Proofs, Large Functions and Combinatorics.

Stan Wainer (Leeds UK)

1. Finite Ramsey Theorem
2. Proofs in EA(I;0)
3. Proofs in PA
4. Large Sets, Modified Ramsey.

Finite Combinatorics – Ramsey's Theorem(s) 1930

$n = \{0, 1, 2, \ldots, n-1\}$

$n^{[k]}$ = all k-element subsets of n

$c : n^{[k]} \to \{0,1\}$ a "2-colouring" of $n^{[k]}$

$S \subseteq n$ is homogeneous/monochrome for c if c constant on $S^{[k]}$.

$n \to (\ell)^k_2$ means every $c : n^{[k]} \to 2$ has a homogeneous S of size ℓ.

EG. $6 \to (3)^2_2$

6 people: A, B, C, D, E, F

Either (a) A knows 3, say B, C, D

Or (b) A does not know 3

Case (a)

Either 2 of B, C, D know eachother in which case, with A, we have 3 people who mutually know eachother.

Or Not, in which case B, C, D are 3 who mutually do not know eachother.

Case (b) Similar

Finite Ramsey Theorem
$\forall k \, \forall \ell \, \exists n \left(n \rightarrow (\ell)^k_2 \right)$

Proof for $k = 2$

Given ℓ compute $n = 2^{2\ell-1} - 1$.

Take any colouring $c : n^{[2]} \rightarrow 2$.

Find $n = S_1 \supseteq S_2 \supseteq \ldots \supseteq S_{2\ell-1}$
and $x_1 \in S_1$, $x_2 \in S_2$, $\ldots$, $x_{2\ell-1} \in S_{2\ell-1}$

Stage $i+1$ $\quad x_i := \min S_i$

$S_{i+1} := \{ z \in S_i : c(x_i, z) = j \}$ $\quad j = 0$ or 1

so that $|S_{i+1}| \geq \frac{1}{2}(|S_i| - 1)$.

Now define $d : \{x_1 \dots x_{2\ell-1}\} \to 2$

$d(x_i) =$ that $j : 0$ or 1 such that

$\forall z \in S_{i+1}\ (c(x_i, z) = j)$

Then d splits $\{x_1 \dots x_{2\ell-1}\}$ into 2 subsets according as $j = 0$ or 1.

One of these subsets has size at least ℓ, say $\{x_{i_1} \dots x_{i_\ell}\}$, and this is our homogeneous set.

<u>Because</u> if $p < q$ and $r < s$

$$c(x_{i_p}, x_{i_q}) = d(x_{i_p})$$
$$= d(x_{i_r}) = c(x_{i_r}, x_{i_s}).$$

<u>Proof for k = 3</u>

Given ℓ compute $n = 2^{2\ell-1} - 1$

and $N = 2^{1 + {}^3C_2 + \dots + {}^nC_2}$

Take any colouring $c : N^{[3]} \to 2$

Find $N \setminus \{0\} = S_1 \supseteq S_2 \supseteq \dots \supseteq S_n$

and $x_1 \in S_1,\ x_2 \in S_2,\ \dots,\ x_n \in S_n$

<u>Stage i+1</u> $\quad x_i := \min S_i$

Split $S_i - \{x_i\}$ into equiv classes:

$y \equiv z$ iff $\forall x, x' \in \{0, x_1, \dots, x_i\}$

$c(x, x', y) = c(x, x', z)$

Choose $S_{i+1} :=$ largest equiv. class

Then $S_{i+1} \subseteq S_i - \{x_i\}$

and $|S_{i+1}| \geq \dfrac{|S_i| - 1}{2^{\,{}^{i+1}C_2}}$

because there are $\leq 2^{\,{}^{i+1}C_2}$ classes.

<u>N.B.</u> N is chosen so that $|S_n| \geq 1$.

By this definition if $i < j < k, k'$

$$c(x_i, x_j, x_k) = c(x_i, x_j, x_{k'})$$

So define $d : \{x_1 \dots x_n\}^{[2]} \to 2$ by

$$* \quad d(x_i, x_j) = c(x_i, x_j, x_k) \qquad j < k$$

By Ramsey$^{[2]}$ this d has a homogeneous ℓ-set $\{x_{i_1} \dots x_{i_\ell}\}$ which is homogeneous for c by $*$.

<u>Size of the Ramsey Function</u>

$R_k(\ell) :=$ least n. $n \to (\ell)^k_2$

$$2^{\ell/2} \lesssim R_2(\ell) \leq 2^{2\ell - 1}$$

$$2^{c\ell^2} \leq R_3(\ell) \leq 2^{2^{c\ell}}$$

$$2^{2^{c\ell^2}} \leq R_4(\ell) \leq 2^{2^{2^{c\ell}}}$$

$$\left.2^{2^{\cdot^{\cdot^{\cdot^{2^{c\ell^2}}}}}}\right\}k-2 \leq R_k(\ell) \leq \left.2^{2^{\cdot^{\cdot^{\cdot^{2^{c\ell}}}}}}\right\}k-1$$

Read Graham, Rothschild & Spencer.

A "Predicative" Arithmetic

Idea of E. Nelson '86 :-

- A number x is an object which satisfies all inductive formulas:

$$A(0) \wedge \forall a\,(A(a) \to A(a+1)) \to \underset{\forall b \leq x\, A(b)}{A(x)}$$

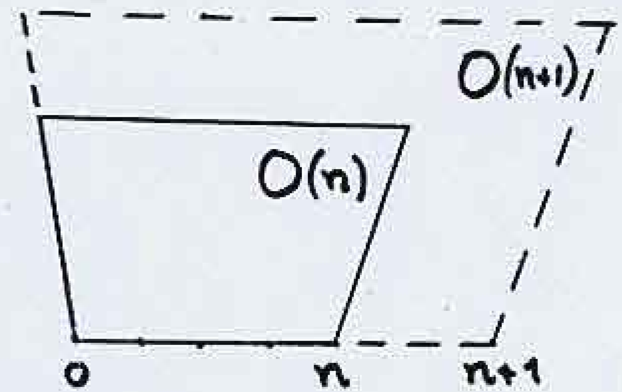
- Quantifying over numbers thus amounts to quantifying over all inductive formulas, including the one you might be trying to write down!

- This is impredicative.

- So allow input parameters $\vec{x} : I$
  Quantify output values $\vec{a} : O(\vec{x})$.

Formulas - $A(\vec{x}\,;\vec{a})$

"Models" - parameterized systems of output domains
$$O(\vec{x} := \vec{n})$$
satisfying finite inductions up to $\vec{n}$.



Extracting Bounds

Given $\vdash \exists a B(x;a)$ find $|O(n)|$ so that $\forall n\, \exists a \in O(n).\, B(n;a)$.

Theory $EA(I;O)$ cf. Leivant '95

Input numerical parameters x

Output computed values $a, b, ..$

> Only basic terms $a, a+1, a \dot{-} 1$
>
> Witness quantifiers $\exists a, \forall a$
>
> But add recursion equations for any partial rec. functions
>
> Then write $t{\downarrow}$ for $\exists a(t=a)$
>
> **By Logic** $t{\downarrow}, A(t) \vdash \exists a\, A(a)$
>
> $t{\downarrow}, \forall a\, A(a) \vdash A(t)$

> **PIND.** $A(0) \wedge \forall a(A(a) \to A(a+1)) \to A(x)$
>
> Once introduced, x remains free.

- **What you cannot do** –

$2.0{\downarrow},\ \forall a(2.a{\downarrow} \to 2.(a+1){\downarrow}) \vdash \forall a.\, 2a{\downarrow}$

$2^0{\downarrow},\ \forall a(2^a{\downarrow} \to 2^{a+1}{\downarrow}) \vdash \forall a.\, 2^a{\downarrow}$

Then another induction gives

$$\vdash \left.2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\right\}x \ {\downarrow} \qquad \text{etc.}$$

- **What you can do** –

$a+0{\downarrow},\ \forall b(a+b{\downarrow} \to a+(b+1){\downarrow}) \vdash a+x{\downarrow}$

Then $\vdash \forall a(a+x{\downarrow})$

$a+x.0{\downarrow},\ \forall b(a+x.b{\downarrow} \to a+x.(b+1){\downarrow}) \vdash a+x^2{\downarrow}$

Furthermore (à la Gentzen) :-

$\vdash \forall a(a+2^0{\downarrow}) \wedge \forall a(a+2^b{\downarrow}) \to \forall a(a+2^{b+1}{\downarrow})$

Hence $\vdash \forall a(a+2^x{\downarrow})$, etc.

- $\Sigma_1\text{-IND}(I;O) \vdash \forall a(a+p(\vec{x}){\downarrow})$

  $\Pi_2\text{-IND}(I;O) \vdash \forall a(a+2^{p(\vec{x})}{\downarrow})$

What you can do

(+) $$\cfrac{\cfrac{a+0\downarrow \qquad \forall b\,(a+b\downarrow \;\to\; a+(b+1)\downarrow)}{a+x\downarrow}}{\forall a\,(a+x\downarrow)}$$

(×) $$\frac{a+x\cdot 0\downarrow \qquad \forall b\,(a+x\cdot b\downarrow \;\to\; a+x\cdot(b+1)\downarrow)}{a+x\cdot y\downarrow}$$

These are Σ_1- inductions $(I;0)$.

(Exp) à la Gentzen :-

$$\frac{\forall a\,(a+2^0\downarrow) \qquad \forall a\,(a+2^b\downarrow)\to\forall a\,(a+2^{b+1}\downarrow)}{\forall a\,(a+2^x\downarrow)}$$

A Π_2-induction.

- $\Sigma_1\text{-IND}(I;0) \vdash \forall a\,(a+p(\vec{x})\downarrow)$
- $\Pi_2\text{-IND}(I;0) \vdash \forall a\,(a+2^{p(\vec{x})}\downarrow)$

E.G. $f(a,b,c) = a+(b!).(c+1)$

$$E \; \begin{cases} f(a,0,c) = a+(c+1) \\ f(a,b+1,0) = f(a,b,b) \\ f(a,b+1,c+1) = f(f(a,b+1,c),b,b) \end{cases}$$

$\Pi_2\text{-IND}(I;0) \vdash \forall a\,(f(a,x+1,0)\downarrow)$

$f(a,b+1,c)=d,\ f(d,b,b)\downarrow \vdash f(a,b+1,c+1)\downarrow$

By logic :

$\forall a(f(a,b,b)\downarrow),\ f(a,b+1,c)\downarrow \vdash f(a,b+1,c+1)\downarrow$

$\forall a(f(a,b,b)\downarrow) \vdash \forall a.\,f(a,b+1,c)\downarrow \to \forall a.\,f(a,b+1,c+1$

$\therefore\ \forall a(f(a,b,b)\downarrow) \vdash \mathrm{Prog}_c\ \forall a(f(a,b+1,c)\downarrow)$

By P-IND on c :

* $\forall a(f(a,b,b)\downarrow) \vdash \forall c\le x\ \forall a(f(a,b+1,c)\downarrow$

$\therefore\ b\le x\to\forall a.\,f(a,b,b)\downarrow \vdash b+1\le x\to\forall a.\,f(a,b+1,b+1$

By P-IND on b :

$\vdash x\le x \to \forall a(f(a,x,x)\downarrow)$

• Upper Bounds

1. Given $\quad EA(I;0) \vdash^{k}_{r} f(x)\downarrow$

   Fix $\quad x := n$

2. Unravel P-inductions up to n:-

$$\dfrac{\dfrac{A(0)\to A(1) \quad A(1)\to A(2)}{A(0)\to A(2)} \qquad \dfrac{A(2)\to A(3) \quad A(3)\to A(4)}{A(2)\to A(4)}}{A(0)\to A(4)}\ \text{Cut}$$

3. Def. Equns. + Logic $\vdash^{|n|.k}_{r} f(n)\downarrow$

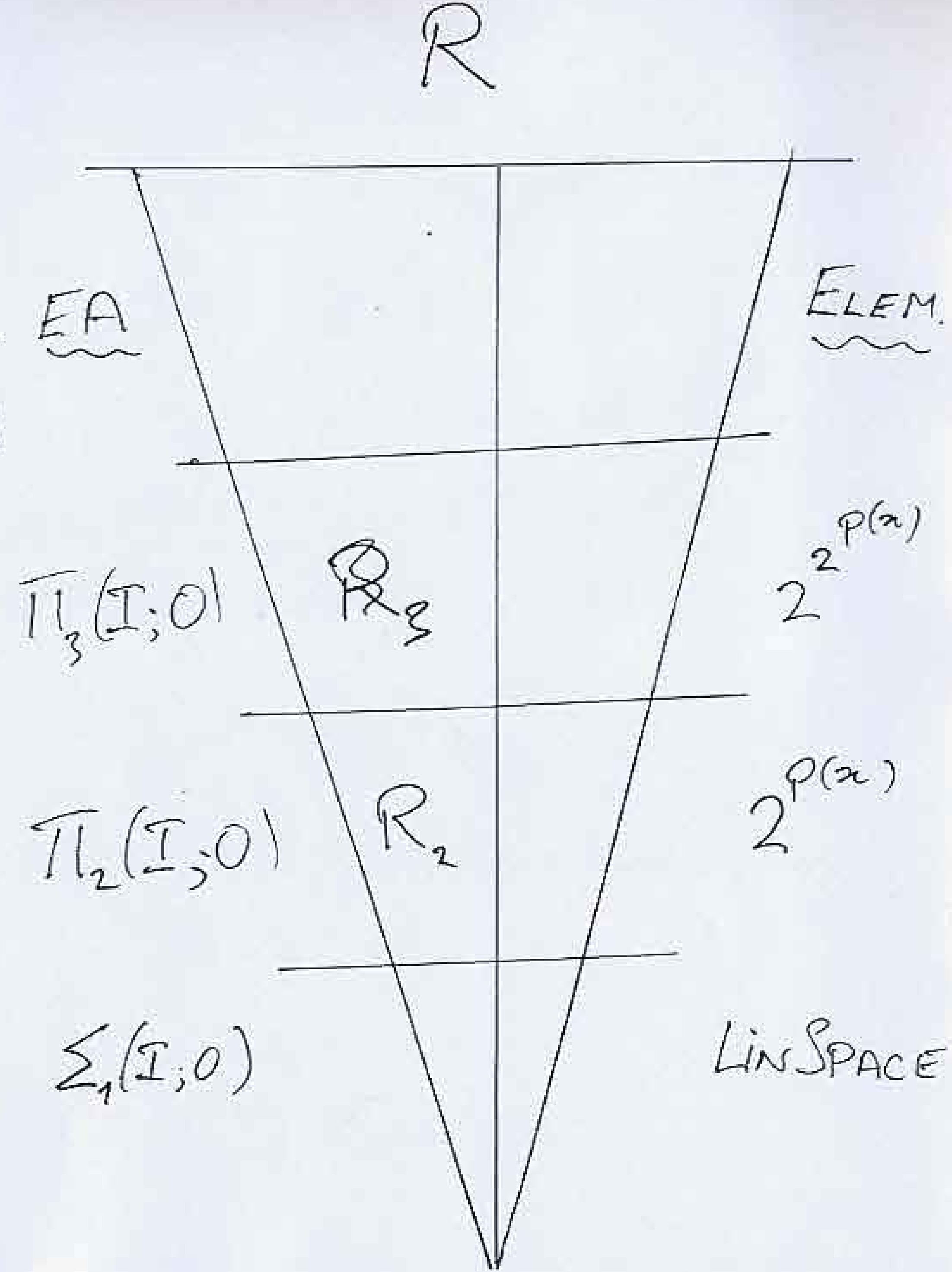
4. Cut-Reduce :-

   Def. Equns. + Logic $\vdash^{2^{2^{\cdot^{\cdot^{2^{|n|.k}}}}}}_{1} f(n)\downarrow$

5. Complexity = # nodes

   $\therefore\ f \in \mathrm{TIME}\left(2^{2^{\cdot^{\cdot^{2^{n^k}}}}}\Big\}{r-1}\right)$

EG. Σ_1-IND$(I;0) \equiv \mathcal{E}^2 \equiv$ LinSpace.



A deficiency

To derive composition in EA(I;0)

$$\frac{\vdash f(x)\downarrow \qquad \vdash g(x)\downarrow}{\vdash f(g(x))\downarrow}$$

is possible (Wirz) but complicated.

So add I-quantifier rules:

$$\frac{A(t(x))}{\exists x\, A(x)} \qquad\qquad \frac{A(x)}{\forall x\, A(x)}$$

Spoors: $\vdash \exists a(g(x){=}a) \Rightarrow \vdash \exists y(g(x){=}y)$

Then $$\frac{\dfrac{\vdash f(x)\downarrow \qquad \vdash g(x)\downarrow}{\vdash \forall y.\, f(y)\downarrow \wedge \exists y(g(x)=y)}}{\vdash f(g(x))\downarrow}$$

$\vdash_1 \Sigma_1 \cong$ computation

$$\text{Cut}\;\frac{\begin{array}{c} g \\ \big\downarrow \\ \exists c\, C(c) \end{array} \qquad \dfrac{C(c) \xrightarrow{\;f\;} \exists a\, A(a)}{\exists c\, C(c) \to \exists a\, A(a)}}{\exists a\, A(a)}$$

Then :-

$$\begin{array}{c} f\circ g \\ \big\downarrow \\ \exists a\, A(a) \end{array}$$

PROVABLE RECURSION IN PA AND INDEPENDENCE RESULTS.

Stan Wainer (Leeds UK)

Peano Arithmetic (PA) has :-

- Defining axioms for basic functions $succ, +, \times, \pi(x,y) = \langle x,y \rangle, \pi_1, \pi_2$ etcetera. Terms built up from these.
- Equality axioms $t_1 = t_2 \to A(t_1) \to A(t_2)$
- Induction axioms $A(0) \wedge \forall x (A(x) \to A(x+1)) \to \forall x A(x)$
- Classical logic $\Gamma \vdash A$ or $\vdash \neg\Gamma, A$.

$I\Sigma_n$ has restricted induction $A \in \Sigma_n$.

The Proof Theoretic Method – Extracting Complexity Bounds.

$$PA \vdash^{k}_{r} \forall x \exists y \, Spec(x,y)$$

$\Downarrow$ Unravel Inductions

$$\vdash^{\omega.k}_{r} \forall x \exists y \, Spec(x,y)$$

$\Downarrow$ Invert $\forall$

$$n : N \vdash^{\omega.k}_{r} \exists y \, Spec(n,y)$$

$\Downarrow$ Cut Elimination

$$n : N \vdash^{\alpha}_{0} \exists y \, Spec(n,y) \quad \alpha = \left.2^{2^{2^{\cdot^{\cdot^{\omega.k}}}}}\right\}r$$

$\Downarrow$ Bounding

$$\forall n \; \exists m < B_{\alpha}(n) \; Spec(n,m)$$

$\Downarrow$ Complete Cut-Elim.

$$\forall n \; \exists m < G_{\alpha^+}(n) \; Spec(n,m).$$

Embedding of PA

$$PA \overset{k}{\underset{r}{\vdash}} A(x) \Rightarrow n:N \overset{\omega.k}{\underset{r}{\vdash}} A(n)$$

Proof

Suppose $\forall x A(x)$ proven by Induction;

from $\overset{k-1}{\vdash} A(0)$ and $\overset{k-1}{\vdash} \forall x (A(x) \to A(x+1))$

$$\text{Cut}\ \frac{\text{Cut}\ \frac{\text{Cut}\ \frac{A(0) \quad A(0)\to A(1)}{A(1)} \quad A(1)\to A(2)}{A(2)} \quad A(2)\to A(3)}{A(3)}$$

$\ldots$ etcetera

$\therefore$ by successive A-Cuts :-

$$n:N \overset{\omega.(k-1)+n}{\underset{r}{\vdash}} A(n)$$

$\therefore$ By $(\forall)^\omega$ $\overset{\omega.(k-1)+\omega}{\underset{r}{\vdash}} \forall x A(x)$

Ordinal Presentations (Ω)

$$\alpha = \bigcup_n \alpha[0] \subset \alpha[1] \subset \ldots \subset \alpha[n] \subset \ldots$$

where $\alpha[n]$ finite

$\beta+1 \in \alpha[n] \Rightarrow \beta \in \alpha[n]$

$\beta \in \alpha[n] \Rightarrow \beta+1 \in \alpha[n+1]$

Predecessors : $P_n(\alpha) = \max \alpha[n]$

Rank Function : $G_\alpha(n) = \text{size}\ \alpha[n]$

EG : $\omega[n] = \{0, 1, 2, \ldots, n-1, n\}$

$G_\alpha(n) = \alpha(\omega := n+1)$

Infinitary System PA^∞

Logic :-

(Ax) $n{:}N \vdash^\alpha \Gamma$ if a true atom $\in \Gamma$

(∃) $\dfrac{n{:}N \vdash^\beta m{:}N \quad n{:}N \vdash^\beta \Gamma, A(m)}{n{:}N \vdash^\alpha \Gamma, \exists x A(x)}$ $\beta \in \alpha[n]$.

(∀) $\dfrac{\max(n,i){:}N \vdash^{\beta_i} \Gamma, A(i) \text{ all } i}{n{:}N \vdash^\alpha \Gamma, \forall x A(x)}$ $\beta_i \in \alpha[\max\ ]$.

+ Propositional rules + Cut.

Computation :-

(N1) $n{:}N \vdash^\alpha \Gamma, m{:}N$ if $m \le n+1$

(N2) $\dfrac{n{:}N \vdash^\beta m{:}N \quad m{:}N \vdash^\beta \Gamma}{n{:}N \vdash^\alpha \Gamma}$

Cut Elimination (Gentzen, Schütte, ...)

1. $n \vdash^\beta_r \neg C, B \,;\, n \vdash^\gamma_r C, B \Rightarrow n \vdash^{\beta+\gamma}_r B$ provided $\gamma[\ ] \subseteq \beta[\ ]$ and $|C| \le r+1$.

2. Hence $n \vdash^\alpha_{r+1} B \Rightarrow n \vdash^{2^\alpha}_r B$.

Proof by induction on γ.

Suppose $C \equiv \exists x D(x)$, and

$\delta \in \gamma[n]$: $\dfrac{n \vdash^\delta m \quad n \vdash^\delta C, D(m), B}{n \vdash^\gamma C, B}$ ∃

∀-Invert $n \vdash^\beta \neg C, B$ to get $m \vdash^\beta \neg D(m), B$.

Then by the ind. hypoth. at $\delta < \gamma$,

(N2) $\dfrac{n \vdash^\delta m \quad m \vdash^\beta \neg D(m), B}{n \vdash^{\beta+1} \neg D(m), B}$

D-Cut $\dfrac{n \vdash^{\beta+1} \neg D(m), B \quad n \vdash^{\beta+\delta} D(m), B}{n \vdash^{\beta+\gamma}_r B}$

Bounding Functions B_α

$\exists)\ \dfrac{n:N \vdash^{\beta}_{0} m:N \qquad n:N \vdash Spec(n,m)}{n:N \vdash^{\alpha}_{0} \exists y\, Spec(n,y)}$

Let $B_\beta(n) = \max\{m \mid n:N \vdash^{\beta}_{0} m:N\}$

If $\dfrac{n:N \vdash^{\gamma} k:N \qquad k:N \vdash^{\gamma} m:N}{n:N \vdash m:N}$

then $m \leq B_\gamma(k) \wedge k \leq B_\gamma(n)$

so $B_{\gamma+1}(n) = B_\gamma \circ B_\gamma(n)$.

To complete the definition add

$B_0(n) = n+1$, $B_\lambda(n) = B_{\lambda_n}(n)$.

Theorem

$\forall n\ \exists m < B_\alpha(n)\ Spec(n,m)$.

Fast-Growing Hierarchy

$$B_0(n) = n+1$$

$$B_{\alpha+1}(n) = B_\alpha \circ B_\alpha(n)$$

$$B_\lambda(n) = B_{\lambda_n}(n)$$

Can be written as

$$B_\alpha(n) = n \oplus 2^\alpha$$

$$n \oplus 2^0 = n+1$$

$$n \oplus 2^{\alpha+1} = n \oplus 2^\alpha \oplus 2^\alpha$$

$$n \oplus 2^\lambda = n \oplus 2^{\lambda_n}$$

Infinite Ramsey Theorem

$$\omega \to (\inf)^2_2$$

Proof

Given any $c : \omega^{[2]} \to \{0,1\}$.

Find infinite $\omega = S_0 \supseteq \ldots \supseteq S_i \ldots$
and take $x_0 \in S_0 \; \ldots \; x_i \in S_i \ldots$

<u>Stage $i+1$</u> $\quad x_i := \min S_i$

Then $S_i - \{x_i\} = T_0 \cup T_1$

$T_0 = \{z : c(x_i, z) = 0\}$ $T_1 = \{z : c(,) = 1\}$

$S_{i+1} := T_{0,1}$ whichever is infinite.

Hence $c(x_i, -)$ is constant on S_{i+1}

Look at $\{x_0, x_1, \ldots, x_i, \ldots\}$

If $i < j, k$ $\; c(x_i, x_j) = c(x_i, x_k)$.

Define $d : \{x_0, x_1, \ldots\} \to \{0,1\}$

$d(x_i) = c(x_i, x_j)$ $\quad$ any $j > i$

Then d splits $\{x_0, \ldots, x_i, \ldots\}$ into 2 subsets according as as $c(x_i, -) = 0$ or 1.

Choose whichever of these subsets is infinite, say

$$\{x_{i_0}, x_{i_1}, x_{i_2}, \ldots\}$$

Then if $p < q$ and $r < s$,

$$c(x_{i_p}, x_{i_q}) = d(x_{i_p}) = d(x_{i_r}) = c(x_{i_r}, x_{i_s})$$

Note

An infinite set of numbers

$$\{ x_0 < x_1 < x_2 < \dots x_i < \dots \}$$

has the property that

For each x_i there is a subset

of size $> x_i$ $\{x_i, x_{i+1}, \dots, x_{i+x_i}\}$

- Def^n A finite set $\{z_0, z_1, \dots, z_k\}$ is large if card $= k+1 > z_0$.
- If we ask for large homogeneous sets, things get VERY BIG.

Modified Finite Ramsey Thm

(Paris-Harrington 1977)

$$\forall n,k,r\ \exists m \left([n,m] \to (\text{large})^k_r \right)$$

is true but not provable in PA.

Idea of Proof (Ketonen-Solovay 1981)

$LR(n,k,r) :=$ least m. $[n,m] \to (\text{large})^k_r$

Then LR is computable, but grows faster than any B_α.

But if it were PA-provable we'd have $\forall n,k,r\ \exists m < B_\alpha \ (\dots)$.

<u>EG.</u> $LR(n,2,r) \geq \mathrm{ACK} \simeq B_{\omega \cdot r}(n)$

Use the following version of

$\mathrm{ACK}(n,r) = f_r(n)$ where

$$f_0(n) = n+1 \ , \ f_{i+1}(n) = f_i^n(n)$$

<u>Claim</u> $LR(n,2,r) \geq f_r(n)$

Let $m := f_r(n) - 1$

Choose a $c : [n,m]^{[2]} \to \{1,\dots,r\}$

$$c(x,y) = \text{least } i. \ f_i^j(n) \leq x < y < f_i^{j+1}(n)$$

for some (any) j

Take any homogeneous set
$X = \{x_1,\dots,x_\ell\}$ say with colour i.

Then for some fixed j,

$$f_i^j(n) \leq x_1 < \dots < x_\ell < f_i(f_i^j(n))$$

<u>Case $i=1$</u> Note $f_1 = 2x$ so

$$f_1^j(n) \leq x_1 < \dots < x_\ell < f_1^j(n) + f_1^j(n)$$

$\therefore \ \ell < f_1^j(n) \leq x_1$

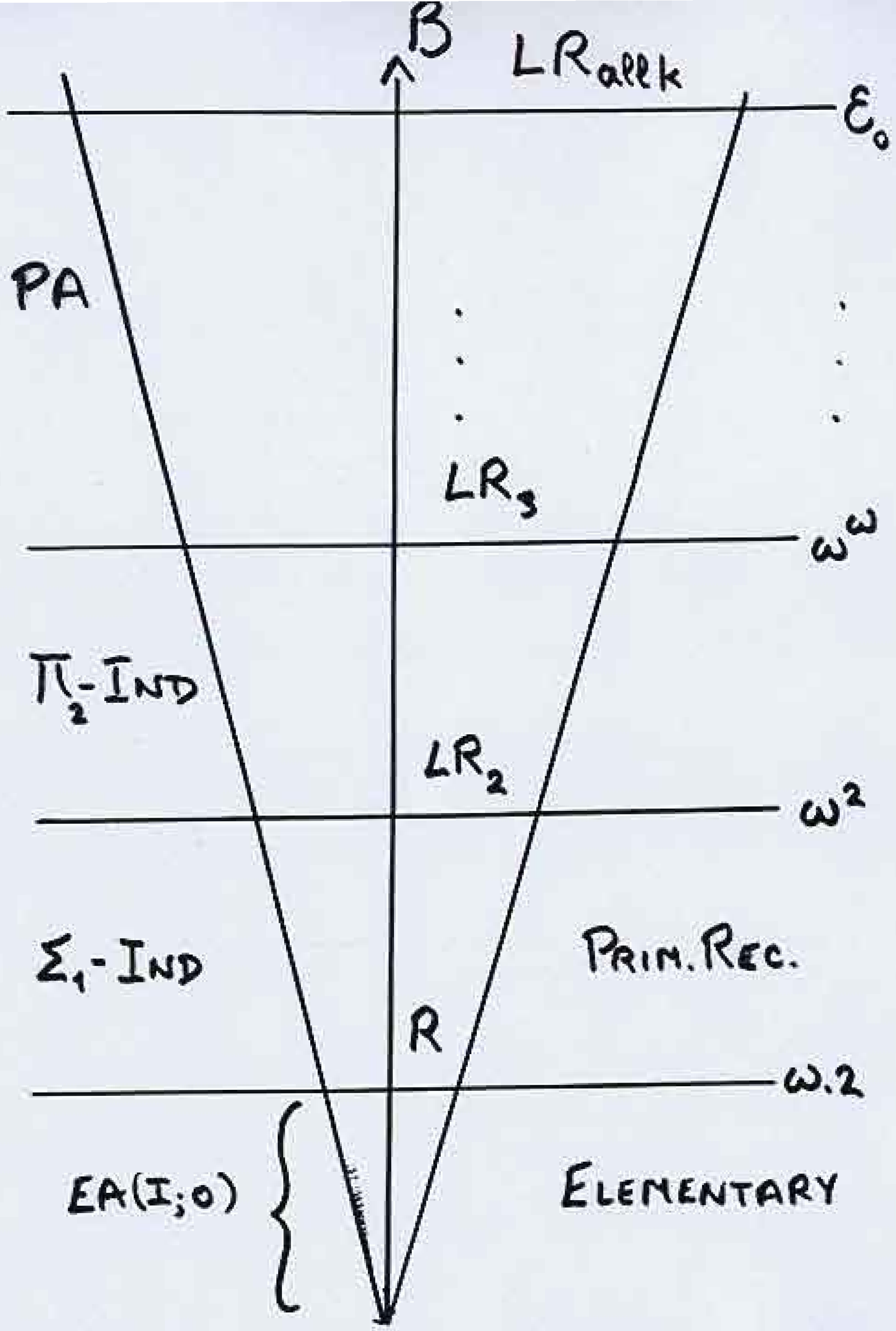
$\therefore$ X is not large.

<u>Case $i>1$</u> Let $s = f_i^j(n) = f_{i-1}^k(n)$

$$s \leq x_1 < \dots < x_\ell < f_i(s) = f_{i-1}^s(s)$$

$$f_{i-1}^k(n) \leq x_1 < \dots < x_\ell < f_{i-1}^{k+s}(n)$$

<u>Cannot have</u> $f_{i-1}^j(n) \leq x < x' < f_{i-1}^{j+1}(n)$.


B
LR_{allk}
ε_0
PA
LR_3
ω^ω
Π_2-IND
LR_2
ω^2
Σ_1-IND
PRIM. REC.
R
$\omega.2$
EA(I;O)
ELEMENTARY