$.
- A is δ-good for (R, D_1) implies A is $(\alpha \cdot \delta)$-good for (R, D_2).

Impagliazzo-Levin Lemma

Lemma: There exists a (essentially uniform) distribution U such that for every R, D there exists a relation R' such that (R, D) reduces to (R', U).

Basic idea:

- Will try to make the relation R' be R composed with D.
- Need to specify z in domain of R given $x = D(z)$.
- Can't ask to invert D — may be hard.
- So specify z essentially by x and an index $w \in \{0,1\}^k$ assuming $D^{-1}(x)$ has about 2^k members.
- (x, w) does specify such a z, provided we

pick x according to $D(z)$. But don't get uniformity!

– So hash (x, w) down to n-bit string u.

Details

- Instances of R' are tuples (u, k, h_1, h_2) where $u \in \{0,1\}^n$, and $h_1 : \{0,1\}^n \to \{0,1\}^k$ and $h_2 : \{0,1\}^{n+k} \to \{0,1\}^n$ are nice pairwise independent has functions.
- $R'((u, k, h_1, h_2), (z, y))$ if $u = h_2(D(z), h_1(z))$ and $R(D(z), y)$.
- Distribution on instances $D_1 = U$ is the following: $u \in_U \{0,1\}^n$, $k \in_U \{0, \ldots, n\}$, h_1, h_2 are uniform from their families.

Reduction

Need to reduce (R, D) to (R', U).

Reduction: Given x, guess k, and string w (supposedly $k = \log |D^{-1}(x)|$ and $w = h_1(z)$ where $z \in_U D^{-1}(x)$). Pick h_1, h_2 uniformly, and then let $u = h_2(x, w)$. Output (u, k, h_1, h_2).

Claim: Instances being generated essentially according to U.

Main step in proof: If we guess k correctly, then very likely there is a unique z such that $D(z) = x$ and $h_1(z) = w$.

Soundness of reduction

- Related distribution D_2 on R': Pick $z \in_U \{0,1\}^n$ and let $k = \log_2 |D^{-1}(D(z))|$. Let h_1, h_2 be uniform on their domain and let $u = h_2(D(z), h_1(z))$.
- Claim 1: (R', D_2) is at least as hard as (R, D).
- Claim 2: D_1 n-dominates D_2.
- Details left to the reader.

A DNP-complete problem

- Easy to massage above into a relation R'' and distribution U' which is actually uniform on its domain.
- But still don't have a single hard problem (i.e., relation and distribution).
- Use the universal relation [Levin].
- Hard problem: R_U has as instances pairs (R, x). $R_u((R, x), y)$ holds if $R(x, y)$.
- Claim R_U on uniform distribution on inputs is at least as hard as (R'', U) - since with probability $1/2^{|R''|}$ (a constant) we will generate R'' as the relation to be solved.

Interlude

- Now have a theory of average-case hardness for problems in NP.
- How does it relate to worst-case hardness?
- Wide open.
- Known techniques relating the two don't seem to work [Feigenbaum-Fortnow]. (Does not rule out all reductions - only known forms.)
- Can we say anything within NP?

Ajtai'96 : Shows that worst-case instances of an "empirically" hard problem can be reduced to random instances of a related problem.

- Major breakthrough!

Lattice problems

- Defn: Lattice L in $\mathbb{R}^n$ is a discrete additive subset of R^n.
  - Discrete: Exists $d > 0$ such that for every point $x \in L$, the ball of radius d around x contains only one point (x) from L.
  - Additive: $x, y \in L$ implies $x + y, x - y \in L$.

Specifying a lattice

- Primal specification: By basis: $b_1, \ldots, b_m \in \mathbb{R}^n$ (for $m \leq n$), b_i's linearly independent, and lattice $L = \{\sum_{i=1}^{m} z_i b_i | (z_1, \ldots, z_m) \in \mathbb{Z}^m\}$.
- Dual specification: By vectors: $b_1^*, \ldots, b_m^* \in \mathbb{R}^n$ (for $m \geq n$), and lattice $L = \{\mathbf{v} \in \mathbb{R}^n | \forall j,\ \langle \mathbf{v}, \mathbf{b}_j^* \rangle \in \mathbb{Z}\}$.
- Can go from one rep'n to another algorithmically.

Lattice problems

- Given lattice L, compute shortest non-zero vector in in lattice. Was open for long time, till [Ajtai] showed it to be NP-complete for randomized reductions.
- Given lattice L and target vector $t \in \mathbb{R}^n$ compute nearest lattice point to t. (Long know to be NP-hard.)
- Given lattice, find short basis.
- Best algorithmic result: Can find $2^{o(n)}$ approximation for all above problems in poly time, for n-dimensional lattice.
- Shortest vector problem/Closest vector problem are of fundamental interest:

- Used in factoring polynomials over integers [LLL].
- Important case of Diophantine approximations.
- Used widely in cryptanalysis.
- Now becoming a basis for cryptography [Ajtai-Dwork].

Ajtai's theorem

Roughly, gives approximation problems R, R' and distribution D such that an avg-P solution to (R, D) implies a RP algorithm for R'.

- R': Instance is a pair — a lattice L and a bound M with the promise that there exists a basis for L with vectors of length at most M. Witness is a basis $b_1, \ldots, b_m$ where all vectors have length at most $\mathrm{poly}(n) \cdot M$.
- R: Instance is a pair — lattice L given by dual vectors $b_1^*, \ldots, b_m^*$ and a bound N with the promise that L has a vector of length at most N. Witness is a vector of length $\mathrm{poly}(n) \cdot N$.

- D: Fix $q = \mathrm{poly}(n)$ and $m = O(n \log q)$, and $N = \mathrm{poly}(n)$. Pick $b_1^*, \ldots, b_m^*$ randomly from $\{0, 1/q, \ldots, q - 1/q, 1\}^n$.

Intuition

Rapid Hand-waving.