Recall From Last Time

Gödel's Completeness Theorem of First-Order Logic

For all first-order formulas, φ, and sets of first-order formulas, Γ,

$$\Gamma \models \varphi \quad \Leftrightarrow \quad \Gamma \vdash \varphi$$

From now on we use the following notation:

$\mathcal{A} \models \varphi$

$\Gamma \vdash \varphi$

Compactness Theorem:

Let Γ be a set of first-order formulas.

Suppose every finite subset of Γ has a model.

Then Γ has a model.

Proof: Suppose that Γ is inconsistent, i.e., $\Gamma \vdash \bot$

Then since proofs are finite, there is a finite subset $\Gamma_0 \subseteq \Gamma$ s.t. $\Gamma_0 \vdash \bot$.

Since Γ_0 is finite, it has a model, $\mathcal{A} \models \Gamma_0$

Thus, by the Soundness Theorem, $\mathcal{A} \models \bot$

$\Rightarrow\Leftarrow$ Thus Γ is consistent.

By the Completeness Theorem, Γ has a model. $\square$

Compactness Applications

$$\begin{aligned} \text{Theory}(\mathbf{N}) &= \{\varphi \in \mathcal{L}(\Sigma_N) \mid \mathbf{N} \models \varphi\} \\ \Gamma &= \text{Theory}(\mathbf{N}) \cup \{c > 0, c > 1, c > 2, c > 3, \ldots\} \end{aligned}$$

Claim: Γ has a model, $\quad N' \models \Gamma$

Proof: Every finite subset of Γ is satisfiable by $(\mathbf{N}, i)$ for i sufficiently large. Thus, by Compactness, Γ is satisfiable. $\square$

Thus, there is a countable model,

$$N' \models \text{Theory}(\mathbf{N}); \qquad N' \not\cong \mathbf{N}$$

Thus, $\mathcal{L}(\Sigma_N)$ cannot uniquely characterize **N**.

“Connectedness” is not expressible in $\mathcal{L}(\Sigma_g)$

Proof: Suppose that $\chi \equiv$ “I am connected.”

$$\Gamma \quad = \quad \{\chi\} \cup \{\neg\text{dist}(s,t,1), \neg\text{dist}(s,t,2), \neg\text{dist}(s,t,3), \ldots\}$$

$$\text{dist}(x_0, x_n, n) \quad \equiv \quad \exists x_1 \cdots x_{n-1} \left(\bigwedge_{i=0}^{n-1} (x_i = x_{i+1} \vee E(x_i, x_{i+1})) \right)$$

Every finite subset of Γ is satisfiable.
By Compactness, Γ has a model, $\mathcal{A}$.
$\mathcal{A}$ is not connected but $\mathcal{A} \models \chi$. $\Rightarrow\Leftarrow$ $\square$

Thus “Connectedness” is not expressible in the first-order language of graphs.

Downward Lowenheim-Skolem Theorem:

If a set of first-order formulas, Γ, has any model at all, Then it has a **countable** model.

Proof: Suppose that Γ has a model.

By the Soundness Theorem, Γ is consistent.

By our proof of the Completeness Theorem, there is a model, $\mathcal{A}$ of Γ whose universe consists of the equivalence classes of the witness constants: $c_1, c_2, \ldots$, i.e., $\mathcal{A}$ is countable. $\square$

The set of real numbers is **uncountable**. But if we define a first-order vocabulary to talk about $\mathbf{R}$, we get a first-order theory, $\text{Theory}(\mathbf{R})$, the set of sentences that are true of $\mathbf{R}$. This theory has a countable model!

Kind of weird.

Zermelo Fraenkel Set Theory plus the Axiom of Choice

ZFC is a first-order axiomatization of set theory.

Extensionality: $\forall x, y(\forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y)$

If two sets have the same elements then they are equal

Empty Set: $\exists x \forall y (y \notin x)$

There is a (unique) empty set; let's call it $\emptyset$

Plus 7 more axioms . . .

"The reader should be reasonably convinced even on a first reading that the axioms easily encompass all of traditional mathematics,"

Paul J. Cohen, *Set Theory and the Continuum Hypothesis*

ZFC is something like what Hilbert was asking for.

Back to the Compactness Theorem

If ZFC is consistent, then it has a countable model, $\mathcal{A}$.

Thus, if you believe Paul Cohen, then $\mathcal{A}$ is a model of all of mathematics. In particular, it has $\mathbf{N}, \wp(\mathbf{N}), \wp(\wp(\mathbf{N})), \ldots$.

Furthermore, ZFC $\vdash$ "$\wp(\mathbf{N})$ is uncountable."

Thus, $\mathcal{A} \models$ "$\wp(\mathbf{N})$ is uncountable."

How can this be, when all these sets are part of the countable universe, $|\mathcal{A}|$?

What does $\mathcal{A} \models$ "$\wp(\mathbf{N})$ is uncountable" mean?

It means that there is no $f : \mathbf{N} \overset{\text{1:1}}{\underset{\text{onto}}{\rightarrow}} \wp(\mathbf{N})$.

Now $\mathbf{N}^{\mathcal{A}}, \wp(\mathbf{N})^{\mathcal{A}} \subseteq |A|$, so they are both countable, so there is such an f.

However, $f \notin |\mathcal{A}|$

$\mathcal{A} \models$ "$\wp(\mathbf{N})$ is uncountable"

Formal Number Theory

$$\begin{aligned}
\mathrm{NT}_1 &\equiv \forall x(\sigma(x) \neq 0) \\
\mathrm{NT}_2 &\equiv \forall xy(\sigma(x) = \sigma(y) \rightarrow x = y) \\
\mathrm{NT}_3 &\equiv \forall x(x = 0 \ \vee \ \exists y(\sigma(y) = x)) \\
\mathrm{NT}_4 &\equiv \forall x(x + 0 = x) \\
\mathrm{NT}_5 &\equiv \forall xy(x + \sigma(y) = \sigma(x + y)) \\
\mathrm{NT}_6 &\equiv \forall x(x \times 0 = 0) \\
\mathrm{NT}_7 &\equiv \forall xy(x \times \sigma(y) = (x \times y) + x) \\
\mathrm{NT}_8 &\equiv \forall x(x \uparrow 0 = 1) \\
\mathrm{NT}_9 &\equiv \forall xy(x \uparrow \sigma(y) = (x \uparrow y) \times x) \\
\mathrm{NT}_{10} &\equiv \forall x(x < \sigma(x)) \\
\mathrm{NT}_{11} &\equiv \forall xy(x < y \rightarrow \sigma(x) \leq y) \\
\mathrm{NT}_{12} &\equiv \forall xy(\neg(x < y) \leftrightarrow y \leq x) \\
\mathrm{NT}_{13} &\equiv \forall xyz((x < y \wedge y < z) \rightarrow x < z) \\
\mathrm{NT}_{14} &\equiv \forall xy(\neg(x < 0) \ \wedge \ ((\sigma(x) < \sigma(y)) \rightarrow x < y))
\end{aligned}$$

$$\mathbf{N} \models \quad \mathrm{NT} \quad = \quad \bigwedge_{i=1}^{14} \mathrm{NT}_i$$

Th 6.1 [Papa]: Let φ have no variables. Then

$$\mathbf{N} \models \varphi \qquad \Leftrightarrow \qquad \mathrm{NT} \vdash \varphi$$

Proof: φ is a boolean combination of $t < t'$, $t = t'$.

Case 1: t, t' numbers: $\sigma(\sigma \cdots \sigma(0) \cdots)$.
= use $\mathrm{NT}_1, \mathrm{NT}_2$
$<$ use NT_{10}, NT_{13}, NT_{14}

Case 2: t, t' involve $+, \times, \uparrow$.
Use $\mathrm{NT}_4, \ldots, \mathrm{NT}_9$ to transform these to numbers. $\square$

Definition

A formula $\varphi \in \mathcal{L}(\Sigma_N)$ is **bounded** iff it can be written with all quantifiers in front, and all universal quantifiers bounded.

Example:

$$\forall x < 9\, \exists y\, \forall z < 2 \uparrow (x \times y)\, (x \uparrow 3 + z \uparrow 3 \neq 17)$$

Remark: If $\varphi(v)$ is bounded and has only one free variable, v, then S_φ is r.e., where,

$$S_\varphi \quad = \quad \left\{ n \in \mathbf{N} \;\middle|\; \mathbf{N} \models \varphi(n) \right\} .$$

Th 6.2 [Papa]: Let φ be a bounded sentence, i.e., no free variables. Then, $\mathbf{N} \models \varphi \quad \Leftrightarrow \quad \mathrm{NT} \vdash \varphi$.

Proof: $\Leftarrow$: Soundness Theorem.

$\Rightarrow$: induction on number of quantifiers in φ.

Assume: $\mathbf{N} \models \varphi$.

Base case: Th 6.1

Inductive step: $\varphi \equiv \exists x(\psi(x))$.

Thus, $\mathbf{N} \models \psi(n)$, for some $n \in \mathbf{N}$.

Thus, $\mathrm{NT} \vdash \psi(n)$

Thus, $\mathrm{NT} \vdash \varphi$.

Inductive step: $\varphi \equiv \forall x < t\,(\psi(x))$.

t is a closed term, thus, $\mathrm{NT} \vdash t = n$, for some $n \in \mathbf{N}$.

$$\mathrm{NT}_{10}, \mathrm{NT}_{11}, \mathrm{NT}_{14} \vdash (x < n \to x = 0 \lor x = 1 \lor \cdots \lor x = n-1)$$

$$\mathbf{N} \models \psi(i), \quad i = 0, \ldots, n-1$$

$$\mathrm{NT} \vdash \psi(i), \quad i = 0, \ldots, n-1$$

$$\mathrm{NT} \vdash \varphi$$

□

Definition

Let $f : \mathbf{N}^k \to \mathbf{N}$. Formula φ_f **represents** f iff for all $n_1, \ldots, n_k, m \in \mathbf{N}$,

$$f(n_1, \ldots, n_k) = m \qquad \Leftrightarrow \qquad \mathbf{N} \models \varphi_f(n_1, \ldots, n_k, m)$$

Example: $f(n) = n^2 + 1$.

Let $\varphi_f(n, m) \equiv (n \times n) + 1 = m$.

$$\mathbf{N} \models \varphi_f(n, m) \quad \Leftrightarrow \quad \mathbf{N} \models (n \times n) + 1 = m \quad \Leftrightarrow \quad f(n) = m$$

To Do Next:

Th: Every primitive recursive function is representable by a bounded formula.

Cor: K is representable by a bounded formula.

Th: FO-THEOREMS is **r.e.** complete.

Gödel's Incompleteness Th: There is no r.e. set of sentences Γ such that

- $\mathbf{N} \models \Gamma$, and
- $\Gamma \vdash \text{Theory}(\mathbf{N})$.

Lemma: Primitive Recursive relations: Prime, PR, IsSeq, length, and ItemR are representable by bounded formulas.
Proof: $\text{PR}(n, p)$ asserts that p is prime number n , by asserting that there exists a number,

$$s \quad = \quad 2^0 \times 3^1 \times 5^2 \times 7^3 \times 11^4 \times \cdots \times p^n$$

$$\begin{aligned}
x|y &\equiv \exists z < y+1\,(x \times z = y) \\
\mathsf{DE}(x,e,y) &\equiv x^e|y \ \wedge \ x^{e+1} \not| y \\
\text{Prime}(x) &\equiv x > 1 \ \wedge \ \forall y, z < x\,(y \times z \neq x) \\
\text{PR}(n,p) &\equiv \exists s\,(\text{Prime}(p) \ \wedge \ 2 \not| s \ \wedge \ \mathsf{DE}(p,n,s) \ \wedge \\
&\qquad \forall q \leq p \, \forall q' < q\,(\neg\text{Prime}(q) \ \vee \ \neg\text{Prime}(q') \\
&\qquad \vee \ \exists q'' < q\,(q' < q'' \wedge \text{Prime}(q'')) \\
&\qquad \vee \ \exists e < q(\mathsf{DE}(q',e,s) \wedge \mathsf{DE}(q,e+1,s))))
\end{aligned}$$

$$\begin{aligned}\text{IsSeq}(x) &\equiv \exists z < x\, \forall i < x\, \exists p < 2 \uparrow x\, (\text{PR}(i,p) \;\wedge \\ &\qquad ((i \le z+1 \;\wedge\; p|x) \;\vee\; (i > z+1 \;\wedge\; \neg p|x)))\end{aligned}$$

$$\begin{aligned}\text{length}(x,\ell) &\equiv \exists k,p,q\, (\text{IsSeq}(x) \;\wedge\; k+1=\ell \;\wedge\; \text{PR}(k,p) \\ &\qquad \wedge\, \text{PR}(\ell,q) \;\wedge\; p|x \;\wedge\; q \not| x)\end{aligned}$$

$$\text{ItemR}(x,i,e) \equiv \exists p\, (\text{IsSeq}(x) \;\wedge\; \text{PR}(i,p) \;\wedge\; \mathsf{DE}(p,e+1,x))$$

□

Th: Every Bloop function is represented by a bdd. formula.

Proof:

Base case: Obvious for initial function, s, and constant 0.

Inductive step: Assignment statement: Suppose that we are in a function defintion: def $f(x_1, \ldots, x_k)$

$v = g(y_1, \ldots, y_r)$

where inductively we may assume that g and $y_1, \ldots, y_r$ are represented by bdd. formulas.

$$\varphi_v(\overline{x}, v) \;\equiv\; \exists y_1, \ldots, y_r(\varphi_g(\overline{y}, v) \wedge \varphi_{y_1}(\overline{x}, y_1) \wedge \cdots \wedge \varphi_{y_r}(\overline{x}, y_r))$$

Inductive step:

a.times do

0. $v_0 = f_0(\overline{x}, \overline{v})$

1. $v_1 = f_1(\overline{x}, \overline{v})$

$\ldots$

$k-1$. $v_{k-1} = f_{k-1}(\overline{x}, \overline{v})$

end

To represent v_k after the times loop, we assert:

$$\exists s\,(\textbf{IsSeq}(s)\ \wedge\ \textbf{length}(s, a \times k)\ \wedge\ \forall i \le k\,\forall j \le a\,(\psi(s,i,j)))$$

where $\psi(s,i,j)$ asserts that item $j \times a + i$ of s is equal to $f_i(\overline{x}, \overline{v})$

and the v_ℓ are the appropriate previous values from s. □

Cor: K is representable by a bounded formula.

$$\varphi_K(n) \equiv \exists c\,(\mathsf{COMP}(n,n,c,1))$$

$$K = \left\{n \;\middle|\; \mathbf{N} \models \varphi_K(n)\right\}$$

$$K = \left\{n \;\middle|\; \mathrm{NT} \vdash \varphi_K(n)\right\}$$

Summary So Far: $$\mathrm{NT} = \bigwedge_{i=1}^{14} \mathrm{NT}_i$$

Definition: A formula $\varphi \in \mathcal{L}(\Sigma_N)$ is *bounded* iff it can be written with all quantifiers in front, and all universal quantifiers bounded.

Theorem 6.2 [Papa]: Let φ be a bounded sentence. Then

$$\mathbf{N} \models \varphi \qquad \Leftrightarrow \qquad \mathrm{NT} \vdash \varphi$$

Definition: φ_f *represents* f iff forall $n_1, \ldots, n_k, m \in \mathbf{N}$,

$$f(n_1, \ldots, n_k) = m \qquad \Leftrightarrow \qquad \mathbf{N} \models \varphi_f(n_1, \ldots, n_k, m)$$

Theorem: Every primitive recursive function is representable by a bounded formula.

Corollary: K is representable by a bounded formula.

$$
\begin{aligned}
\varphi_K(n) &\equiv \exists c(\mathsf{COMP}(n,n,c,1)) \\
K &= \{n \mid \mathbf{N} \models \varphi_K(n)\} \\
K &= \{n \mid \mathrm{NT} \vdash \varphi_K(n)\}
\end{aligned}
$$

Sameer's Corollary: S is representable by a bounded formula iff S is r.e.

$$W_i \;=\; \{n \mid M_i(n) = 1\} \;=\; \{n \mid \mathrm{NT} \vdash \exists c(\mathsf{COMP}(i,n,c,1))\}$$

Def: For a structure $\mathcal{A} \in \mathrm{STRUC}[\Sigma]$,

$$\begin{aligned} \mathrm{Theory}(\mathcal{A}) &= \{\varphi \in \mathcal{L}(\Sigma) \mid \mathcal{A} \models \varphi\} \\ \mathrm{Theory}(\mathbf{N}) &= \{\varphi \in \mathcal{L}(\Sigma_N) \mid \mathbf{N} \models \varphi\} \end{aligned}$$

Gödel's Incompleteness Theorem: There is no r.e. set of sentences Γ such that

1. $\mathbf{N} \models \Gamma$, and
2. $\Gamma \vdash \mathrm{Theory}(\mathbf{N})$.

There is no axiomatization of number theory, much less all of mathematics.

Proof: Let Γ be r.e. and $\mathbf{N} \models \Gamma$.

$$S \quad = \quad \{n \in \mathbf{N} \mid \Gamma \vdash \neg\varphi_K(n)\}$$

S is r.e. and $S \subseteq \overline{K}$.

Intuitively, $\quad S \quad = \quad \{n \in \mathbf{N} \mid \Gamma \vdash n \in \overline{K}\}$

Since $\overline{K}$ is not r.e., there exist infinitly many $n \in \mathbf{N}$ s.t.,

$$\mathbf{N} \models \neg\varphi_K(n) \quad \text{and} \quad \Gamma \not\vdash \neg\varphi_K(n) \qquad \Box$$

Th: FO-THEOREMS is **r.e.** complete.

Proof: We have already seen that FO-THEOREMS is **r.e.**.

Recall K is represented by bounded formula φ_K.

$$n \in K \quad \Leftrightarrow \quad \mathbf{N} \models \varphi_K(n) \quad \Leftrightarrow \quad \mathrm{NT} \vdash \varphi_K(n)$$

$$n \in K \qquad \Leftrightarrow \qquad \text{“}\mathrm{NT} \rightarrow \varphi_K(n)\text{”} \in \text{FO-THEOREMS}$$

Thus, $K \leq$ FO-THEOREMS.

$$f(n) = \mathrm{NT} \rightarrow \varphi_K(n)$$

□

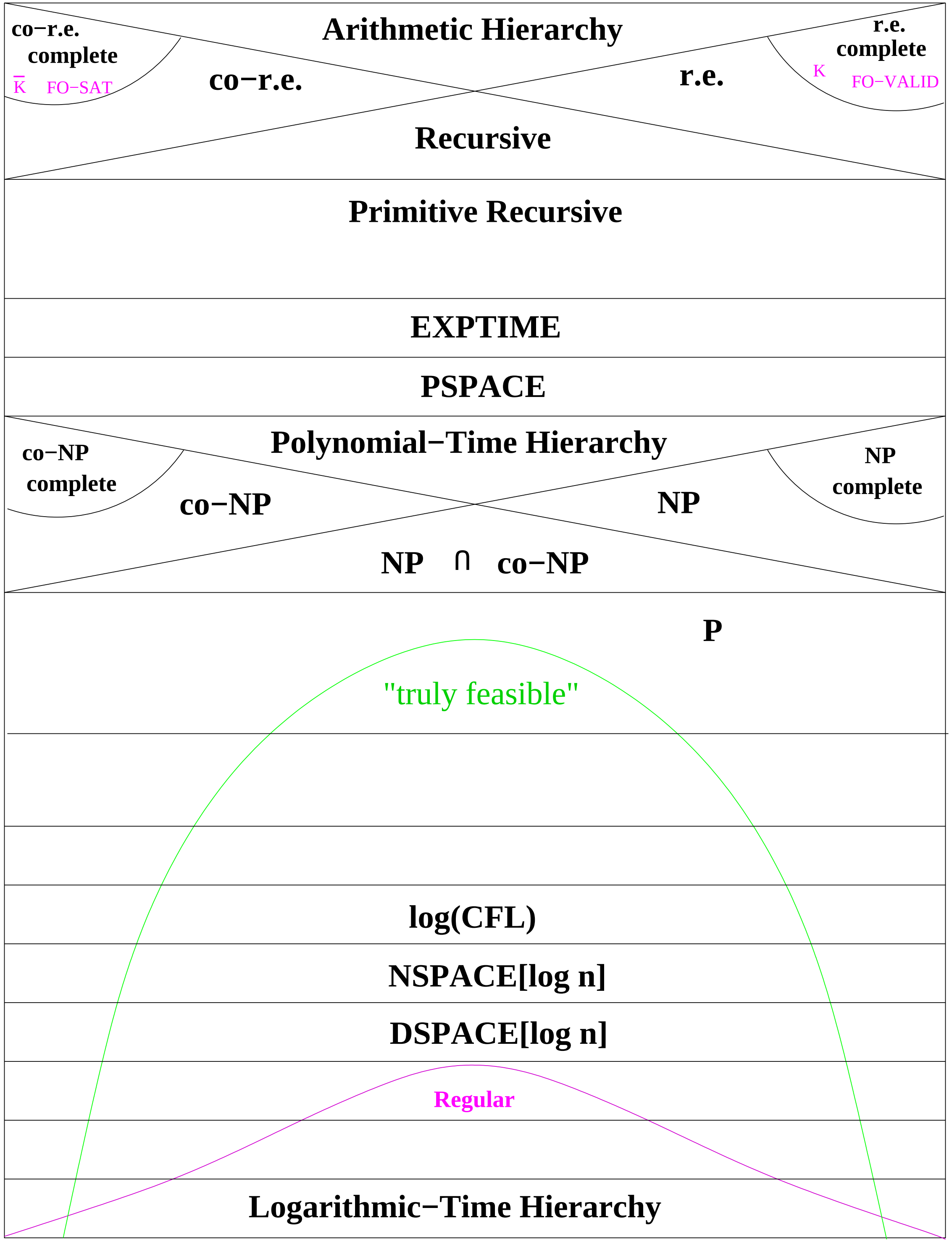
Sketch of Gödel's Original Proof

- Encode symbols as natural numbers.
- Encode formulas as finite sequences of natural numbers.
- Encode proofs as finite sequences of formulas.

- Let Γ be a primitive recursive axiomatization of some portion of mathematics including number theory.

  The following predicates are primitive recursive and thus definable by bounded first-order formulas:
  - Formula(x): "x is the number of a formula"
  - Axiom(x): "x is the number of an axiom"
  - Proof(x): "x is the number of a proof"
  - Theorem(x): "x is the number of a theorem"

- Let $R_0, R_1, \ldots$ list all formulas from $\mathcal{L}(\Sigma_N)$ with one free variable, i.e., all first-order definable sets.
- Let $G \quad = \quad \{n \mid \neg\,\text{Theorem}(R_n(n))\}$
- $G = \{n \mid R_q(n)\}$ for some q
- $R_q(q) \;\equiv\; \neg\,\text{Theorem}(R_q(q)) \;\equiv\;$ "I am not a theorem"
- If $R_q(q)$ then $\Gamma \not\vdash R_q(q)$; If $\neg R_q(q)$ then $\Gamma \vdash R_q(q)$.


Arithmetic Hierarchy
co−r.e.
complete
K̄ FO−SAT
co−r.e.
r.e.
r.e.
complete
K FO−VALID
Recursive
Primitive Recursive
EXPTIME
PSPACE
Polynomial−Time Hierarchy
co−NP
complete
co−NP
NP
NP
complete
NP ∩ co−NP
P
"truly feasible"
log(CFL)
NSPACE[log n]
DSPACE[log n]
Regular
Logarithmic−Time Hierarchy