LECTURE NOTES ON ENORMOUS INTEGERS

by
Harvey M. Friedman
Department of Mathematics
Ohio State University
friedman@math.ohio-state.edu
http://www.math.ohio-state.edu/~friedman/
November 22, 2001

Abstract. We discuss enormous integers and rates of growth after [PH77]. This breakthrough was based on a variant of the classical finite Ramsey theorem. Since then, examples have been given of greater relevance to a number of standard mathematical and computer science contexts, often involving even more enormous integers and rates of growth.

1. $F(x_1,\ldots,x_k) = F(x_2,\ldots,x_{k+1})$

N = the nonnegative integers.

THEOREM 1.Let $F:N^k \rightarrow \{1,\ldots,r\}$. There exists $x_1 < \ldots < x_{k+1}$ such that $F(x_1,\ldots,x_k) = F(x_2,\ldots,x_{k+1})$.

This is an immediate consequence of a more general combinatorial theorem called Ramsey's theorem, but it is much simpler to state. We call this adjacent Ramsey theory.

There are inherent finite estimates here.

THEOREM 1.2. For all k,r there exists t such that the following holds. Let $F:N^k \rightarrow \{1,\ldots,r\}$. There exists $x_1 < \ldots < x_{k+1} \leq t$ such that $F(x_1,\ldots,x_k) = F(x_2,\ldots,x_{k+1})$.

QUESTION: What is the least such t = Adj(k,r)?

THEOREM 1.3. Adj(k,1) = k. Adj(k,2) = 2k.

THEOREM 1.4. Let $k \geq 5$. Adj(k,3) is greater than an exponential stack of k-2 1.5's topped off with k-1. E.g., $\text{Adj}(6,3) > 10^{173}$, $\text{Adj}(7,3) > 10\text{^}10^{172}$.

THEOREM 1.5. Adj(k,r) is at most an exponential stack of k-1 2's topped off with a reasonable function of k and r.

Our adjacent Ramsey theory from the 80's is lurking in the background in [DLR95].

2. THE ACKERMANN HIERARCHY

There is a good notation for really big numbers - up to a point. We use a streamlined version of the Ackerman hierarchy.

Let $f:Z^+ \rightarrow Z^+$ be strictly increasing. We define the critical function $f':Z^+ \rightarrow Z^+$ of f by: $f'(n)$ = the result of applying f n times at 1.

Define $f_1:Z^+ \rightarrow Z^+$ to be the doubling function, and $f_{n+1}:Z^+ \rightarrow Z^+$ be f_n'.

Thus f_1 is doubling, f_2 is exponentiation, f_3 is iterated exponentiation; i.e., $f_3(n) = E^*(n)$ = an exponential stack of n 2's. f_4 is confusing.

We can equivalently present this by the recursion equations $f_1(n) = 2n$, $f_{k+1}(1) = f_k(1)$, $f_{k+1}(n+1) = f_k(f_{k+1}(n))$, where $k,n = 1$. We define $A(k,n) = f_k(n)$.

Note that $A(k,1) = 2$, $A(k,2) = 4$. For $k \geq 3$, $A(k,3) > A(k-2,k-2)$, and as a function of k, eventually strictly dominates each f_n, $n \geq 1$.

$A(3,4) = 65,536$. $A(4,3) = 65,536$. $A(4,4) = E^*(65,536)$. And $A(4,5)$ is $E^*(E^*(65,536))$.

It seems safe to assert, e.g., that A(5,5) is incomprehensibly large. We propose this number as a sort of benchmark.

3. VECTOR REDUCTION

Let $k \geq 1$ and $x \in N^k$. We perform the "reduction" on $x = (x_1,...,x_k)$ as follows. Find the greatest $i < k$ such that $x_i > 0$, and replace x_i,x_{i+1} by $x_i-1,x_1+...+x_k$.

THEOREM 3.1. For all $k \geq 1$ and $x \in N^k$, this reduction can be performed only finitely many times.

The number of times this reduction can be performed at $x \in N^k$ is very large. E.g.,

THEOREM 3.2. The number of times this reduction can be performed at (2,0,0,0,0) is greater than $E^*(2^{1,000,000})$.

THEOREM 3.3. For all $k \geq 3$ and $n \geq 2$, the number of times this reduction can be applied to $(n,0,...,0) \in N^k$ is greater than $A(k-1,n)$ and less than $A(k,n+c)$, where c is a universal constant.

4. BOLZANO WEIERSTRASS

We start with the usual statement of BW.

THEOREM 4.1. Let $x[1],x[2],...$ be an infinite sequence from the closed unit interval $[0,1]$. There exists $k_1 < k_2 < ...$ such that the subsequence $x[k_1],x[k_2],...$ converges.

We can obviously move towards estimates like this:

THEOREM 4.2. Let $x[1],x[2],...$ be an infinite sequence from the closed unit interval $[0,1]$. There exists $k_1 < k_2 < ...$ such that $|x[k_{i+1}]-x[k_i]| < 1/i^2$, $i \geq 1$.

But now we shake things up:

THEOREM 4.3. Let $x[1],x[2],...$ be an infinite sequence from the closed unit interval $[0,1]$. There exists $k_1 < k_2 < ...$ such that $|x[k_{i+1}]-x[k_i]| < 1/k_{i-1}^2$, $i \geq 2$.

Still true since we can first find a convergent subsequence, and then make a recursive construction. But note added combinatorial sophistication.

THEOREM 4.4. For each $n \geq 1$ there exists a positive integer $B(n)$ such that the following holds. Let $x[1],x[2],...$ be an infinite sequence from the closed unit interval $[0,1]$. There exists $k_1 < ... < k_n \leq B(n)$ such that $|x[k_{i+1}]-x[k_i]| < 1/k_{i-1}^2$, $2 \leq i \leq n-1$.

This is proved by compactness of the Hilbert cube.

Now set $B(n)$ to be the least integer such that for all $x[1],x[2],... \in [0,1]$, there exists $k_1 < ... < k_n \leq B(n)$ such that $|x[k_{i+1}]-x[k_i]| < 1/k_{i-1}^2$, $2 \leq i \leq n-1$.

THEOREM 4.5. $B(11) > E^*(64)$. I.e., $B(11)$ is greater than an exponential stack of 64 2's. $B(n) > A(n-8,64)$ for $n \geq 10$. Specifically, $B(13) > A(5,64)$. Also, $B(n) > A(n+c,n+c)$.

5. WALKS IN LATTICE POINTS

Let $k \geq 1$. A walk in N^k is a finite or infinite sequence $x_1,x_2,... \in N^k$ such that the Euclidean distance between successive terms is exactly 1.

A self avoiding walk in N^k is a walk in N^k in which no term repeats.

Each successive term must be obtained from the preceding term by leaving all but one coordinate fixed, and moving that one coordinate up or down by 1.

Let $x,y \in N^k$. We say that x points inward to y iff for all $1 \leq i \leq k$, $x_i \geq y_i$.

Here is a well known result more general than walks.

THEOREM 5.1. For all $k \geq 1$, every infinite sequence from N^k has an infinite subsequence in which each term points inward to all earlier terms.

THEOREM 5.2. Let $x \in N^k$. In every sufficiently long finite self avoiding walk in N^k starting at x, some term points inward to an earlier term with at most half the (lattice or Euclidean) norm.

Now let W(x) be the greatest length of a self avoiding walk in N^k starting at x such that no term points inward to an earlier term with at most half the (lattice or Euclidean) norm.

THEOREM 5.3. $W(2,2,2) \geq 2^{192,938,011}$. For $n \geq 2$, $W(n,n,n) \geq E^*(n-1,192,938,011)$. $W(1,1,1,1) \geq E^*(192,938,011)$. $W(2,2,2,2) \geq E^*E^*(192,938,011)$. There exist constants $c,d > 0$ such that for all $k,n \geq 1$, $A(k,n+c) \leq W(n,...,n) \leq A(k,n+d)$, where there are k n's. Also, $W(1,1,1,1,1,1) >> A(5,5)$.

6. SPECIFIC FINITE TREES

A finite ordered tree is a finite (rooted) tree with an assignment to each vertex of a linear ordering of its immediate successors (children). The assigned linear orderings give a left/right sense to the children of any vertex, and so to the entire vertex set.

We define x □* y iff either x is to the left of y or x □ y.

It can be shown that □* is a linear ordering on all vertices, and agrees with depth first search.

We let d(v) be the position of v in □* counting from 1. Thus d(root) = 1.

The height of a vertex v is the number of edges in the unique path from the root to v. So the root has height 0. The height of T is the largest height among its vertices.

For k ≥ 0, define T[k] to be the ordered tree of height k in which every vertex v of height □ k-1 has exactly d(v) children.

THEOREM 6.1 For all k ≥ 0 there is exactly one such ordered tree T[k] up to isomorphism.

THEOREM 6.2. |T[0]| = 1, |T[1]| = 2, |T[2]| = 4, |T[3]| = 14, |T[4]| = $82(2^{38})-2$, T[5] has more than an exponential stack of 2^{38} 2's vertices. |T[k]| grows like the Ackermann function.

7. ALGEBRAIC APPROXIMATIONS

Let k ≥ 1 and F be a field. An algebraic subset of F^k is a subset of F^k which is the set of simultaneous zeros of a finite set of polynomials in the polynomial ring $F[x_1,...,x_k]$.

The (presentation) degree of an algebraic set A □ F^k is the least d such that A is the set of simultaneous zeros of a finite set of polynomials in $F[x_1,...,x_k]$ whose degrees are each at most d.

THEOREM 7.1. Let F be a field and k ≥ 1. Every strictly decreasing sequence of algebraic subsets of F^k is finite.

Proof: Use the Hilbert basis theorem. QED

Let A □ F^k and d ≥ 0. The d-th approximation to A, written A[d], is the least algebraic set of degree □ d containing A. By linear algebra, A[d] must exist.

THEOREM 7.2. For every k ≥ 1 and A □ F^k, there exists d ≥ 0 such that A[d] = A[d+1].

THEOREM 7.3. For each $k \geq 1$ there exists $r \geq 0$ such that the following holds. For all fields F and $A \subseteq F^k$, there exists $0 \leq d \leq r$ such that $A[d] = A[d+1]$.

Let r(k) be the least r in Theorem 7.3.

THEOREM 7.4. For all $k \geq 7$, $A_{k-6}(k-6) \leq r(k) \leq A_{2k}(2k)$.

8. BLOCKS IN SEQUENCES FROM {1,...,k}

The block subsequence theorems will push us well beyond the Ackerman rate of growth. This work appears in [Fr01].

THEOREM 8.1. Block Subsequence Theorem. Let $k \geq 1$. There is a longest finite sequence $x_1,...,x_n$ from {1,...,k} such that for no $i < j \leq n/2$ is $x_i,...,x_{2i}$ a subsequence of $x_j,...,x_{2j}$.

For $k \geq 1$, let n(k) be the length of this longest finite sequence.

Paul Sally runs a program for gifted high school students at the University of Chicago.

He asked them to find n(1), n(2), n(3).

They all got n(1) = 3. One got n(2) = 11. Nobody reported much on n(3).

I asked several mathematicians to give an estimate on n(3), some of them very famous. I got guesses like this:

60, 100, 150, 200, 300, 2000, 20,000.

It turns out that 20,000 was the best guess, as we now see.

THEOREM 8.2. n(3) > A(7,184).

Recall the discussion about A(5,5) being incomprehensibly large. With the help of computer investigations (with R. Dougherty), I got:

THEOREM 8.3. n(3) > A(7198,158386).

See Long Finite Sequences, JCTA, 95, 102-144 (2001).

A good upper bound for n(3) is work in progress. Crude result: A(n,n) where n = A(5,5).

Note that this crude upper bound is a short composite of the Ackermann function with small constants.

The number n(4) is a whole 'nother kettle of fish. Define A(k) = A(k,k).

THEOREM 8.4. n(4) > AA...A(1), where there are A(187196) A's.

Here is a summary of the key metamathematical properties of the Block Subsequence Theorem.

THEOREM 8.5. The function n(k) eventually dominates every multirecursive function, but is eventually dominated by their natural diagonalization up to a constant factor in the argument. It eventually dominates every provably recursive function of 2 quantifier arithmetic, but is a provably recursive function of 3 quantifier arithmetic. The statement "for all k, n(k) exists" is provable in 3 quantifier arithmetic but not in 2 quantifier arithmetic.

9. LOW VALUES

We now move to yet higher rates of growth which can only be measured by means of the ordinal ε_0 and the formal system PA = Peano Arithmetic.

For $A \subseteq N$, let $A = \{A_1 < A_2 < ...\}$. We start with an infinitary theorem.

THEOREM 9.1. Let $k,p \geq 1$ and $F:N^k \to N$. There exists infinite $A \subseteq [p,\infty)$ such that $F[A^k] \cap [0,A_1] \subseteq F[\{A_1,...,A_k\}^k]$.

We now give a finite form.

THEOREM 9.2. Let $n \gg k,p,r \geq 1$ and $F:[0,n]^k \to N$. There exists $A \subseteq [p,n]$ with r elements such that $F[A^k] \cap [0,A_1] \subseteq F[\{A_1,...,A_k\}^k]$.

We now give a weaker finite form.

THEOREM 9.3. Let $n \gg k,r \geq 1$ and $F:[0,n]^k \to N$. There exists $A \subseteq [1,n]$ with 2k elements such that $F[A^k] \cap [0,A_1] \subseteq F[\{A_1,...,A_k\}^k]$.

Theorem 9.3 cannot be proved in Peano Arithmetic (PA), and the growth rate of n as a function of k,r grows faster than all provable recursive functions of PA.

10. REGRESSIVE FUNCTIONS

Let $F:N^k \to N^r$. We say that F is regressive iff for all $x \in N^k$, every coordinate of F(x) is $\leq$ every coordinate of x.

This work appears in [Fr98]. See Theorems 0.4 and 1.6.

THEOREM 10.1. Let k,r,p ≥ 1 and $F:N^k \to N^r$ be regressive. There is a p element set $S \subseteq N$ such that $|F[S^k]| \leq k^k(p)$.

Using a finitely branching tree argument or "compactness" argument, we obtain the following uniformity:

THEOREM 10.2. For all k,r,p there exists t such that the following holds. Let $F:N^k \to N^r$ be regressive. There is a p element set $S \subseteq [0,t]$ such that $|F[S^k]| \leq k^k(p)$.

What does the least t look like a function of k,r,p?

THEOREM 10.3. In Theorem 10.2, the least t, as a function of k,p,r, appears at level ε_0 in the standard transfinite hierarchy of functions. At k,k,k, it eventually dominates every $< \varepsilon_0$ recursive function. If we replace N by [0,t] then we obtain a finite sentence that is not provable in Peano Arithmetic but provable just beyond it.

11. SOLVABILITY OF INEQUALITIES IN NUMERICAL FUNCTIONS

We stay at the rate of growth measured by means of the ordinal ε_0 and the formal system PA = Peano Arithmetic.

For $x,y \in N^r$, we write $x \leq y$ for $(\forall i)(1 \leq i \leq k)(x_i \leq y_i)$.

THEOREM 11.1. For all k,r ≥ 1 and $F:N^k \to N^r$, there exists $x_1 < \ldots < x_{k+1}$ such that $F(x_1,\ldots,x_k) \leq F(x_2,\ldots,x_{k+1})$.

The obvious uniformity that we seek is false. We need the concept of limited function.

We say that $F:N^k \to N^r$ is limited iff for all $x \in N^k$, $\max(F(x)) \leq \max(x)$.

THEOREM 11.2. For all $k,r \geq 1$ there exists t such that the following holds. Let $F:N^k \to N^r$ be limited. There exists $x_1 < \ldots < x_{k+1} \leq t$ such that $F(x_1,\ldots,x_k) \leq F(x_2,\ldots,x_{k+1})$.

THEOREM 11.3. In Theorem 11.2, the least t, as a function of k,r, appears at level ε_0 in the standard transfinite hierarchy of functions. At k,k, it eventually dominates every $<\varepsilon_0$ recursive function. If we replace N by [0,t] then we obtain a finite statement that is not provable in PA but provable just beyond it.

Theorem 11.2 degenerates into a triviality if r = 1.

But we can sharpen the theorem to obtain the conclusion

$$F(x_1,\ldots,x_k) \leq F(x_2,\ldots,x_{k+1}) \leq \ldots \leq F(x_m,\ldots,x_{k+m-1}).$$

Everything above holds for this sharpening.

But now we can set r = 1 and m = 3 and obtain independence from PA even for the one dimensional inequality

$$F(x_1,\ldots,x_k) \leq F(x_2,\ldots,x_{k+1}) \leq F(x_3,\ldots,x_{k+2}).$$

In this connection, there is a general theory of sets of inequalities. We don’t have time to go into this here.

12. EMBEDDINGS OF FINITE TREES

Here we make a huge jump in the rates of growth involved. This work appears in [Fr02].

We consider finite trees, defined as posets in the usual way.

The n-labeled finite trees are finite trees with a labeling of vertices from {1,...,n}.

The valence of a vertex is the number of its immediate successors. The valence of T is the largest of the valences of its vertices.

The height of a vertex in a finite tree is the number of its strict predecessors.

Note that for finite trees $T = (V(T),\leq)$, and vertices $x,y \in V(T)$, x inf y exists.

Let T_1 and T_2 be finite trees. An inf preserving embedding from T_1 into T_2 is a one-one map $h:V(T_1) \to V(T_2)$ such that for all $x,y \in V(T_1)$, h(x inf y) = h(x) inf h(y).

Recall the classic theorem of J.B. Kruskal (in the context of n-labeled trees):

THEOREM 12.1. Let $n \geq 1$ and $T_1,T_2,\ldots$ be an infinite sequence of finite n-labeled trees. There exists $i < j$ such that T_i is inf preserving embeddable into T_j.

Best proof: Nash-Williams, "On well-quasi ordering finite trees," Proc. Cambridge Phil. Soc., 59 (1963), 833-835.

A finite tree is said to be perfect if and only if
i) all nonterminal vertices have the same valence;
ii) all terminal vertices have the same height.

An embedding is said to be terminal preserving iff it maps terminal vertices into terminal vertices.

Every perfect tree of height t has t+1 truncations of respective heights 0,1,...,t.

THEOREM 12.2. Let $k,n \geq 1$ and T be a sufficiently tall finite perfect n-labeled tree of valence $\leq k$. There exists an inf, label, and terminal preserving embedding from some truncation of T into a truncation of T of greater height.

For $k,n \geq 1$, let TR(k,n) be the least height for Theorem 12.2. TR grows so fast that to describe its growth we need formal systems and proof theoretic ordinals.

There is a fairly well accepted formal system for predicative mathematics, where one is forbidden to define sets of integers by predicates that refer to all sets of integers.

This corresponds to positions advocated by Poincare and Weyl. The accepted formalism corresponds to the proof theoretic ordinal Γ_0.

THEOREM 12.3. TR eventually dominates every provably recursive function of predicative mathematics. TR does not occur in the usual transfinite hierarchies of functions up through ϵ_0. It occurs at level $\theta(\Omega^\omega,0)$, and not sooner.

What about, say, TR(2,4)? We have investigated such questions for the original finite forms of Kruskal's theorem before we discovered Theorem 12.2. We expect corresponding results for TR(2,4).

Specifically, we expect that any proof within predicative mathematics of the existence of TR(2,4) will have incomprehensibly many symbols; e.g., more than A(5,5) symbols.

REFERENCES

[DLR95] D. Duffus, H. Lefman, V. Rodl, Shift graphs and lower bounds on Ramsey numbers $r_k(l;r)$, Discrete Mathematics 137 (1995), 177-187.

[Fr98] H. Friedman, Finite functions and the necessary use of large cardinals, Annals of Mathematics, 148 (1998), 803-893.

[Fr01] H. Friedman, Long Finite Sequences, Journal of Combinatorial Theory, Series A 95, 102-144 (2001).

[Fr02] H. Friedman, Internal finite tree embeddings, Feferest volume, ASL, 2002.

[PH77] J. Paris, L. Harrington, An Incompleteness in Peano Arithmetic, in: Handbook for Mathematical Logic, ed. Jon Barwise, 1977.