Finite canonization

Saharon Shelah

Abstract. The canonization theorem says that for given \( m, n \) for some \( m^* \) (the first one is called \( ER(n; m) \)) we have

for every function \( f \) with domain \([1, \ldots, m^*]^n\), for some \( A \in [1, \ldots, m^*]^m \), the question of when the equality \( f(i_1, \ldots, i_n) = f(j_1, \ldots, j_n) \) (where \( i_1 < \cdots < i_n \) and \( j_1 < \cdots j_n \) are from \( A \)) holds has the simplest answer: for some \( v \subseteq \{1, \ldots, n\} \) the equality holds iff \( \bigwedge_{\ell \in v} i_\ell = j_\ell \).

We improve the bound on \( ER(n, m) \) so that fixing \( n \) the number of exponentiation needed to calculate \( ER(n, m) \) is best possible.

Keywords: Ramsey theory, Erdős-Rado theorem, canonization

Classification: 05, 05C55

§0. Introduction

On Ramsey theory see the book Graham Rothschild Spencer [GrRoSp]. This paper is self-contained.

The canonical Ramsey theorem was originally proved by Erdős and Rado, so the relevant number is called \( ER(n, m) \). See [ErRa], [Ra86] and more in the work of Galvin. The theorem states that if \( m \) and \( n \) are given, and \( f \) is an \( n \)-place function on a set \( A \) of size \( \geq ER(n, m) \), then there is an \( A' \in [A]^m \) such that \( f \) is canonical on \( A' \). That is, for some \( v \subseteq \{1, \ldots, n\} \) and for every \( i_1 < \cdots < i_n \in A' \) and \( j_1 < \cdots < j_n \in A \)

\[
f(i_1, \ldots, i_n) = f(j_1, \ldots, j_n) \iff \bigwedge_{\ell \in v} i_\ell = j_\ell.
\]

Galvin got in the early seventies by the probability method a lower bound which appeared in [ErSp, p. 30], \( ER(2; m) \geq (m + o(1))^m \).

Lefmann and Rödl [LeRo93] proved

\[
2^{cm^2} < ER(2; m) \leq 2^{2^{cm^3}}.
\]

I thank Alice Leonhardt for the beautiful typing.
Written 4/June/94 - Publ.No. 564.
Latest Revision - 4/Aug/95
Lefmann and Rödl [LeRo94] proved:

(i) \(2c^2 m^2 \leq ER(2; m) \leq 2c^2 (m^2 \log m)\)

(ii) \(\exists_n(c_k m^2) \leq ER(n + 1; m) \leq \exists_{n+1} \left( c_k^* m^{2k-1} \log m \right)\).

See more on this in [LeRo94] and below for the definition of \(\exists_n\).

We thank Nešetřil for telling us the problem; which for us was finding the right number of exponents (i.e. the subscript for \(\exists\) in (ii) above) in \(ER(n; m)\) (for a fixed \(n\)). We prove here that this number is \(n\).

Why is the number of exponentiations best possible? Let \(r^n_t(m)\) be the first \(r\) such that:

\[ r \to (m)^n_t, \text{ now trivially } ER(n; m) \geq r^n_t(m) \text{ when } m \text{ is not too small, and } r^n_t(m) \text{ needs } n - 1 \text{ exponentiations when } t \text{ is not too small.} \]

§1. The finitary canonization lemma

**Notation.** \(\mathbb{R}, \mathbb{N}\) are the set of reals and natural numbers respectively. The letters \(k, \ell, m, n\) will be used to denote natural numbers, as well as \(i, j, \alpha, \beta, \gamma, \zeta, \xi\). We let \(\varepsilon\) be a real (usually positive).

If \(A\) is a set,

\[ [A]^n = \{ u \subseteq A : |u| = n \}. \]

We call finite subsets \(u, v\) of \(\mathbb{N}\) neighbors if:

\[ |u| = |v|, \ |u \setminus v| = 1 \]

and

\[ [k \in u \setminus v, \ell \in v \setminus u, m \in u \cap v \Rightarrow k < m \equiv \ell < m]. \]

For \(m \in \mathbb{N}\), we let \([m] = \{1, \ldots, m\}\).

For a set \(A\) of natural numbers and \(i \in \mathbb{N}\), \(A < i\) means \((\forall j \in A)(j < i)\). We similarly define \(i < A\).

With \(i, A\) as above

\[ A_{>i} \text{ denotes the set } \{ j \in A : j > i \}. \]

We use the convention that \(A_{>\sup \emptyset}\) is \(A\).

Let \(\exists_n(m)\) be defined by induction on \(n : \exists_0(m) = m\) and \(\exists_{n+1}(m) = 2\exists_n(m)\).

Usually, \(c_i\) denotes a constant.

**1.1 Lemma** (Finitary Canonization). Assume \(n\) is given, then there is a constant \(c\) computable from \(n\), such that if \(m\) is large enough:

If \(f\) is an \(n\)-place function from \([m^\otimes] = \{1, \ldots, m^\otimes\}\) and \(m^\otimes > \exists_{n-1}(cm^{8(2n-1)})\) then for some \(A' \in [(1, \ldots, m^\otimes)]^m\), \(f\) is canonical on \(A'\); i.e. for some \(v \subseteq \{1, \ldots, n\}\) for every \(i_1 < \cdots < i_n\) from \(A'\) and \(j_1 < \cdots < j_n\) from \(A'\), we have

\[ f(i_1, \ldots, i_n) = f(j_1, \ldots, j_n) \Leftrightarrow \bigwedge_{\ell \in v} i_\ell = j_\ell. \]
The proof is broken into several claims.

Explanation of our proof.

We inductively on $n^* = n^\otimes, \ldots, 1$ decrease the set to $A_{n^*}$ while increasing the amount of “partial homogeneity”, i.e. conditions close to: results of computing $f$ on an $n$-tuple from $A_{n^*}$ are not dependent on the last $p = n^\otimes - n^*$ members of the $n$-tuple. Having gone down from $n^\otimes$ to $n^*$, we want that: if $u_1, u_2 \in [A_{n^*}]^n$ are neighbors differing in the $\ell$-th place element only then: if $\ell < n^*$, the truth value of $f(u_1) = f(u_2)$ depends on the first $n^*$ elements of $u_1$ and $u_2$ only; if $\ell > n^*$ the truth value of $f(u_1) = f(u_2)$ depends on the first $n^*$ elements of $u_1$ only. Lastly if $\ell = n^*$, it is little more complicated to control this; but the truth value is monotonic and we introduce certain functions, (the $h$’s) which express this. Arriving to $n^* = 1$ we eliminate the $h$’s (decreasing a little) so we get the sufficiency of the condition for equality, but we still have the necessity only for $u_1, u_2$ which are neighbors. Then by random choice (as in [Sh37]), we get the necessity for all pairs of sets. The earlier steps cost essentially one exponentiation each, the last two cost only taking a power.

1.2 Claim. Assume

\begin{equation}
(*)_0 \quad \text{\textit{\textup{(}}0\text{\textit{\textup{)}}}} \quad m \geq 2^{(1+\varepsilon)c_1(m^*)^{n^*}}
\end{equation}

\begin{equation*}
t > 0, \quad n^* > 1, \quad k(*) > 0 \quad (c_1 \text{ is defined in the proof from } k(*), \quad n^*)
\end{equation*}

and $m^*$ is large enough (relative to $1/\varepsilon, t, k(*), n^*$)

\begin{equation}
(*)_1 \quad A \subseteq \mathbb{N}, \quad |A| > m
\end{equation}

$f_k$ a function with domain $[A]^n^*$ for $k < k(*)$, 

$h_k$ is a function from $[A]^n^*$ to $\mathbb{N}$ for $k < k(*)$, and 

$g$ is a function with domain $[A]^n^*$ such that $\text{Rang}(g)$ has cardinality $\leq t$.

Then we can find $A^*, j^*$ such that:

\begin{equation}
(*)_2 \quad A^* \subseteq A, \quad |A^*| > m^* \text{ and } j^* \in A_{\text{sup}(A^*)} \text{ and we have:}
\end{equation}

\begin{enumerate}
\item[\textit{(a)}] if $u, v$ are neighbors, then for all $i \in A_{\text{sup}(u \cup v)}$ we have

\begin{equation*}
f_k(u \cup \{i\}) = f_k(v \cup \{i\}) \iff f_k(u \cup \{j^*\}) = f_k(v \cup \{j^*\})
\end{equation*}

\item[\textit{(b)}] if $u = v$ then for every $i_0 < i_1$ from $A^*_{\text{sup}(u)}$ we have

\begin{equation*}
f_k(u \cup \{i_0\}) = f_k(u \cup \{i_1\}) \iff f_k(u \cup \{i_0\}) = f_k(u \cup \{j^*\})
\end{equation*}

\item[\textit{(c)}] for all $i \in A^*_{\text{sup}(u)}$

\begin{equation*}
g(u \cup \{i\}) = g(u \cup \{j^*\})
\end{equation*}
\end{enumerate}

\textsuperscript{1}This is used later to define the $h_k$ for the “next step”.
either for all \( i \in A^*_{>\sup(u)} \cup \{j^*\} \) we have 
\[ h_k(u) \geq i \]

or for all \( i \in A^*_{>\sup(u)} \cup \{j^*\} \) we have 
\[ h_k(u) < i. \]

1.2 A Remark. (1) We could have also related \( f_{k_1}(u), f_{k_2}(u) \) for various \( k_1, k_2 \), this would not have influenced the bounds.

Proof: Standard ramification. For \( B \subseteq A \) we define an equivalence relation \( E_B \) on \( A_{>\sup(B)} \) as follows. We let:
\[ i_0 E_B i_1 \iff i_0, i_1 \in A_{>\sup(B)} \] and for every \( u, v \in [B]^{n^*-1}, d \in \text{Rang}(g), w \in [B]^{n^*} \) and \( k < k(*) \) the truth value of the following is the same for \( \ell \in \{0, 1\} \):

\[
\begin{align*}
(\alpha) \quad & f_k(u \cup \{i\}) = f_k(v \cup \{i\}) \text{ if } u, v \text{ are neighbors} \\
(\beta) \quad & f_k(u \cup \{i\}) = f_k(w) \text{ if } u = w \setminus \{\max(w)\} \\
(\gamma) \quad & g(u \cup \{i\}) = d \\
(\delta) \quad & h_k(u) \geq i. 
\end{align*}
\]

Clearly \( E_B \) is an equivalence relation and \( E_\emptyset \) is the equality (as \( n^* > 1 \)).

For \( i \in A_{>\sup(B)} \) we let \( i/E_B \) denote the equivalence class of \( i \) via \( E_B \).

Note that if \( B \subseteq B^* \), then \( i/E_{B^*} \subseteq i/E_B \).

We now define a tree \( T \) by defining by induction on \( \ell \in \mathbb{N} \) objects \( t_{\leq \ell}, \leq \ell \) and \( \langle A_i : i \in t_{\leq \ell} \rangle \) such that:

\[
\begin{align*}
(\alpha) \quad & (t_{\leq \ell}, \leq \ell) \text{ is a tree, } t_{\leq \ell} \text{ a subset of } A, \leq \ell \text{ a partial order on } t_{\leq \ell} \text{ such that for every } x \in t_{\leq \ell}, \{y : y < x\} \text{ is linearly ordered} \\
(b) \quad & t_{\leq \ell} \subseteq t_{\leq \ell+1} \text{ and } t_{\leq \ell+1} \upharpoonright t_{\leq \ell} = t_{\leq \ell} \\
(c) \quad & t_{\leq 0} = \{\min(A)\}, A_{\min(A)} = A_{>\min(A)} \\
(d) \quad & t_{\leq (\ell+1)} \setminus t_{\leq \ell} \text{ is the } (\ell + 1)\text{-th level of } (t_{\leq (\ell+1)}, \leq (\ell+1)) \\
(e) \quad & \text{if } i_0 < i_1 < \cdots < i_\ell \in t_{\leq \ell} \text{ (so } \{i_0, \ldots, i_\ell\} \text{ is a branch) then} \\
(\alpha) \quad & A_{i_\ell} = i_\ell/E_{\{i_0, \ldots, i_{\ell-1}\}} \\
(\beta) \quad & \text{the set of immediate successors of } i_\ell \text{ in } (t_{\leq (\ell+1)}, \leq (\ell+1)) \text{ is } \\
& Y_{i_\ell} := \{\min(j/E_{\{i_0, i_1, \ldots, i_\ell\}}) : j \in A_{i_\ell} \text{ but } j \neq i_\ell\}. 
\end{align*}
\]

This is straight. Let \( t_\ell = t_{\leq \ell} \setminus \bigcup_{m < \ell} t_{\leq m} \) and \( T = \bigcup_{\ell} t_{\leq \ell} \).

Note also that \( i \leq \ell, j \Rightarrow i \leq j \) and that

\[ \otimes \text{ if we consider the definition of } E_{\{i : i \leq \ell, j\}} \text{ restricted just to } A_j \setminus \{j\} \text{ we may restrict ourselves: for clause (}\alpha\text{) only to the } u, v \in [[i : i \leq \ell, j]]^{n^*-1} \text{ with } \max(u \cup v) = j, \text{ and for clause (}\beta\text{) only to those } u \in [[i : i \leq \ell, j]]^{n^*-1}, w \in [[i : i \leq \ell, j]]^{n^*} \text{ with } \max(w) = j. \]

For (\gamma) and (\delta) we may assume \( \max(u) = i_\ell \).
Now it is easy to see that

\[ (*)_3 \quad A = \bigcup_{\ell} t_\ell \]

\[ (*)_4 \quad \text{if } j \in t_\ell \text{ then the number of immediate successors of } j \text{ in } (t_{\leq \ell+1}; \leq \ell+1) \]

(necessarily they are all in \( t_{\ell+1} \)) is at most

\[
\left( 2^{(n^*_{\ell-1})(n^*-1)} \right)^{k(\ast)} \times \left( 2^{(n^*_{\ell-1})} \right)^{k(\ast)} \times \ell^{(n^*_{\ell-2})} \times \left( (n^*_{\ell-2}) \cdot k(\ast) + 1 \right).
\]

[Why this inequality? The four terms in the product correspond to the four clauses \((\alpha), (\beta), (\gamma), (\delta)\) in the definition of \(E_B\) for the branch \( B = \{ i_0, \ldots, i_\ell = j \} \) of \((t_{\leq \ell}; \leq)\). The power \( k(\ast) \) in the first two terms comes from dealing with \( f_k \) for each \( k < k(\ast) \) and “2 to the power \( x \)” as we have \( x \) choices of yes/no. Now the first term comes from counting the possible \( u \cup v \) (from clause \((\alpha)\)). At the first glance their number is \([\{i_0, \ldots, i_\ell\}]^{n^*}\) as being neighbors each with \( n^* - 1 \) elements they have together \( n^* \) elements, but by \( \bigotimes \) we can restrict ourselves to the case \( i_\ell \in u \cup v \), so we have to consider \([\{i_0, \ldots, i_{\ell-1}\}]^{n^*-1} = (n^*_{\ell-1}) \) sets \( u \cup v \); then we have to choose \( u \cup v \setminus (u \cap v) \) (as we do not need to distinguish between \((u, v)\) and \((v, u)\)). As \( u, v \) are neighbors we have \( n^* - 1 \) possible choices (as the two members of \((u \cup v)\setminus (u \cap v)\) are successive members of \( u \cup v \) under the natural order).

For the second term, we should consider \( u, w \) as in clause \((\beta)\), and so as \( u = w \setminus \{ \max(w) \} \) we know \( w \) gives all the information, and by \( \bigotimes \) above \( \max(w) = i_\ell \), so the number of possibilities is \((n^*_{\ell-1})\).

For the third term we have a choice of one from \( \leq t (= |\text{Rang}(g)|) \) for each \( u \in [[i_0, \ldots, i_\ell]]^{n^*_{\ell-1}} \), but again by \( \bigotimes \), with \( \max(u) = i_\ell \), so the number is \((n^*_{\ell-2})\).

Lastly, in the fourth term the number of questions “\( h_k(u) \geq i \)” is again \((n^*_{\ell-2}) \cdot k(\ast)\), but by the properties of linear orders there are \((n^*_{\ell-2}) \cdot k(\ast) + 1\) possible answers. So \((*)_4\) really holds.]

Clearly (with \( c_0 = k(\ast)/(n^* - 2)! + k(\ast)/(n^* - 1)!\))

\[
(*)_5 \quad \left( 2^{(n^*_{\ell-1}) \times n^*-1} \right)^{k(\ast)} \times \left( 2^{(n^*_{\ell-1})} \right)^{k(\ast)} \times \ell^{(n^*_{\ell-2})} \times \left( (n^*_{\ell-2}) \cdot k(\ast) + 1 \right)
\]

\[
\leq 2^{k(\ast)\ell n^*-1/(n^*-2)!} \times 2^{k(\ast)\ell n^*-1/(n^*-1)!} \times 2^{\log(t)\ell n^*-2/(n^*-2)!} \times \ell^{n^*-2} \cdot k(\ast)/(n^* - 2)! \leq 2c_0 \ell^{n^*-1}(1+\varepsilon).
\]

(any positive \( \varepsilon \), for \( \ell \) large enough; actually we can replace \( \varepsilon \) by e.g. \( 1/\ell^{1-\varepsilon}, \varepsilon > 0 \)).

So (for some constant \( c_0^2 \))
Claim. Assume $A \subseteq \mathbb{N}$, $|A| \geq m(\subseteq) + 1$, $g$ is a function with domain $[A]^{n \otimes}$ and range with $\leq t$ members; $f_k$ is a function with domain $[A]^{n \otimes}$ (for $f < k(*)$), and for simplicity $\mathcal{P}([0,1,\ldots,n \otimes - 1]) \cap \text{Rang}(f_k) = \emptyset$.

Then we can find $A' \subseteq [A]^{m(n^*)+1}$ and $j^*_k \in A$ for $k \in [n^*,n^{\otimes})$ satisfying $A' < j^*_n < j^*_{n+1} < \ldots$, and functions $g'$, $g_k$, $h_k$ ($k < k(*)$) with domain $[A']^{n^*}$ such that (letting $w^* = \{j^*_k \colon k \in [n^*,n^{\otimes})\}$):

(a) for $w \in [A']^{n^*}$ we have $g(u \cup w) = g'(u) = g(u \cup w^*)$

(b) for $k < k(*)$ we have $h_k(u) \in \mathbb{N}$ and $g_k(u) \in \{v : v \subseteq (n^*,n^{\otimes})\}$
Proof: We prove this by induction on $n^\otimes - n^*$ and $k < k(*)$ and: (note: $|u| = n^*$)

\[
\{ i \in w_1 : |u| + |i \cap w_1| \in g_k(u) \} = \{ i \in w_2 : |u| + |i \cap w_2| \in g_k(u) \}
\]
and $\min(w_1 \cup w_2) < h_k(u) \Rightarrow \min(w_1) = \min(w_2)$

then

\[
f_k(u \cup w_1) = f_k(u \cup w_2).
\]

(d) Assume $k < k(*)$, $w_1 \cup w_2 \subseteq A'$, $u < w_1 < i < j < w_2$ and $|w_1 \cup w_2| = n^\otimes - n^* - 1$:

(i) if $w_1 \neq \emptyset$

\[
f_k(u \cup w_1 \cup \{ i \} \cup w_2) = f_k(u \cup w_1 \cup \{ j \} \cup w_2) \iff |u \cup w_1| \notin g_k(u)
\]

(ii) if $w_1 = \emptyset$

\[
f_k(u \cup \{ i \} \cup w_2) = f_k(u \cup \{ j \} \cup w_2) \iff h_k(u) \leq i.
\]

(e) for $k < k(*)$ and neighbors $u_0, u_1 \in [A']^{n^*}$ and $w \in [A'_{\max(u_0 \cup u_1)}]^{n^\otimes - n^*}$ we have:

\[
f_k(u_0 \cup w) = f_k(u_1 \cup w) \iff f_k(u_0 \cup w^*) = f_k(u_1 \cup w^*).
\]

Remark.. (1) Note particularly clause (d). So $g_k(u)$ is intended to be like the $v$ in 1.1, only fixing an initial segment of both $\{ i_\ell : \ell < n^\otimes \}$ and $\{ j_\ell : \ell < n^\otimes \}$ as $u$. But whereas the equality demand in clause (d) is as expected, the non-equality demand is weaker: only for neighbors.

(2) Note that we can in some clauses above replace $A'$ by $A' \cup w^*$.

Proof: We prove this by induction on $n^\otimes - n^*$. If it is zero, the conclusion is trivial.

Use the induction hypothesis with $n^\otimes$, $n^* + 1$, $f_k$, $(k < k(*)$, $g$ now standing for $n^\otimes$, $n^*$, $f_k$, $(k < k(*)$, $g$ in the induction hypothesis. We get $A' \subseteq [A]^{m(n^* + 1) + 1}$ and functions $g', g_k, h_k$ (for $k < k(*)$) and $j^*_\ell$ for $\ell \in [n^* + 1, n^\otimes]$ satisfying $(*)_{11}$ of Claim 1.3. Now we apply 1.2 to $n^* + 1$ and $m = m(n^* + 1), A', g', f^\otimes, h^\otimes (k < k(*)$) where we define the function $g^\otimes$ with domain $[A']^{n^* + 1}$ by $g^\otimes(u) = \langle g'(u), g_k(u) : k < k(*) \rangle$, $h^\otimes_k = h_k$ and the function $f^\otimes_k$ with domain $[A']^{n^* + 1}$ is defined by

\[
f^\otimes_k(u) = f_k(u \cup \{ j^*_\ell : \ell \in [n^* + 1, n^\otimes] \}).
\]

We get there $A^* \subseteq [A']^{m(n^*) + 1}$ and $j^* \in (A')_{\sup A^*}$. Let $j_{n^*} =: j^*$. Now we have to define $h_k$ with domain $[A^*]^{n^*}$ (for $k < k(*)$). For $u \in [A^*]^{n^*}$ let

\[
B^k_u =: \{ i \in A^*_{\sup(u)} : f^\otimes_k(u \cup \{ i \}) \neq f^\otimes_k(u \cup \{ j^* \}) \}.
\]
By clause (β) of Claim 1.2, \( B^k_i \) is an initial segment of \( A^*_\sup(u) \). Let \( h_k(u) = \max(B^k_i) + 1 \).

Lastly, for \( u \in [A^*]^{n^*} \) we have to define \( g_k(u) \). By 1.2 (δ), the answer to
“\( h_k^\Box (u \cup \{j\}) < j_n^* \)” does not depend on \( j \in A^*_\sup u \). Let \( g_k^\Box \) be the “old” \( g_k \)
(with domain \([A']^{n^*+1}\)) and let
\[
g_k(u) = \begin{cases} 
  g_k^\Box(u \cup \{j_n^*\}) & \text{if } h_k^\Box(u \cup \{j\}) < j_n^* \\
  g_k^\Box(n \cup \{j_n^*\}) & \text{otherwise}.
\end{cases}
\]

Now \( A^*, g_k, h_k, j_n^*, j_n^{*+1}, \ldots \) are as required. \( \Box 1.3 \)

1.4 Claim. (1) Assume \( m(1) \geq (k(*) \cdot m(0))^{k(*)+1} \) and \( A' \subseteq \mathbb{N}, |A'| \geq m(1) \) and
for \( k < k(*) \), \( h_k \) is a function from \( A' \) into \( \mathbb{N} \), \( h_k(i) \geq i \).

Then we can find \( A'' \subseteq A', |A''| \geq m(0) \) such that
\[ (*)_{12} \text{ for each } k < k(*) \text{ we have:} \]
\[
\begin{align*}
  & \text{either } (\forall i, j \in A'')[i < j \Rightarrow h_k(i) \geq j] \\
  & \text{or } (\forall i, j \in A'')[i < j \Rightarrow h_k(i) < j].
\end{align*}
\]

(2) If \( m(1) > 2^{k(*)+1}, A \subseteq \mathbb{N}, |A| > m(1), g_k \) is a function from \( A \) to \( \{1, \ldots, d\} \), and \( f_k \) is a function from \( A \) to \( \mathbb{N} \) for \( k < k(*) \) then we can find
\( A' \subseteq A, |A'| > m(0) \) such that:
\[ \bigotimes \text{ for each } k, f_k \uparrow A' \text{ is constant or one to one and } g_k \uparrow A' \text{ is constant.} \]

Proof: (1) We can find \( A_1 \subseteq A', |A_1| \geq m(1)/k(*)^{k(*)} \) such that for all \( i, j \in A_1, \)
\( \ell, k < k(*) \Rightarrow [h_\ell(i) \leq h_k(i) \equiv h_\ell(j) \leq h_k(j)]. \)

So without loss of generality
\[ (*) \text{ } \ell < k < k(*) \& i \in A_1 \Rightarrow h_\ell(i) \leq h_k(i). \]

By renaming we can assume \( A_1 = \{1, 2, \ldots, m(0)^{k(*)+1}\} \).

Now if for some \( \ell, 0 < \ell \leq m(0)^{k(*)+1} - m(0), \) and
\( (\forall \alpha) \left( \alpha \in [\ell, \ell + m(0)] \Rightarrow h_\ell(\alpha) \geq \ell + m(0) \right) \) then \( A'' = [\ell, \ell + m(0)] \) is as required
for all \( h_\ell \) by (*).

If not, then we can find \( \alpha_\ell \in [1, m(0)^{k(*)+1}] \) for \( \ell = 1, \ldots, m(0)^{k(*)} \), strictly
increasing with \( \ell \) such that \( h_\ell(\alpha_\ell) < \alpha_{\ell+1} \). We repeat the argument for \( h_1 \), etc.

(2) Also easy. \( \Box 1.4 \)

Remark. We can use \( m(1) > k(*)! \cdot m(0)^{k(*)+1} \) instead. The only point is the choice of \( A \).
1.5 Claim. Assume we have the assumptions of 1.3. If we first apply 1.4 getting $A'$ and then apply 1.4 to get $A'' \subseteq A'$ such that for each $k$ and $u \in [A'']^{n*}$ either $h_k(u) \leq \min\{\ell \in A' : u < \ell\}$ or $h_k(u) > \max(A'')$ (we assume now $n^* = 1$ so $u = \{j\}$), and in addition

$$(*_{13}) \quad m2^{n^* - n^*} \cdot (2^{n^* - n^*})^{(2^{n^* - n^*}) - 1} \cdot k(*) \leq |A''|$$

then there is $A^* \in [A'']^{m}$ such that (in addition to $(*)_{11}(a)-(e) + (*)_{12}$ we have

$$(*_{14}) \quad \text{for all } u \in [A^*]^{n^*}$$

(f) if $w_1, w_2 \in [A^*_{sup(u)}]^{n^* - n^*}$, $k < k(*)$ then

$$f_k(u \cup w_1) = f_k(u \cup w_2) \Leftrightarrow \{i \in w_1 : |i \cap w_1| + |u| \in g_k(u)\} = \{i \in w_2 : |i \cap w_2| + |u| \in g_k(u)\}.$$ 

Remark. Here we are rectifying the gap between the equality ($(*)_{11}(d)$) and the inequality ($(*)_{11}(e)$) demand.

Proof: First note that

$$(*_{15}) \quad \text{for all } u \in [A'']^{n^*} \text{ the implication } \Rightarrow \text{ holds.}$$

[why? just use clause (c) of $(*)_{11}$ of Claim 1.3].

So we are left with proving $\Rightarrow$.

Choose randomly $m$ members of $A''$. We shall prove that the probability that the set they form has exactly $m$ members and satisfies clause (f), is positive. This suffices. Let us explain. We fix $n^*$ among these elements and call the set they form $u$.

In clause $(*)_{12}$ for $\ell = 1, 2$ we let $v_\ell = \{i \in w_\ell : |u| + |i \cap w_\ell| \in g_k(u)\}$.

By $(*)_{15}$ the problem is that $\Rightarrow$ may fail.

Let $x_1, \ldots, x_m$ be random variables on $A''$. The probability that $\bigwedge_{i \neq j} x_i = x_j$

is $\leq \frac{(m)}{2} \cdot \frac{1}{|A''|}$.

Now for $k < k(1)$, $u \in \{1, \ldots, m\}^{n^*}$, $w_1, w_2 \in \{1, \ldots, m\} \setminus u$,$^{n^* - n^*}$, $v_1 \subseteq w_1, v_2 \subseteq w_2$ defined as above, and a possible linear order $<^*$ on $u^* = u \cup w_1 \cup w_2$, we shall give an upper bound for the probability that

$$\bigwedge_{\ell_1, \ell_2 \in u^*} (\ell_1 <^* \ell_2 \Leftrightarrow x_{\ell_1} < x_{\ell_2})$$

and they form a counterexample to clause (f) (of Claim 1.5). So in particular $u < w_1, u < w_2$. 


Choose $\ell \in v_1 \setminus v_2$ (as $v_1 \neq v_2$ and $|v_1| = |g_k(u)| = |v_2|$ it exists). We can first draw $x_j$ for $j \neq \ell$. Now we know $f_k(u \cup w_2)$; note: we may not know $w_2$ as possibly $\ell \in w_2$, but as $\ell \notin v_2$, by the choice of $A'$ it is not necessary to know $w_2$. Now there is at most one bad choice of $x_\ell$ (the others are good (inequality) or irrelevant ($<^*$ is not right) by (d) + (e)) so the probability of this is $\leq \frac{1}{|A'|}$. So if we fix the set $u^* = u \cup w_1 \cup w_2$ and concentrate on the case $|u^*| = 2n^\otimes - n^*$, we have $2n^\otimes - n^*$ possibilities to choose $\ell \in u^*$ and then having to choose $x_i$ for $i \neq \ell$, we know $u$ and have $\leq \left(\frac{2(n^\otimes - n^*)}{n^\otimes - n^*} - 1\right)$ ways to choose $w_2$, so the probability of failure is $\leq (2n^\otimes - n^*)(\frac{2(n^\otimes - n^*)}{n^\otimes - n^*} - 1) \cdot \frac{1}{|A'|}$.

So the probability that some failure occurs is at most (the cases $|u^*| < 2n^\otimes - n^*$ and $x_1 = x_2$ are swallowed when $m$ is not too small)

$$m^{2n^\otimes - n^*} \cdot k(\ast)(2n^\otimes - n^*) \left(\frac{2(n^\otimes - n^*)}{n^\otimes - n^*} - 1\right) \cdot \frac{1}{|A'|}.$$

Now by assumption $(\ast)_1$ this probability is $< 1$ so the conclusion is clear. $\square_{1.5}$

Before we state and prove the last fact, which finishes the proof of the theorem, we remind the reader of the following observation. The proof is easily obtained by induction on $\ell$.

1.6 Observation. (1) $\nmid_\ell(kx) \geq k\nmid_\ell(x)$ when $x, k \geq 2$ and $\ell \geq 1$.
(2) $\nmid_\ell(kx) \geq (\nmid_\ell(x))^k$ when $x \geq 2$, $k \geq 2$ and $\ell \geq 1$.

1.7 Fact. Assume that $n^\otimes, n^*, m(n^*), k(\ast), \varepsilon, t$ and $c_1$ are as in $(\ast)_9$ (a) and (c).

Let us define

$$c_2 = \text{Max}\{1 + \varepsilon, c_1, 2\}$$

$$c_3 = n^\otimes \times (c_2)^2$$

(in fact $n^\otimes \times c_2$ suffices)

and the function $m(-)$ as follows: for $n \in (n^*, n^\otimes]$ by

$$m(n) = \nmid_{n-n^*}(m^{n^*+1}c_3^{n-n^*})$$

where

$$m(n^*) = m.$$

Then $(\ast)_9$ (b) holds.

Proof: We need to check that for $n \in [n^*, n^\otimes)$

$$m(n + 1) \geq 2^{(1+\varepsilon)c_1m(n)^{n+1}}$$
or equivalently
\[ \log_2(m(n+1)) \geq (1+\varepsilon)c_1 m(n)^{n+1} \]
so it is enough that
\[ \log_2(m(n+1)) \geq c_2 m(n)^{n+1} \]
i.e.
\[ \log_2(\underbrace{m_{n+1-n^*}}_{m_{n^*+1}}) \geq c_2 m(n)^{n+1} \]
i.e., when \( n > n^* \)
\[ \underbrace{m_{n-n^*}}_{c_3(n-n^*)} m_{n^*+1} \geq c_2(\underbrace{m_{n-n^*}}_{c_3(n-n^*) m_{n^*+1}})^{n+1} \]
It suffices by the above observation that
\[ \underbrace{m_{n-n^*}}_{c_3(n-n^*)} m_{n^*+1} \geq \underbrace{m_{n-n^*}}_{c_2(n+1)c_3^{n-n^*} m_{n^*+1}}^{n+1} \]
which is true by the definition of \( c_3 \) when \( n > n^* \).
For \( n = n^* \) we need that
\[ m(n^*+1) \geq 2(1+\varepsilon)c_1 m_{n^*+1} \]
i.e.
\[ 2^{m_{n^*+1}} c_3 \geq 2(1+\varepsilon)c_1 m_{n^*+1} \]
which is true as \( c_3 \geq c_2 \geq (1+\varepsilon)c_1 \).

\[ \square_{1.7} \]

1.8 Proof of Lemma 1.1. So \( m, n, \varepsilon \) are given. Let

(a) \( n^* = 1, n^\otimes = n, k(*) = 1, t = 1, c_1 \) as in 1.2, and \( c_2, c_3 \) as in 1.7
(b) \( m_0 = m \)
\[ m_1 = k(*) \cdot (2n^\otimes - n^*) \cdot \left( \frac{2(n^\otimes - n^*) - 1}{n^\otimes - n^*} \right) (m_0)^{2n^\otimes - n^*} \]
\[ = (2n - 1) \left( \frac{2n - 3}{n - 1} \right) m^{2n-1} \]
\[ m_2 = (k(*)m_1)^{k(*)+1} = (m_1)^2 \]
\[ m_3 = (m_1)^2 \cdot 2^{k(*)} = 2(m_1)^2 \]
(c) we define function \( m(-) \) with domain \([n^*, n^\otimes] \):
for \( \ell = 1 \) we let \( m(1) = m_3 \)

for \( \ell > 1 \) we let \( m(\ell) = \sum_{i=1}^{\ell-1}(c_3^{i-1} \cdot (m_3)^2) \).

So we are given \( m^{\otimes} > m(n) \). In Claim 1.3 from the assumption \((\ast)_9\), clauses (a), (c) hold and clause (b) holds by Fact 1.7. Also assumption \((\ast)_{10}\) of 1.3 holds (with \( \{1, \ldots, m^{\otimes}\} \) standing for \( A, f_0 \) the given function \( f \) (in 1.1), and \( g \) constantly zero).

So there are \( A \in [(1, \ldots, m^{\otimes})]^{m(1)+1} \), \( g', g_0, h_0 \) satisfying the conclusion of 1.3 i.e. \((\ast)_{11}\). \( A \) here stands for \( A' \) in 1.3. Note \( |A| = m_3 + 1 \). Now apply 1.4 (2) with \( A, m_3, m_2, f_0, g_0, 1 \) here standing for \( A, m(1), m(0), f_0, g_0, k(\ast) \) there and get \( A' \in [A]^{m^2_2+1} \). Next we apply Claim 1.4 (1) with \( A', m_2, m_1, h_0, 1 \) here standing for \( A', m(1), m(0), h_0, k(\ast) \) there and get \( A'' \in [A']^{m_1} \) satisfying the conclusion of 1.4 (1) i.e. \((\ast)_{12}\). Lastly apply Claim 1.5 and get \( A^* \in [A'']^{m_0} = [A'']^m \) satisfying the conclusion of 1.5; i.e. \((\ast)_{14}\). Now \( A^* \) is as required.

1.9 Remark. We could have applied 1.5 in each stage, or just for \( n = 3 \), this saves, somewhat.

References


Institute of Mathematics, The Hebrew University, Jerusalem, Israel

Rutgers University, Department of Mathematics, New Brunswick, NJ, USA

(Received September 11, 1995)