ENORMOUS INTEGERS IN REAL LIFE

by

Harvey M. Friedman
friedman@math.ohio-state.edu
www.math.ohio-state.edu/~friedman/

June 1, 2000

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

N = the nonnegative integers.

THEOREM 1.Let $F:N^k \to \{1,\ldots,r\}$. 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 conse-quence 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 $F:N^k \to \{1,\ldots,r\}$. 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) = 1. Adj(k,2) = 2k+1.

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., Adj(6,3) > 10^{173}, Adj(7,3) > $10\hat{}10^{172}$.

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

Laziness prevented me from being more precise than this. The related literature - upper bounds for higher Ramsey numbers - is virtually all asymptotic, so I can't just quote it.

Our adjacent Ramsey theory from the 80's is lurking in the background in

"Shift graphs and lower bounds on Ramsey numbers $r_k(l;r)$," Duffus, Lefmann, Rodl, Discrete Mathematics 137 (1995), 177-187.

2. THE ACKERMAN HIERARCHY

There is a good notation for really big numbers - up to a point. We use a streamlined version of the Ackerman hierarchy. Let $f:Z^+ \to Z^+$ be strictly increasing. We define the critical function $f':Z^+ \to Z^+$ of f by: $f'(n)$ = the result of applying f n times at 1.

For $n \geq 1$, the n-th function of the Ackerman hierarchy is the result of applying the ′ operator n-1 times starting at the doubling function.

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 $k,n \geq 1$. 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, $n \geq 1$.

$A(3,5) = 2^{65,536}$. $A(4,3) = 65,536$. $A(4,4) = E^*(65,536)$. 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. BOLZANO WEIERSTRASS

We start with the usual statement of BW.

THEOREM 3.1. Let x[1],x[2],... be an infinite sequence from the closed unit interval [0,1]. There exists $k_1 < k_2 < \ldots$ such that the subsequence $x[k_1],x[k_2],\ldots$ converges.

We can obviously move towards estimations like this:

THEOREM 3.2. Let x[1],x[2],... be an infinite sequence from the closed unit interval [0,1]. There exists $k_1 < k_2 < \ldots$ such that $|x[k_{i+1}]-x[k_i]| < 1/i^2$, $i \geq 1$.

But now we shake things up:

THEOREM 3.3. Let x[1],x[2],... be an infinite sequence from the closed unit interval [0,1]. There exists $k_1 < k_2 < \ldots$ 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 3.4. Let x[1],x[2],... be an infinite sequence from the closed unit interval [0,1], and $n \geq 1$. There exists $k_1 < \ldots < k_n <$?(n) such that $|x[k_{i+1}]-x[k_i]| < 1/k_{i-1}^2$, $2 \leq i \leq n$.

This is proved by compactness of the Hilbert cube.

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

THEOREM 3.5. ?(11) > E*(64). I.e., ?(11) is greater than an exponential stack of 64 2's. ?(n) > A(n-8,64) for $n \geq 10$. Specifically, ?(13) > A(5,64). Also, ?(n) > A(n+c,n+c).

4. WALKS IN LATTICE POINTS

Let $k \geq 1$. A walk in N^k is a finite or infinite sequence $x_1,x_2,\ldots \in N^k$ 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 outward to y iff for all $1 \leq i \leq k$, $x_i \leq y_i$.

Here is a well known result more general than walks.

THEOREM 4.1. For all $k \geq 1$, every infinite sequence from N^k has an infinite subsequence in which each term points outward to the next term.
THEOREM 4.2. Let $x \in N^k$. In every sufficiently long finite self avoiding walk in N^k start-ing at x, some term points

outward to a later term which is at least twice the (lattice or Euclidean) distance from the origin.

Note that the obvious infinite form of 4.2 is an immediate consequence of 4.1. Then apply compactness or a finitely branching tree argument.

Now let W(x) be the least n such that:

in every self avoiding walk in N^k of length n starting at x, some term points outward to a later term which is at least twice the (lattice or Euclid-ean) distance from the origin

THEOREM 4.3. $W(2,2,2) \geq 2^{192,938,011}$. For $n \geq 2$, $W(n,n,n) \geq E^*(n-1,192,938,011)$. $W(1,1,1,1) \geq E^*(102,938,011)$. $W(2,2,2,2) \geq E^*E^*(102,938,011)$. 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, $W(1,1,1,1,1,1) >> A(5,5)$.

5. SPECIFIC FINITE TREES

We define some specific finite ordered trees T. An ordered tree is a triple $(V,\leq,<')$ where $(V,\leq)$ is a finite poset with a least element (root), in which the set of predeces-sors under $\leq$ of each vertex is linearly ordered by $\leq$, and where for each vertex, $<'$ is a strict linear ordering on its immediate successors (child-ren). We think of $<'$ as giving a left to right sense to the set of children of any vertex.

This defines a notion of left to right among all vertices in the tree. I.e., x is to the left of y iff x,y are incomparable (under $\leq$), and if you take the paths from x,y down to the root, then just before these paths meet, the first path's vertex is to the left of the second path's vertex.

We now define $x \leq^* y$ iff either x is to the left of y or $x \leq y$.

It can be shown that $\leq^*$ is a linear ordering on all vertices, and agrees with depth first search. We let d(v) be the position of v in $\leq^*$ count-ing from 1. Thus d(root) = 1.

The height of a vertex v is the number of edges in the longest path from the root to v. Thus the height of the root is 0. The height of T is the largest of all of the heights of its vertices.

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

THEOREM 5.1 For all k ≥ 0 there is exactly one such ordered tree T[k] up to isomorphism.

THEOREM 5.2. |T[0]| = 1, |T[1]| = 2, |T[2]| = 4, |T[3]| = 14, |T[4]| > 2^{43}, |T[5]| ≥ E*(2^2^95). |T[k]| grows like the Ackerman function.

6. ALGEBRAIC SUPERSETS

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 6.1. Let F be a field and k ≥ 1. Every strictly decreasing sequence of alge-braic subsets of F^k is finite.

Proof: Use the Hilbert basis theorem. QED

Let A □ F^k. For d ≥ 0 we say that A is d-inexact iff every algebraic superset of A of degree d contains an algebraic superset of A of degree < d.

THEOREM 6.2. Every subset of F^k is d-inexact for some d ≥ 0.

THEOREM 6.3. For each k ≥ 1 there exists r ≥ 0 such that the following holds. For all fields F, every subset of F^k is p-inexact for some 0 □ p □ r.

What can we say about the least possible value of r = r(k) as a function of k? Here is a crude estimate.

THEOREM 6.4. For all k ≥ 7,
$A_{k-6}(k-6)$ □ r(k) □ $A_{2k}(2k)$.

7. DIVISIBILITY IN FINITE SETS OF POSITIVE INTEGERS

Let k ≥ 0. We say that A is special above k iff A is a set of positive integers where every element x > k of A divides the product of all elements y < x of A and does not divide any element y > x. An empty product is taken to be 1.

E.g., {1,2,3,4} is special above 4 but not special above 3. {1,2,4,8} is special above 4 but not special above 3. {1,2,3,6,12} is special above 6 but not special above 5.

THEOREM 7.1. For all k ≥ 1, there are finitely many A which are special above k. All of them are finite.

We write #(k) for the largest cardinality of any set that is special above k.

#(0) = 1, #(1) = 1, #(2) = 2, #(3) = 5, #(4) = 8, #(5) = 37, #(6) = 26,948, #(7) > 2^2^2^60, #(11) > E*(1000) = A_3(1000), #(13) > A_4(5000).

THOEREM 7.2. Let k ≥ 7. Then A(t-1,t-1) ≤ #(k) ≤ A(k,k), where t is the number of primes ≤ k.

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

These block subsequence theorems will push us well beyond the Ackerman rate of growth.

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

For k ≥ 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 then started to ask several mathematicians to give an estimate on n(3), some of them very famous. I got guesses like this:

60, 100, 150, 200, 300.

They were not in combinator-ics. Recently I asked Lovasz, telling him about these five guesses. He guessed 20,000.

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

Lovasz wins, as his guess is closer to $A(7,184)$ than the other guesses.

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

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

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 Ackerman 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.

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 domin-ates every provably recursive function of 2 quantifier arithmetic, but is a provably recursive function of 3 quan-tifier arithmetic. The statement "for all k, n(k) exists" is provable in 3 quantifier arithmetic but not in 2 quan-tifier arithmetic.

9. REGRESSIVE FUNCTIONS

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.

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

THEOREM 9.1. Let $k,r,p \geq 1$ and $F:N^k \rightarrow N^r$ 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 9.2. 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 9.3. In Theorem 9.2, 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.

10. SOLVABILITY OF INEQUALI-TIES 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 10.1. For all $k,r \geq 1$ 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 10.2. 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 10.3. In Theorem 10.2, 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 10.2 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. We can even set r = 1 and m = 3 and obtain the same results. We get independence from PA even for the one dimensional inequality

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

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

11. EMBEDDINGS OF FINITE TREES

Here we make a huge jump in the rates of growth involved.

We will consider finite trees, which are finite partial orderings with a minimum ele-ment (root), where the predecessors of every vertex are linearly ordered. The valence of a vertex is the number of its immediate successors (children). The valence of T is the largest of the valences of its vertices. The set of vertices of T is denoted by V(T).

Note that for finite trees T = (V(T),□), and vertices x,y □ 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 $h:V(T_1) \square V(T_2)$ such that for all x,y □ $V(T_1)$, h(x inf y) = h(x) inf h(y).

Recall the classic theorem of J.B. Kruskal:

THEOREM 11.1. Let $T_1,T_2,...$ be an infinite sequence of finite 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.

Let T[□i] be the subtree con-sisting of all vertices with at most i strict predecessors. Let T[i] be the set of vertices with exactly i strict predecessors.

THEOREM 11.2. Let k ≥ 1 and T be a finite tree of valence □ k whose height hgt(T) is suf-ficiently large. There exists 1 □ i < j □ hgt(T) and an inf preserving embedding from T[□i] into T[□j] mapping T[i] into T[j].

For $k \geq 1$, let TR(k) be the least number of vertices that T must have in Theorem 11.2. TR grows so fast that the best way to describe it's growth is in terms of formal systems and proof theoretic ordinals.

There is a fairly well accep-ted 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 11.3. TR eventually dominates every provably recursive function of predicative mathematics. TR does not occur in the usual transfinite hierarchies of functions up through Γ_0. It occurs at level $\theta(\Omega^\omega,0)$.

What about, say, TR(9)? We have investigated such ques-tions for the original finite forms of Kruskal's theorem before we discovered Theorem 11.2. We expect corresponding results for TR(9).

Specifically, we expect that any proof within predicative mathematics of the existence of TR(9) will have incomprehensibly many symbols; e.g., more than A(5,5) symbols.

12. PLANE GEOMETRY

This is at the same rates of growth as in section 11.

A circle is taken to be the circumference of a nondegener-ate circle in the Euclidean plane.

THEOREM 12.1. For all $k \geq 1$ there exists $n \geq 1$ such that the following holds. Let $C_1,C_2,...,C_n$ be pairwise disjoint circles. There exists $k \leq i < j \leq n/2$ and a homeomorphism of the plane mapping $C_i \cup ... \cup C_{2i}$ into $C_j \cup ... \cup C_{2j}$.

THEOREM 12.2. Theorem 12.1 is at the Γ_0 and Peano Arithmetic level.

A p-circle is the union of p circles. (Some of the p circles may intersect or even be identical).

THEOREM 12.3. For all $k \geq 1$ there exists $n \geq 1$ such that the following holds. Let $C_1, C_2, \ldots, C_n$ be pairwise disjoint k-circles. There exists $1 \leq i < j \leq n/2$ and a homeomorphism of the plane mapping $C_i \cup \ldots \cup C_{2i}$ into $C_j \cup \ldots \cup C_{2j}$.

THEOREM 12.4. Theorem 12.3 is at the high level of the previous section that goes be-yond predicative mathematics.

13. TRANSCENDENTAL INTEGERS.

I call an integer n transcendental if and only if the following holds. Let M be a Turing machine. Assume that M can be proved to halt at input 0 within ZFC using at most 2^{1000} symbols. Then M halts in $\leq n$ steps.

Transcendental integers should fall out very naturally and explicitly in Boolean relation theory. Stay tuned.