Witness Theorems.

NP-Completeness Theorem.
HN_R is universal NP-complete problem (over R, an integral domain or field).
(eg $\mathbb{Z}_2$, $\mathbb{R}$, $\mathbb{C}$)

Let $\widetilde{Q}$ be the algebraic closure of $\mathbb{Q}$.

Transfer Theorem. P = NP over $\mathbb{C} \Leftrightarrow$ P = NP over $\widetilde{Q}$.
Can replace $\mathbb{C}$ by any algebraically closed field F of characteristic 0.

A key element in the proof is to show how to quickly test if a polynomial $F_x(t) = F(x, t_1, ..., t_n) \equiv 0$. Here $x = (x_1, \dots, x_p) \in \widetilde{Q}^p$ and $t = (t_1, ..., t_n)$ are indeterminants substituting for algebraically independent constants built into a machine over $\mathbb{C}$ (which we want to eliminate).

If the polynomial is given in standard form then $F_x(t) \equiv 0$ if and only if all the coefficients are 0. But the polynomial may be presented in other forms, e.g. as a straight line program, as in this case. We want to ***quickly construct*** a **witness w** such that $F_x(\mathbf{w}) = 0$ implies $F_x \equiv 0$.

This is of independent interest.

Theorem (DeMillo & Lipton, 1978; Schwartz, 1980; Zippel, 1979).
Suppose $\mathbb{F}$ is an integral domain and $p \in \mathbb{F}[x_1, \dots, x_n]$ of degree d and $S \subset \mathbb{F}$. If $p \not\equiv 0$, then

$$\Pr_{w \in S^n}[p(w) = 0] \leq \frac{d}{|S|}.$$

This is the basis of many probabilistic algorithms and also for transfer results such as:
P = NP$_{\mathbb{C}} \Longrightarrow$ BPP $\supset$NP (bit model).

Theorem (Kabanets & Impagliazzo, 2004).
If (in the bit model) one can test in polynomial time whether a polynomial $F \in \mathbb{Z}[x_1, \dots, x_n]$ given by an arithmetic circuit is identically zero, then get lower bounds. In particular, then either i) NEXP $\not\subset$ P/poly or ii) Permanent is not computable by polynomial size arithmetic circuits.

Two Witness Theorems give polynomial time tests in the algebraic model.

Given $G \in \mathbb{Z}[t_1,\ldots,t_m]$. **Define $\tau(G)$:**
Consider the finite sequences: $(u_0, u_1,\ldots, u_m, u_{m+1}, \ldots, u_{m+s} = G)$
where $u_0 = 1$, $u_1 = t_1$, …, $u_m = t_m$, and for $m < k \le m+s$, $u_k = v*w$ for some $v, w \in \{u_0, u_1, \ldots, u_{k-1}\}$ and $*$ is $+$, $-$ or $\times$. Then $(u_0, u_1,\ldots, u_m, u_{m+1}, \ldots, u_{m+s} = G)$ is a straight line program for G and $\tau(G)$ is the minimum such $s+1$.

Let $F(x, t) = F(x_1, \ldots, x_p, t_1, \ldots, t_n)$ be a polynomial in p+n variables with coefficients in $\mathbb{Z}$.
For each $x \in \widetilde{\mathbb{Q}}^p$, let $F_x \in \widetilde{\mathbb{Q}}$ **[$t_1, \ldots, t_n$]** be defined as $F_x(t) = F(x, t)$.
Definition. $w = (w_1, \ldots, w_n) \in \widetilde{\mathbb{Q}}^n$ is a **witness** for F_x if : $F_x(w) = 0 \Longrightarrow F_x \equiv 0$.

1. **Witness Theorem (BCSS,1996)**
Suppose N is a positive integer satisfying: $\log N \ge 4(p+n)\tau^2 + 4\tau$, $\tau = \tau(F)$.
Then for each $x \in \widetilde{\mathbb{Q}}^p$, there exists w_1 in $\{2^N, x_1^N,\ldots, x_p^N\}$ such that
$w = (w_1, \ldots, w_n)$, where $w_{i+1} = w_i^N$, is a witness for F_x .* (In particular, over $\widetilde{\mathbb{Q}}$, we can choose w_1 of largest height in $\{2^N, x_1^N,\ldots, x_p^N\}$.)

*By the Transfer property for algebraically closed fields, $\widetilde{\mathbb{Q}}$ can be replaced by any algebraically closed field of characteristic 0.

Proof uses properties of heights of algebraic numbers.

Def. Let **W'(n, p, v)** be the set of polynomials over $\mathbb{C}$ in **n variables** that can be computed by **straight-line programs of length at most v** using **p complex parameters**.

2. **Theorem (P. Koiran, 1997)**
There are are universal constants c_1 and c_2 such that the following holds:
Let $d = 2^{(n+v)^{c_1}}$ and $M = 2^{2^{(n+v)^{c_2}}}$. (Can let $d = 2^{v^{c_1}}$ and $M = 2^{2^{v^{c_2}}}$.)
Let $v_1,\ldots,v_{n(p+1)}$ be a sequence of integers such that
$v_1 \ge M+1$ and $v_k \ge 1 + d^{k-1}v_{k-1}^d$ for $k \ge 2$.
Let $u_1,\ldots,u_s$ be a sequence of points in N^n defined by: $u_i = (v_{1+n(i-1)}, v_{2+n(i-1)}, \ldots, v_{ni})$.
Then $(u_1,\ldots,u_{p+1})$ is a correct test sequence for W'(n,p,v).

Def. Let F be a family of polynomials in $K[x_1, \ldots, x_n]$. A sequence $\{u_i\}$ $i=1, \ldots, s$ of points in K^n is a **correct test sequence** for F if for any $p \in F$, $p(u_i) = 0$ for all $i = 1, \ldots, s$, implies $p \equiv 0$.

(By the Transfer property for algebraically closed fields, $\mathbb{C}$ can be replaced by any algebraically closed field of characteristic 0.)

Proof uses fast quantifier elimination for algebraically closed fields giving bounds on sizes of integers coefficients.

Proof of Witness Theorem 1.

See, Lang, Diophantine Geometry, Springer-Verlag, 1991 and BCSS (1996,1998).
Over $\widetilde{Q}$ there is a height function H: $\widetilde{Q} \to R^+$ (see Lang) with the following properties:

Proposition 3.

a. **H(1) = H(0) =1; H(2) = 2, H(w) ≥ 1, H(-w) = H(w), H (1/w) = H (w)**
b. **H(v+w) ≤ 2H(v) H(w)**
c. **$H(w^k) = H(w)^k$, H(vw) ≤ H(v) H(w)**
d. **H(v+w) ≥ 1/2H(v)/H(w)**
e. **H(vw) ≥ H(v)/H(w) if w≠ 0**

(Over $\mathbb{Q}$, we can define a height function H(p/q) = max (|p|,|q|) where gcd (p,q) =1; and H (0) =1.
Exercise: Check Proposition 3 over $\mathbb{Q}$ with this height function.)

a, b ⟹ d: H(v) = H ((v+w) –w) ≤ 2H(v+w)H(w) ∴ H(v+w) ≥ ½ H(v)/H(w).
a, c ⟹ e: H(v) = H (vw(1/w)) ≤H(vw)H(w) ∴ H(vw) ≥ H(v)/H(w).

Also, in general (from b):

$$H(\sum_{i=0}^{n} v_i) \le 2^n \prod_{i=0}^{n} H(v_i).$$

Let $g(t)=\sum_{i=0}^{d} a_i t^i \in \widetilde{Q}[t]$ be a polynomial in **one variable** over $\widetilde{Q}$ of degree d.

Define. $H(g)=\prod_{i=0}^{d} H(a_i)$.

Want to prove: If H(w) > 2^dH(g) then: g(w) = 0 ⟹ g≡0.

Proposition 4. For $w \in \widetilde{Q}$, H(g(w)) ≤ 2^dH(w)^{d}H(g). (Use Horner's rule.)
Proof.

$$H(g(w)) = H(\sum_{i=0}^{d} a_i w^i) = H(a_0 + w(a_1 + w(a_2 + \ldots + w(a_{d-1} + wa_d))\ldots))$$

$$\le_{(3b,3c)} 2^d H(a_0)H(w)H(a_1)H(w)\ldots H(a_d)H(w) = 2^d H(w)^d H(g).$$ ■

Proposition 5. Suppose d > 0. Then, for $w \in \widetilde{Q}$, H(g(w)) ≥ H(w)/2^dH(g).

Proof. (Uses Propositions 3 and 4.)

$$H(g(w)) = H(a_d w^d + \sum_{i=0}^{d-1} a_i w^i) \geq_{(3d)} 1/2 \frac{H(a_d w^d)}{H(\sum_{i=0}^{d-1} a_i w^i)} \geq_{(3c,3e)} 1/2 \frac{H(w^d)}{H(a_d) H(\sum_{i=0}^{d-1} a_i w^i)}$$

$$\geq_{(4)} 1/2 \frac{H(w^d)}{H(a_d) 2^{d-1} H(w)^{d-1} H(a_0) H(a_1) \ldots H(a_{d-1})} =_{(3c)} (1/2^d) \frac{H(w)}{H(g)}$$ ■

*****Corollary. If H(w) > 2^dH(g) then: g(w) = 0 ⟹ g≡0.**

Proof. By Proposition 5, if H(w) > 2^dH(g), then H(g(w)) > 1. ■

Many variables:

Let $G(t) = \sum_\alpha a_\alpha t^\alpha = \sum_{\alpha=(\alpha_1,\ldots,\alpha_n)} a_\alpha t_1^{\alpha_1} \ldots t_n^{\alpha_n} \in \widetilde{Q}[t_1,\ldots,t_n]$ be a polynomial **in n variables** over $\widetilde{Q}$.

Define. $H(G) = \prod_\alpha H(a_\alpha)$.

Proposition 6. Suppose G ∈ Z[t_1, …, t_m] and τ = τ(G). Then $H(G) \leq 2^{2^{(2m\tau^2)}}$.

Lemma 1. Let D = 2^τ. Then the degree of G is less than or equal to D. The number of monomials in G, indexed by α, is less than D^m.

Proof of Proposition 6.
Induction on τ. τ =1, ok!
Let G = FF' where τ(F), τ(F') < τ. (Other cases easier.)

Let $F(t) = \sum_\alpha a_\alpha t^\alpha$, $F'(t) = \sum_\beta b_\beta t^\beta$ and $G(t) = \sum_\gamma c_\gamma t^\gamma$ where $c_\gamma = \sum_\beta a_{\gamma-\beta} b_\beta$.

Here $\alpha = (\alpha_1,\ldots,\alpha_m), \beta = (\beta_1,\ldots,\beta_m)$ and $\gamma = (\gamma_1,\ldots,\gamma_m)$.

The degrees of F, F' and G are ≤ D. The number of terms of each are ≤ D^m.

So, $H(c_\gamma) \leq 2^{D^m} \prod_\beta H(a_{\gamma-\beta}) H(b_\beta) \leq 2^{D^m} H(F) H(F')$.

So, $H(G) \leq (2^{D^m} H(F) H(F'))^{D^m} \leq_{\text{by induction}} 2^{D^{2m}} ((2^{2^{(2m(\tau-1)^2)}})(2^{2^{(2m(\tau-1)^2)}}))^{D^m} = 2^{D^{2m}} (2^{2^{(2m(\tau-1)^2)}+1})^{D^m}$.

So, $H(G) \leq 2^{D^{2m}} 2^{D^m 2^{2m(\tau-1)^2+1}}$

So, $\log H(G) \leq D^{2m} + D^m 2^{2m(\tau-1)^2+1} = 2^{2m\tau} + 2^{m\tau} 2^{2m(\tau-1)^2+1} \leq_{\text{do the arithmetic}} 2^{2m\tau^2}$, for $\tau \geq 2$. ■

For $x = (x_1, ..., x_p) \in \widetilde{Q}^p$, let $H(x) = \max H(x_i)$.

For $G = \sum a_\alpha t^\alpha \in \widetilde{Q}\ [t_1, ..., t_n]$ and $x = (x_1, ..., x_p) \in \widetilde{Q}^p$, $p < n$,

let $G_{x_1,..,xp}(t_{p+1}, ..., t_n) = G(x_1, .., x_p, t_{p+1}, ..., t_n)$.

Proposition 7. $H(G_{x_1,...,x_p}) \le H(G)(2H(x))^{D^{n+1}}$, where degree G $\le$ D. (See Proposition 4.)

Proof.

$G_{x_1,..,x_p} \in \widetilde{Q}[t_{p+1}, ..., t_n]$ is a polynomial whose coefficients may be indexed by $(\alpha_{p+1}, ..., \alpha_n)$,

and for each $(\alpha_{p+1}, ..., \alpha_n)$, have the form $\sum_{\alpha=(\alpha_1,...,\alpha_p,\alpha_{p+1},...\alpha_n)} a_\alpha x_1^{\alpha_1} ... x_p^{\alpha_p}$. (Has $\le D^p$ monomials.)

Thus, $G_{x_1,..,x_p} = \sum_{(\alpha_{p+1},...,\alpha_n)} \left(\sum_{(\alpha_1,...,\alpha_p,\alpha_{p+1},...\alpha_n)} a_\alpha x_1^{\alpha_1} ... x_p^{\alpha_p} \right) t^{(\alpha_{p+1},...,\alpha_n)}$. (Has $\le D^{n-p}$ monomials.)

We must estimate the product of the heights of those coefficients (similar to Proposition 4).
The height of each coefficient:

$$\le 2^{D^p} \prod_{(\alpha_1,...,\alpha_p)} H(a_\alpha) H(x_1)^{\alpha_1} ... H(x_p)^{\alpha_p} \le 2^{D^p} \prod_{(\alpha_1,...,\alpha_p)} H(a_\alpha) H(x)^D.$$

Taking products of all coefficients:

$$H(G_{x_1,...,x_p}) \le 2^{D^n} H(G)(H(x))^{D^{n+1}}. \blacksquare$$

Now for proof of Witness Theorem:

$$F(x,t) = F\left(x_1, ..., x_p,\ t_1,\ ...,\ t_n\right) = \sum_{\alpha,\beta} a_{\alpha,\beta} x^\alpha t^\beta,\ \alpha = (\alpha_1, ..., \alpha_p),\ \beta = (\beta_1, ..., \beta_n), a_{\alpha,\beta} \in Z.$$

Let $\tau = \tau(F)$ and N be a positive integer satisfying: $\log N \ge 4(p+n)\tau^2 + 4\tau$.

Let x= $(x_1, ..., x_p) \in \widetilde{Q}^p$.

Choose w_1 of largest height from $\{2^N, x_1^N, \dots, x_p^N\}$ and let $w_{i+1} = w_i^N$, i =1,… , n.
Then $H(w_1) > 1$ and $H(w_{i+1}) = H(w_i)^N > H(w_i)$. Let $w = (w_1, \dots, w_n)$,

To show: $F_x(w) = 0 \Longrightarrow F_x \equiv 0$.

For each j = 1,…, n and $\widehat{\beta} = (\widehat{\beta}_{j+1}, ..., \widehat{\beta}_n)$ we define a one variable polynomial $G_{\widehat{\beta}}^j$ so we can reduce to the 1-variable case:

Define $G_{\widehat{\beta}}^j(t) = \sum_{\substack{\alpha=(\alpha_1,...,\alpha_p) \\ \beta=(\beta_1,...,\beta_j,\widehat{\beta}_{j+1},...,\widehat{\beta}_n)}} a_{\alpha,\beta} x^\alpha w_1^{\beta_1} ... w_{j-1}^{\beta_{j-1}} t_j^{\beta_j}$.

So if $\widehat{\beta} = \varnothing$ then $G_\varnothing^n(t) = \sum a_{\alpha,\beta} x^\alpha w_1^{\beta_1} ... w_{n-1}^{\beta_{n-1}} t_n^{\beta_n} = F_{x,w_1,...,w_{n-1}}(t_n)$.

and $G_\varnothing^n(w_n) = \sum a_{\alpha,\beta} x^\alpha w_1^{\beta_1} ... w_{n-1}^{\beta_{n-1}} w_n^{\beta_n} = F_x(w_1, ..., w_{n-1}, w_n)$.

Lemma 2. $H(w_j) > 2^D H(G^j_{\hat{\beta}})$ where $D = 2^\tau$.

*****So, by the Corollary to Proposition 5, if** $G^j_{\hat{\beta}}(w_j) = 0$, then $G^j_{\hat{\beta}} \equiv 0$.

Proof .

Sufficient to show: $H(w_j) > 2^D H(F_{x,w_1,\ldots,w_{j-1}})$

(since $F_{x,w_1,\ldots,w_{j-1}}(t) = \sum_{\substack{\alpha=(\alpha_1,\ldots,\alpha_p) \\ \beta=(\beta_1,\ldots,\beta_j,\hat{\beta}_{j+1},\ldots,\hat{\beta}_n)}} a_{\alpha,\beta} x^\alpha w_1^{\beta_1} \ldots w_{j-1}^{\beta_{j-1}} t_j^{\beta_j} t_{j+1}^{\beta_{j+1}} \ldots t_n^{\beta_n}$).

Or by Proposition 7, that: $H(w_j) > 2^D H(F) \left(2H\left((x_1, \ldots, x_p, w_1, \ldots, w_{j-1})\right)\right)^{D^{n+1}}$

Now by Proposition 6, letting m = p+n, it is sufficient to show:

$$H(w_j) > 2^D 2^{2^{(2m\tau^2)}} \left(2H(w_{j-1})\right)^{D^{n+1}} \text{ if j>1 or}$$

$$H(w_j) > 2^D 2^{2^{(2m\tau^2)}} \left(2\max(2, H(x)\right)^{D^{n+1}} \text{ if j=1.}$$

Take logs of LHS and RHS.

If j >1,

$\log(\text{LHS}) = \log H(w_j) = N \log H(w_{j-1})$

$\log(\text{RHS}) = D + 2^{(2m\tau^2)} + D^{m+1}(1 + \log(H(w_{j-1}))$

$= 2^\tau + 2^{(2m\tau^2)} + 2^{\tau(m+1)} + 2^{\tau(m+1)} \log(H(w_{j-1}))$

But, $\log N > \tau + 2m\tau^2 + 2(m+1)\tau$. (Easy to check, noting m = p+n.) So LHS > RHS.

(Similarly for case j=1 noting $H(w_1) = \max(2, H(x))^N$.) ■

For $j = n$, we have $\hat{\beta} = \varnothing$ and $G^n_\varnothing(t) = \sum a_{\alpha,\beta} x^\alpha w_1^{\beta_1} \ldots w_{n-1}^{\beta_{n-1}} t_n^{\beta n} = F_{x,w_1,\ldots,w_{n-1}}(t_n)$.

By Lemma 2, we have $H(w_n) > 2^D H(G^n_\varnothing)$.

So: $G^n_\varnothing(w_n) = 0 \Rightarrow G^n_\varnothing \equiv 0$.

So: $F_{x,w_1,\ldots,w_{n-1}}(w_n) = 0 \Rightarrow F_{x,w_1,\ldots,w_{n-1}} \equiv 0$.

So all the coefficients of $F_{x,w_1,\ldots,w_{n-1}}$ must be 0, that is: for each $\hat{\beta}_n$,

$$\sum_{\substack{\alpha=(\alpha_1,\ldots,\alpha_p) \\ \beta=(\beta_1,\ldots,\beta_{n-1},\hat{\beta}_n)}} a_{\alpha,\beta} x^\alpha w_1^{\beta_1} \ldots w_{n-1}^{\beta_{n-1}} = 0$$

Continuing to s-1, s-2, …, 1 we obtain eventually for any $\hat{\beta} = (\hat{\beta}_1, \ldots, \hat{\beta}_n)$ that $\sum_\alpha a_{\alpha,\hat{\beta}} x^\alpha = 0$.

Therefore, all coefficients of F_x are = 0. Therefore $F_x \equiv 0$. ■

<u>Outline Proof Witness Theorem 2.</u>

(Fast) QuantifierElimination Theorem. (Fichtas, Galligo and Morgenstern, 1990)
Let K be and algebraically closed field and Φ a 1st order formula over K in prenex form.
Let **| Φ| be the length of Φ, r the number of quantifier blocks, n total # of variables**, and

$\sigma\left(\Phi\right) = 2 + \sum_{i=1}^{s} \deg F_i$ where $\{F_i\}_{i=1}^{s}$ are the polynomials occuring in Φ.

Then Φ is equivalent to a quantifier free formula Ψ in which all polynomials have degree at most $2^{n^{O(r)}(\log\sigma(\Phi))^{O(1)}}$. The number of polynomials occurring in Ψ is $O(\sigma(\Phi)^{n^{O(r)}}$.
Moreover, if ch K = 0 and all the constants in Φ are integers of bit size at most L,
the constants in Ψ are integers of bit size at most $L2^{n^{O(r)}(\log\sigma(\Phi)^{O(1)}}$.

Comment. By quantifier elimination, every set definable by a 1st order formula Φ over K is a union of quasi-algebraic sets defined by systems of the type:
$P_1(x) = 0, \ldots, P_k(x) = 0, Q_1(x)\neq 0, \ldots, Q_m(x) \neq 0$ where the P_i's and Q_j's are polynomials in *n* variables $x = (x_1, \ldots, x_n)$ over K. (So, if all constants in Φ are integers, then above gives bounds on each of the coefficients in the P's and Q's.)

Lemma A. (Sontag,1996, also implicit in Heintz, Schnorr, 1980)
Let P: $C^p \times C^n \to C$ be a polynomial map.
For $l \in$ N, let $A_l = \{(u_1,\ldots,u_l) \in C^{\ln} \mid \exists\alpha \in C^p[P(\alpha,.) \neq 0 \wedge P(\alpha,u_1) = 0 \wedge \ldots \wedge P(\alpha,u_l) = 0]\}$.
Then A_l is a quasi-algebraic set of dimension at most p+*l*(n-1).
So, A_{p+1} has dimension at most pn + n - 1 in C^{pn+n}, i.e. A_{p+1} has positive co-dimension.
So "most" sequences of length p+1 are correct test sequences for the family$\{x \mapsto P(\alpha, x) \mid \alpha \in C^p\}$.

Lemma B. (Heintz, Schnor, 1980; Koiran 1997)

Let $P \in Z[X_1, \ldots, X_n]$ be a degree d poly with coefficients bounded by M in absolute value.
Let $w = (w_1, \ldots, w_n)$ be any sequence of integers satisfying
$w_1 \geq M + 1$ and $w_k \geq 1 + M(d+1)^{k-1} w_{k-1}^{d}$ for $k \geq 2$.
Then, if P is not identically zero, $P(w) \neq 0$.

Proof of Witness Theorem 2.

Fix a straight line program of length $\leq$ v which uses p parameters and let $P = \{P_{\alpha} \mid \alpha \in C^p\}$ be the family of polynomials computed by the straight-line program as α ranges over C^p.

Let S be the set of correct test sequences of length p+1 for P. Then.

$$u = (u_1, \ldots, u_{p+1}) \in S \subset C^{(p+1)n} \Leftrightarrow \forall\ \alpha \in C^p\ \forall\ x \in C^n [\vee_{i=1}^{p+1} P_{\alpha}(u_i) \neq 0 \vee P_{\alpha}(x) = 0].$$

By adding v universally quantified variables for the values computed at each stage in the straight line program, the condition $P_{\alpha}(x) = 0$ can be expressed by a 1st order formula of length O(v).

Similarly, for each of the p+1 conditions, $P_{\alpha}(u_i) \neq 0$.

Now put the above formula in prenex formula with a single block of universal quantifiers and at most p + (n+v)(p+2) variables.

By Quantifier Elimination, S is the union of basic quasi-algebraic sets $S_1, \ldots, S_k$.

Since the map $(\alpha, x) \mapsto P_{\alpha}(x)$ is polynomial, by Lemma A, S is full dimensional.

Therefore, one of the quasi-algebraic sets that make up S must be defined by inequations of the form: $Q_1(u) \neq 0, \ldots, Q_m(u) \neq 0$.

By Quantifier Elimination, there is a $2^{(n+v)^{O(1)}}$ bound on the degree and bit size of the Q_i's.

Then, by Lemma B, $(u_1, \ldots, u_{p+1})$ is a correct test sequence for W'(n,p,v). ■