SORTING IN $c \log n$ PARALLEL STEPS

M. AJTAI, J. KOMLÓS and E. SZEMERÉDI

Received 6 June 1982

We give a sorting network with $cn \log n$ comparisons. The algorithm can be performed in $c \log n$ parallel steps as well, where in a parallel step we compare $n/2$ disjoint pairs. In the i-th step of the algorithm we compare the contents of registers $R_{j(i)}$, and $R_{k(i)}$, where $j(i), k(i)$ are absolute constants then change their contents or not according to the result of the comparison.

1. Introduction

Let L be a linearly ordered set with n elements. The elements of L are originally stored in n registers $(R_1, R_2, ..., R_n)$. The set of registers will be denoted by $\mathscr{R}$. We want to give an algorithm which rearranges the elements of L in the registers such that the least element of L be in R_1 the next one in R_2 etc. the greatest in R_n. An *elementary step* of this algorithm consists of the comparison of two elements a, a' located at two given registers R, R'. We have either $a \leqq a'$ or $a > a'$. In both cases we can exchange the locations of a and a' or leave them unchanged. Thus, we can have four different rules. Now the algorithm consists of a sequence of pairs (R, R') of registers and a sequence of associated rules (of the above kind). In other words we obtain a network. The constructed network will contain only $O(n \log n)$ of the above steps $((R, R')$ and a rule$)$, and we will show that the first $n/2$ steps can be performed simultaneously (i.e. the pairs (R, R') involved are disjoint) and so can the second $n/2$ steps, etc. Thus we get a sorting algorithm working in $O(\log n)$ parallel steps. In the following by a parallel step we mean a set of at most $n/2$ disjoint elementary steps.

Parallel sorting algorithms has been intensively studied. The best known parallel sorting algorithm with maximum parallelity (and disjoint comparisons) reduce sorting to merging. There are algorithms which use only $\log n$ steps for merging (Batcher, Pratt and others see Knuth [2]. These lead to sorting algorithms using $O((\log n)^2)$ steps.

The sorting algorithm presented here were originally a random algorithm, but

AMS subject classification (1980): 68 E 05

(using explicitly given expander graphs see [1] and [3]) we transformed it into a deteıministic one. We give the algorithm in that form.

Following the suggestion of D. Knuth we modified our original algorithm in an other way so that it became "oblivious" in that it is a sorting network with $O(n \log n)$ modules, see also Knuth [2].

The structure of the algorithm can be visualized the easiest way as a tree like file organization. We use a binary tree with n leaves (if n is a power of 2) in which the nodes on the same level are ordered. The registers are assigned to some nodes, originally each registers is assigned to the root (the upmost node). The algorithm is organized into cycles, one cycle consist of the application of subroutines and each subroutin rewrites the tree, i.e. reaasignes the registers to nodes. After one cycle each register have moved some level down or some levels up on the tree. The point is that the majority moved down and only few registers moved up. We will show that after $O(\log n)$ such cycles all registers will have moved down to the leaves, different registers to different leaves, and that stage the leaves define the ordering.

At each stage, there is a lowest nonempty level of nodes, and most elements will stay on this level, the number of element on higher and higher levels will form a geometric series. In each cycle we perform some parallel steps. The sequence of the parallel steps in the α-th cycle will be denoted by P^{α}. The length of P^{α} will be less then some constant c_0. After the α-th cycle the set of registers assigned to the element t of the tree will be denoted by $S^{\alpha}(t)$. $S^{0}(t)$ is $\mathscr{R}$ if t is the root of the tree, otherwise it is the empty set. The restriction of the function S^{α} to a fixed level of height i will be denoted by $S^{\alpha, i}$.

We will define S^{α} and P^{α} by recursion on α.

2. The description of the algorithm

We will define our algorithm using the constants $c_1, c_2, q_1, q_2, \varepsilon_1, d_1, g$. We do not give the actual values of these constants only assume certain inequalities between them.

We choose the constants in the following order: $c_1, q_1, g, q_2, \varepsilon_1, c_2, d_1$ so that $q_1, g, q_2, \varepsilon_1 \in (0, 1)$; $c_1, c_2, d_1 > 1$;

$$\varepsilon_1 \ll q_2 \ll 1-g \ll q_1 \ll \frac{1}{c_1} \ll 1 \quad \text{and}$$

$$1 \ll c_2, \quad \frac{1}{1-g} \ll c_2, \quad d_1 \gg \frac{1}{q_2}$$

where $a \ll b$ means that a is sufficiently small compared to b (or b is sufficiently large compared to a).

We will not use the constant q_2 in the actual definition of the algorithm, only in the proofs.

Definitions. Let T be the set of all finite 0, 1 sequences (including the empty sequence 0). (Actually we will use only sequences of length less than n.) We consider T as a tree whose levels (the set of sequences of the same length) are ordered by the lexicographic ordering, that is $\langle a_1, \ldots, a_k\rangle < \langle b_1, \ldots, b_k\rangle$ iff they are different and $a_i < b_i$ where i is the smallest index where the two sequences differ.

$\langle a_1, \ldots, a_i\rangle \prec \langle b_1, \ldots, b_j\rangle$ means that $i \geqq j$ and for all $k \leqq j$, $a_k = b_k$.

If $t = \langle a_1, \ldots, a_i\rangle$ then $\langle t, b_1, \ldots, b_j\rangle$ will denote the sequence $\langle a_1, \ldots, a_i, b_1, \ldots, b_j\rangle$.

Dom (f) will denote the domain of the function f, $l(t)$ will be the length of the sequence t.

A one-to-one map of $\mathscr{R}$ onto L will be called a *position*. If $X \subseteqq \mathscr{R}$ and F is a position then we will use the following notations:

$$\mathrm{Cont}_F(X) = \{a \in L \mid \exists R \in X\ a = F(R)\}.$$

$$\mathrm{reg}_F(a) = F^{-1}(a) \quad \text{if} \quad a \in L.$$

We will omit the subscript F, if it is uniqually determined by the context.

C is a *chain* iff C is a function defined on some level of T and for all $x, y \in \mathrm{Dom}\,(C)$ we have $C(x) \subseteqq \mathscr{R}$, $C(x) \cap C(y) = 0$ and $|C(x)| = |C(y)|$.

The chains C_1 and C_2 are disjoint iff $C_1(x) \cap C_2(y) = 0$ for all $x \in \mathrm{Dom}\,(C_1,)$ $y \in \mathrm{Dom}\,(C_2)$.

We want to define the function S^α so that $S^{\alpha, i}$ be a chain for all i.

If C is a chain we will use the following notations:

$l(C) = \log_2 |\mathrm{Dom}\,(C)|$,

$N(C) = |C(x)|$ for some (all) $x \in \mathrm{Dom}\,(C)$,

$|C| = |\mathrm{Dom}\,(C)|$,

$\bigcup C = \bigcup\limits_{t \in \mathrm{Dom}(C)} C(t)$,

$\mathrm{Cont}_F(C) = \bigcup\limits_{t \in \mathrm{Dom}(C)} \mathrm{Cont}_F C(t)$ where F is a position.

If C_1, C_2 are disjoint chains with $l(C_1) = l(C_2)$ $C_1 \cup C_2$ will be the chain defined by $(C_1 \cup C_2)(t) = C_1(t) \cup C_2(t)$ for all $t \in \mathrm{Dom}\,(C_1)$.

Now we will define operations on chains. In order to make this operations uniqually defined we will suppose that the set $\mathscr{R}$ is ordered in an arbitrary but fixed way.

Suppose that C is a chain and $0 < q < 1$. Then CH1 (C, q) will be a chain with the following properties:

(1) Dom (CH1 (C, q)) = Dom (C)

(2) (CH1 (C, q))(t) consists of the first $4\left[\frac{1}{4} q |C(t)|\right]$ elements of $C(t)$, where $[x]$ denotes the integral part of the number x.

CH2 (C, q) is a chain with the same domain defined by

$$(\mathrm{CH2}(C, q))(t) = C(t) - (\mathrm{CH1}(C, q)(t)).$$

The following lemmas are necessary for the definition of S^α.

Lemma 1. *Let C be a chain, $l(C) = i$, $0 \leqq j < i$ and suppose that $N(C) \geqq 2$. Let us define a chain $V(C, k)$ for all k, $0 \leqq k < i$.*

If $l(t)=j$ *let* $(V(C,j))(t)$ *be the set consisting of the first element of* $C(t_0)$ *and the first element of* $C(t_1)$ *where* t_0 *and* t_1 *are sequences of length* i *defined by* $t_0=\langle t, 0, \dots, 0\rangle$, $t_1=\langle t, 1, 0, \dots, 0\rangle$.

If $j<k<i$ *and* $l(t)=k$ *let* $(V(C,k))(t)$ *be the set whose only element is the first element of* $C(t_0)$ *where* $t_0=\langle t, 1, 0, \dots, 0\rangle$, $l(t_0)=i$.

If $l(t)=i$ *let* $(V(C,i))(t)=C(t)-\cup\{\cup V(C,k) \mid j\leqq k<i\}$. *If* $0\leqq k<j$ *and* $l(t)=k$ *let* $V(C,k)(t)=0$. *Then* $V(C,k)$ *is a chain for all* $0\leqq k\leqq i$ *and the following conditions are satisfied:*

(1.1) $l(V(C,k))=k$.

(1.2) $(\cup V(C,k))\cap\cup V(C,k')=0$ *if* $k\neq k'$.

(1.3) $N(V(C,k))=1$ *if* $j<k<i$, $N(V(C,j))=2$,

$N(V(C,k))=0$ *if* $0\leqq k<j$.

(1.4) *For all* $t'\in T$, $j\leqq l(t')\leqq i$ *we have*

$$\bigcup_{l(t)=i,\, t\prec t'} C(t) \supseteqq V(C,k)(t').$$

(1.5) *For all* $t\in \mathrm{Dom}\,(C)$

$$\Big|C(t)\cap\bigcup_{0\leqq k<i}(\cup V(C,k))\Big| = 1.$$

Since (1.1), ..., (1.5) are all immediate consequences of the definition of V we omit the proof of this Lemma.

Lemma 2. *Suppose that* C *is a chain* $l(C)=i$ *and* $\langle a_k\rangle$, $0\leqq k<i$ *is a sequence of nonnegative integers with the following properties:*

(2a) $$2\Big(\sum_{k<i} a_k\Big) < N(C)$$

and

(2.b) $\exists s'<s\ a_{s'}>0$ *implies that* $\sum_{k<s} a_k<a_s$ *for all* $s<i$. *Then for all* $k, 0\leqq k<i$ *there exists a chain* $W(C,k)$ *such that properties* (1.1), (1.2) *and* (1.4) *hold with* $j=0$ *and* $V=W$ *and:*

(2.3) *for all* $0\leqq k<i$ $a_k-1\leqq N(W(C,k))\leqq a_k$

and

(2.5) *the function* W *on* $\mathrm{Dom}\,(C)$ *defined by*

$$\overline{W}(t) = C(t)-\bigcup_{k<i}(\cup W(C,k))$$

is a chain and

$$N(C)-\sum_{k<i} a_k \leqq N(\overline{W}) \leqq N(C).$$

Proof. For all $0\leqq k<i$ we define a sequence of chains $Y_{s,k}$ $s=0, 1, 2, \dots$ with $l(Y_{s,k})=k$ and we will put

(2.6) $$W(C,k) = \bigcup_s Y_{s,k}$$

We define the sequence $Y_{s,k}\, s=0, 1, \dots$ by induction on s. Let us suppose that for $s'<s$ $Y_{s,k}$ is defined for all $0 \leqq k<i$ with $l(Y_{s,k})=k$.

Let j be the greatest integer with the following property: $0 \leqq j<i$ and for all $0 \leqq k<j$

$$\sum_{s'<s} N(Y_{s'k}) \geqq a_k-1.$$

If j does not exist we do not define $Y_{s,k}$. Suppose $j<i$. For all $t, l(t)=i$ let

$$C'(t) = C(t) - \bigcup_{\substack{s'<s \\ k<i}} (\cup Y_{s,k}).$$

For all $0 \leqq k<i$ let $Y_{s,k}=V(C', k)$ where V is the function defined in Lemma 1, (with the j given above). It is easy to check that the W defined by (2.6) meets the requirement of Lemma 2. ▌

Now using Lemma 2 we will define S^α. $S^0(t)$ has already been defined by

$$S^0(t) = \begin{cases} \mathscr{R} & \text{if } t=0 \\ 0 & \text{otherwise.} \end{cases}$$

Suppose that $2^{-\alpha-2}n>c_2$ and S^α is defined, then we define $S^{\alpha+1}$ as follows: let

$$C_1^i = \mathrm{CH1}(S^{\alpha,i}, g)$$

$$C_2^i = \mathrm{CH2}(S^{\alpha,i}, g)$$

Definition. If C is a chain then the chains $\pi_{-1}C, \pi_1 C, \pi_2 C$ are defined by

$$(\pi_{-1}C)(t) = C(\langle t, 0\rangle) \cup C(\langle t, 1\rangle) \quad \text{for all} \quad l(t) = l(C)-1.$$

$(\pi_1 C)(\langle t, 0\rangle)$ is the first $1/2|C(t)|$ element of $C(t)$ if $t \in \mathrm{Dom}\,(C)$, $\pi_1(C)(\langle t, 1\rangle)=C(t)-(\pi_1 C)(\langle t, 0\rangle)$ ($\pi_1 C$ is defined only if $N(C)$ is even).

$\pi_2 C=\pi_1(\pi_1 C)$, $\pi_2 C$ is defined only if $4|N(C)$. Clearly

$$l(\pi_1 C)=l(C)+1,\ l(\pi_2 C)=l(C)+2,\ l(\pi_{-1}C)=l(C)-1.$$

Let $D^\alpha=\pi_1 C_1^\alpha \cup \pi_3 C_1^{\alpha-1}$ (for $\alpha=0$ let $D^\alpha=\pi_1 C_1^j$). Since $4|N(C_1^0)$ for all j, D^α is always defined. Let us apply Lemma 2 with $C=D^\alpha$, $i=a+1$ and $a_k=0$ if $q_1^{\alpha+1-k}2^{-\alpha-2}n<c_1$ $a_k=[q_1^{\alpha+1-k}2^{-\alpha-2}n]+2$ otherwise. We will prove by induction on α that the sequence $\langle a_k\rangle$ satisfies the conditions of Lemma 2 (see Lemma 7). Let $W(D^\alpha, k)$ be the chains guaranteed by Lemma 2 and k_0 the smallest integer with

$$q_1^{\alpha+1-k_0}2^{-\alpha-2}n \geqq C_1 \tag{2.7}$$

Now for all $k_0<k \leqq \alpha$ put

$$S^{\alpha+1,k} = W(D^\alpha, k) \cup \pi_{-1}C_2^{k+1} \cup \pi_2 C_1^{k-2} \tag{2.8}$$

and for $k=k_0$

$$S^{\alpha+1,k_0} = W(D^\alpha, k_0) \cup \pi_{-1}C_2^{k_0+1} \cup \tag{2.9}$$

$$\cup\, \pi_2 C_1^{k_0-2} \cup C_2^{k_0} \cup \pi_1(C_2^{k_0-1} \cup \pi_1 C_2^{k_0-2})$$

and for $k<k_0$ $S^{\alpha,k}(t)=0$ for all $l(t)=k$. We omit the last term in (2.8) if $k=1$ and in (2.9) if $k_0=0$; we substitute the last term in (2.9) by $\pi_1 C_2^{k_0-1}$ if $k_0=1$ and omit the term $\pi_2 C_1^{k_0-2}$ if $k_0=0, 1$. For $k=\alpha$ we omit $\pi_{-1} C_2^{k-1}$. Finally we define $S^{\alpha+1,\alpha+1}$ by

$$S^{\alpha+1,\alpha+1}(t) = D^{\alpha}(t) - \bigcup_{k<\alpha} \left(\bigcup W(D^{\alpha}, k)\right)$$

Since C_1^j is always divisible by 4 the operations $\pi_1 C_1^j$, $\pi_2 C_1^j$ can be performed in the definition of $S^{\alpha+1,k}$, $S^{\alpha+1,k_0}$. Later we will prove that the operations π_1 in the last term of (2.9) can be performed as well.

To give the sequence P^{α} we need further definitions.

Definition 2.2. Suppose that A and B are disjoint sets. We call the graph G a *$\langle k, \varepsilon\rangle$ expander on $\langle A, B\rangle$* if $A \cup B$ is the set of vertices of G, no edge of G is in A or B, and the degree of every point is at most k and if Γ_X denotes the set of neighbours of the set X then for all $X \subseteqq A$ we have

$$|\Gamma_X| > (1-\varepsilon)\frac{1}{\varepsilon}\min\{|X|, \varepsilon|B|\}$$

and for all $Y \subseteqq B$, we have

$$|\Gamma_Y| > (1-\varepsilon)\frac{1}{\varepsilon}\min\{|Y|, \varepsilon|A|\}.$$

Lemma 3. *For all $0<\varepsilon<1$, $c \geqq 1$ there exists a positive integer $k(\varepsilon, c)$ such that for all disjoint A, B with $1/c \leqq |A|/|B| \leqq c$ there exists a $\langle k, \varepsilon\rangle$ expander on $\langle A, B\rangle$.*

The assertion of the Lemma and an explicit construction for the graph easily follows from Margulis results [3], but he proves only the existence of the function $k(\varepsilon, c)$. Gabber and Galil [1] gave the function $k(\varepsilon, c)$ as well in an explicit form. (The usual definition of an expander graph is somewhat different from the one given here.) In the following we will suppose that $k(\varepsilon, c)$ is a fixed function satisfying the requirements of Lemma 3.

Definition 3.1. If A, B are disjoint subsets of $\mathscr{R}$ and $\varepsilon>0$, then let $G_{\varepsilon}(A, B)$ be a fixed $\langle k(\varepsilon, |A|/|B|), \varepsilon\rangle$ expander on $\langle A, B\rangle$.

According to the remarks after Lemma 3 we may suppose that $G_{\varepsilon}(A, B)$ is given in some explicit way.

Definition 3.2. If A, B are disjoint subsets of $\mathscr{R}$, $\varepsilon>0$ then let $E_{\varepsilon}(A, B)$ be the set of all elementary steps of the following type: R_1, R_2, "if the content of R_1 is greater than the content of R_2 then exchange the contents of these registers, otherwise leave them unchanged", where $R_1 \in A$, $R_2 \in B$ and $\langle R_1, R_2\rangle$ is an edge of $G_{\varepsilon}(A, B)$.

The role of the expander graphs in our algorithm is based on the following Lemma to be proved later.

Definition 3.3. Let J be an ordered set $S \subseteqq J$. S is called a lower (resp. upper) section of J if for all $x, y \in J$ we have $y \in S$, $x \leqq y$ (resp. $x \geqq y$) implies $x \in S$.

Lemma 4. *Suppose A, B are disjoint subsets of $\mathscr{R}$ and $\varepsilon > 0$, then after the elementary steps of $E_\varepsilon(A, B)$ had been performed in an arbitrary order, we have:*

if S is a lower section of $\mathrm{Cont}(A \cup B)$ *and* $|S| \leqq |A|$ *then* $|S - \mathrm{Cont}(A)| \leqq \varepsilon |S|$, *and the corresponding assertion holds for upper sections.*

Definition 4.1. If i is a positive integer, then an *i-parallel step* will be a set of disjoint elementary steps of at most i elements. Suppose Z is a sequence of i-parallel steps for some i and F is a position, then $Z(F)$ will denote the position that we get after the elements of Z had been performed in the given order. Suppose that $H_1, \ldots, H_j$ are sequences of i_1-parallel steps, ..., i_j-parallel steps. The r-th element of H_s will be denoted by $H_s(r)$. $\bigcup_{s=1}^{j} H_s$ will denote the sequence whose r-th term is $\bigcup_{s=1}^{j} H_s(r)$. If the elementary steps of the different $H_s(r)$'s for any fixed r are disjoint (that is no register occurs in the elementaiy steps of both $H_{s_1}(r)$ and $H_{s_2}(r)$ if $s_1 \neq s_2$) then $\bigcup_{s=1}^{j} H_s$ is a sequence of $\left(\sum_{s=1}^{j} i_s\right)$-parallel steps.

Definition 4.2. Suppose C is a chain, $\varepsilon > 0$, then for $i = 0, 1$ we define $\mathrm{imp}_i(C, \varepsilon)$ as $\mathrm{imp}_i(C, \varepsilon) = \bigcup \{E_\varepsilon(C(s), C(t)) | s, t$ are consecutive elements of $\mathrm{Dom}(C)$, $s < t$ and the last element of s is $i\}$. $\mathrm{IMP}_i(C, \varepsilon)$ will be a fixed sequence of parallel steps so that every elementary step of $\mathrm{imp}_i(C, \varepsilon)$ is contained in some parallel step and no other elementary steps occur in any member of the sequence. We may suppose that $\mathrm{IMP}_i(C, \varepsilon)$ is given in an explicit form and its length is $k(\varepsilon, 1)$. Let $\mathrm{IMP}(C, \varepsilon)$ be the concatenation of $\mathrm{IMP}_0(C, \varepsilon)$ and $\mathrm{IMP}_1(C, \varepsilon)$. $\mathrm{IMP}^i(C, \varepsilon)$ will be a sequence of parallel steps consisting of i copies of $\mathrm{IMP}(C, \varepsilon)$. If $C_1, \ldots, C_j$ are disjoint chains then $\bigcup_j \mathrm{IMP}^i(C_j, \varepsilon)$ is a sequence of $2jik(\varepsilon, 1) = \sum_{s=1}^{j} ik(\varepsilon, 1) \cdot 2$ parallel steps.

Definition 4.3. Suppose that C is a chain and $0 < q < 1$. Then $\mathrm{CH3}(C, q)$ is a chain with the following properties:

(4.1) $\mathrm{Dom}(\mathrm{CH3}(C, q)) = \mathrm{Dom}(C)$.

(4.2) $(\mathrm{CH3}(C, q))(t)$ consists of the first $[1/2|(\mathrm{CH2}(C, q))(t)|]$ elements of $(\mathrm{CH2}(C, q))(t)$.

$\mathrm{CH4}(C, q)$ is a chain defined by

$$(\mathrm{CH4}(C, q))(t) = (\mathrm{CH2}(C, q))(t) - (\mathrm{CH3}(C, q))(t).$$

Definition 4.4. Suppose that C is a chain $0 < q < 1$, $\varepsilon > 0$. For any $t \in \mathrm{Dom}(C)$ let

$$\bar{I}_t^1(C, q, \varepsilon) = E_\varepsilon(\mathrm{CH3}(C, q)(t), \mathrm{CH1}(C, q)(t))$$

$$\bar{I}_t^2(C, q, \varepsilon) = E_\varepsilon(\mathrm{CH1}(C, q)(t), \mathrm{CH4}(C, q)(t)).$$

The elementary steps of $\bar{I}_t^j(C, q, \varepsilon)$ can be performed in $k\left(\varepsilon, \frac{1-q}{2q}\right)$ parallel steps if $N(C) \geqq 4/q$. In this let $I_t^j(C, q, \varepsilon)$ be a sequence of parallel steps of length at most $k\left(\varepsilon, \frac{1-q}{2q}\right)$ whose elements contain the elementary steps of $\bar{I}_t^j(C, q, \varepsilon)$

and no other elementary stεps. Let $I_t(C, q, \varepsilon)$ be the concatenation of $I_t^1(C, q, \varepsilon)$ and $I_t^2(C, q, \varepsilon)$. Finally let

$$I(C, q, \varepsilon) = \bigcup_{t \in \mathrm{Dom}(C)} I_t(C, q, \varepsilon).$$

The following Lemma which is an immediate consequence of Lemma 4 shows the effect of $I(C, q, \varepsilon)$.

Lemma 5. *Suppose C is a chain, $0<q<1$, $\varepsilon>0$, $t \in \mathrm{Dom}(C)$ and S is a lower or upper section of $C(t)$. If*

$$|S| < \tfrac{1}{2}(|C(t)| - 4[\tfrac{1}{4}q|C(t)|]),$$

then after $I(C, q, \varepsilon)$ had been performed we have

$$|S \cap \mathrm{Cont}(\mathrm{CH1}(C, q)(t))| \leqq \varepsilon |S|.$$

Now we define P^α the sequence of parallel steps of the α-th cycle. We define P^α only for α's with $2^{-\alpha-1}n > C_2$. (S^α is defined for these α's.) The sequence P^α will be the concatenation of the sequences P_1^α, P_2^α and P_3^α.

Let $P_1^\alpha = \bigcup_{0 \leqq i \leqq \alpha} I(S^{\alpha, i}, g, \varepsilon_1)$. We will prove later that $N(S^{\alpha, i}) = 0$ or $N(S^{\alpha, i}) \geqq \dfrac{4}{1-g}$, therefore we may suppose that the length of P_1^α is at most $k\left(\varepsilon_1, \dfrac{g}{2(1-g)}\right)$.

$$P_2^\alpha = \mathrm{IMP}^{d_1}(\mathrm{D}^\alpha, \varepsilon_1)$$

$$P_3^\alpha = \bigcup_{0 \leqq i \leqq \alpha} \mathrm{IMP}^{d_1}(S^{\alpha+1, i}, \varepsilon_1).$$

The content of the register R after P^α had been performed will be denoted by $F^{\alpha+1}(R)$. $F^0(R)$ is the original content of the register R. $F_1^\alpha(R)$ (resp. $F_2^\alpha(R)$) will denote the content of the register R after P_1^α (resp. P_2^α) had been performed.

Let P' be the concatenation of $P^0, P^1, \ldots, P^{\alpha'}$ where α' is the greatest integer with $2^{-\alpha'-1}n > c_2$.

We will prove later that after P' had been performed the elements of L are almost "ordered" in the following sense:

Lemma 6. *There exist constants u_1, u_2, u_3 such that if $\alpha' - u_1 \leqq i \leqq \alpha'$ then $N(S^{\alpha' i}) \leqq u_2$ and otherwise $N(S^{\alpha, i}) = 0$, moreover if for all $t \in T$ $s'(t)$ denotes the number $2^{-l(t)}|\{t' < t \,|\, l(t') = l(t)\}|$, then for all $t_1, t_2 \in T$ $s'(t_1) - s'(t_2) > u_3 2^{-\alpha'}$ and $x \in \mathrm{Cont}_F \alpha'(S^{\alpha'}(t_1))$, $y \in \mathrm{Cont}_F \alpha'((S^{\alpha'} t_2))$ implies $x > y$, (here we allow $l(t_1) \neq l(t_2)$).*

Lemma 6 implies that there exists a sequence of parallel steps P'' with constant length, so that after P' and then P'' had been performed the elements of L are in a known order. As an exercise we leave the proof of this fact to the reader. Thus we completed the definition of our algorithm.

3. The use of the expander graph

In this section we prove Lemma 6 and other assertions having already been accepted in the last section without their proofs.

Proof of Lemma 4. Suppose that our assertion is not true. Then $|S\cap \mathrm{Cont}_G(B)| > \varepsilon|S|$ where G is the position after $E_\varepsilon(A, B)$ had been performed. Let $X=\{R\in B | G(R)\in S\}$ and $Y\subseteqq A$ the set of neighbours of the elements of X. The definition of $E_\varepsilon(A, B)$ implies that

(6.1) The contents of the registers in A are decreasing, the contants of the registers in B are increasing (not necessarily strictly) in every elementary step of $E_\varepsilon(A, B)$.

(6.2) For all $R\in X$ the content of the register R is an element of S throughout the whole algorithm.

(6.3) For all $R\in Y$ the content of the register R is an element of S at the end of the algorithm (i.e. $G(R)\in S$).

(6.1) and (6.2) are immediate consequences of the definition. By (6.2), if $R\in Y$ the content of Y is in S after the elementary step corresponding to the edge between R and an element of X had been performed. Therefore (6.1) implies (6.3). Thus we have $\mathrm{Cont}_G(X)\cup\mathrm{Cont}_G(Y)\subseteqq S$. On the other hand $\mathrm{Cont}_G(X)\cap \cap\mathrm{Cont}_G(Y)=0$ and since $G_\varepsilon(A, B)$ is a $\langle k(\varepsilon, |A|/|B|), \varepsilon\rangle$ expander graph

$$|\mathrm{Cont}_G(X)|+|\mathrm{Cont}_G(Y)| > \varepsilon|S|+(1-\varepsilon)\frac{1}{\varepsilon}\varepsilon|S| = |S|,$$

a contradiction.

4. Basic definitions

Definition 6.1. Suppose that C is a chain $x\in L$ and F is a position. Then let

$$p_C^E(x) = |\cup C|^{-1}|\{y\in \mathrm{Cont}_F(C) | y \leqq x\}|.$$

For any $t\in T$ let

$$s(t) = 2^{-l(t)}|\{t' < t | l(t') = l(t)\}|+2^{-l(t)-1}.$$

If C, D are chains, F is a position $t\in \mathrm{Dom}\,(C)$ and μ is a real number then let

$$G_D^E(t, \mu, C) = \{x\in L | \exists t'\in \mathrm{Dom}(C) t' \geqq t,\ x\in \mathrm{Cont}_F(C(t'))$$

$$\text{and}\quad s(t)-p_D^F(x) > \mu+\tfrac{1}{2}|C|^{-1}\}.$$

$$H_D^F(t, \mu, C) = \{x\in L | \exists t'\in \mathrm{Dom}(C) t' \leqq t,\ x\in \mathrm{Cont}_F(C(t'))$$

$$\text{and}\quad p_D^E(x)-s(t) > \mu+\tfrac{1}{2}|C|^{-1}\}.$$

Let us define the relation $Q_a^F(C, D, q, M)$; where C, D are chains F is a position a, q, M are real numbers $0<q<1$. $M>0, a>0$; as follows:

$Q_a^F(C, D, q, M)$ iff for all $t\in \mathrm{Dom}\,(C)$ and $\lambda\geqq a$ we have

$$|G_D^F(t, |C|^{-1}2^\lambda, C)| \leqq M\cdot q^\lambda \quad\text{and}\quad |H_D^F(t, |C|^{-1}2^\lambda, C)| \leqq M\cdot q^\lambda.$$

If D is a chain with $\bigcup D=\mathcal{R}$ then we use the following notations: $p(x)=p_D^F(x)$ for all $x\in L$. (In this case $p_D^F(x)$ clearly does not depend on F.)

$$G^F(t,\mu,C)=G_D^F(t,\mu,C)$$

$$H^F(t,\mu,C)=H_D^F(t,\mu,C)$$

$$Q_a^F(C,q,\mu)=Q_a^F(C,D,q,M).$$

Lemma 7. *Suppose that $2^{-\alpha-1}n>c_2$. Then S^α is defined and for all $x\in L$ there exists exactly one $t\in T$ with $x\in\mathrm{Cont}\,(S^\alpha(t))$. Moreover $S^{\alpha,i}$ is a chain for all $0\leqq i\leqq\alpha$ and there exists a constant q_2 such that for all $0\leqq i\leqq\alpha$ the following conditions are satisfied.*

(i) *$S^{\alpha,i}$ is a chain and $N(S^{\alpha,i})\leqq q_1^{\alpha-i}2^{-\alpha}n$,*
(ii) *if $q_1^{\alpha-1}2^{\alpha-1}n<c_1$ then $N(S^{\alpha,i})=0$ otherwise $N(S^{\alpha,i})\geqq q_1^{\alpha-1}2^{-\alpha-1}n$,*
(iii) *$Q_1^{F^\alpha}(S^{\alpha,i},q_2,q_1^{\alpha-i}2^{-\alpha}n)$.*

First we prove that Lemma 6 follows from Lemma 7. The definition of α', (i) and (ii) clearly implies the existence of u_1 and u_2 with the required properties.

Now suppose that $t\in T$ with $\alpha'-u_1\leqq l(t)\leqq\alpha'$. Let us apply (iii) with $\alpha=\alpha'$ and $i=l(t)$; we get

$$|G^{F^{\alpha'}}(t,2^{-l(t)}2^\lambda,S^{\alpha',i})|\leqq q_1^{\alpha'-i}2^{-\alpha'}nq_2^\lambda \tag{7.1}$$

for all $\lambda\geqq 1$.

Let $\lambda_0\geqq 1$ with $q_1^{\alpha'-i}2^{-\alpha'}n\,q_2^{\lambda_0}<1$. (7.1) implies that $G^{F^{\alpha'}}(t,2^{-i}2^\lambda,S^{\alpha',i})=\emptyset$, that is for all $z\in\mathrm{Cont}_F\,\alpha'(S^{\alpha'}(t))$ we have

$$s(t)-p(z)\leqq 2^{-i}2^{\lambda_0}+2^{-i-1}.$$

Similarly if we use H instead of G we get $-(s(t)-p(z))\leqq 2^{-i}2^{\lambda_0}+2^{-i-1}$. Thus if $u_3>2(2^{u_1}2^{\lambda_1}+2^{u_i-1})$ then $s'(t_1)-s'(t_2)>u_32^{-\alpha'}$ implies that $p(x)>p(y)$ that is $x>y$. ▮

5. The properties of $N(S^{\alpha,i})$

We prove Lemma 7 by induction on α. Suppose that the assertions of the Lemma hold for some fixed α and $2^{-(\alpha+1)-1}n>c_2$. Since $S^{\alpha,i}$ is a chain for all $0\leqq i\leqq\alpha_i C_1^i$, C_2^i are defined and clearly they are pairwise disjoint chains. As we mentioned after the definition of D^α and $S^{\alpha,k}$ the chaine $\pi_1C_1^i,\pi_2C_2^i$ are always defined and therefore $S^{\alpha+1,k}$ is also defined for $k_0<k\leqq\alpha+1$ it is a chain and for different k's the corresponding chains are disjoint.

We have to show that $\pi_1(C_2^{k_0-1}\cup\pi_1C_2^{k_0-2})$ is defined if $k_0\geqq 2$. (The case $k_0=0$ is trivial, for $k_0=1$ we can prove by the same method that $\pi_1C_2^{k_0-1}$ is defined.) Obviously it is sufficient to show that

$$2|N(C_2^{k_0-2})\quad\text{and} \tag{7.1}$$

$$2|N(C_2^{k_0-1}\cup\pi_1C_2^{k_0-2}). \tag{7.2}$$

If $l<k_0-2$ that is $q_1^{\alpha+1-(i+2)}2^{-\alpha-2}n<c_1$ then

$$q_1^{\alpha-i}2^{-\alpha-1}n=2q_1\cdot q_1^{\alpha+1-(i+2)}2^{-\alpha-2}n<2q_1c_1<c_1$$

and therefore according to the inductive hypothesis

$$N(S^{\alpha,i}) = \emptyset. \tag{7.3}$$

By the inductive assumption $\mathscr{R} = \bigcup_{0\leqq i\leqq\alpha} (\bigcup S^{\alpha,i})$ and hence by (7.3)

$$\mathscr{R} = \bigcup_{k_0<i\leqq\alpha+1} (\bigcup S^{\alpha+1,i}) \cup (\bigcup K) \cup (\bigcup C_2^{k_0-1}) \cup (\bigcup C_2^{k_0-2})$$

where K is the union of the first four terms of (2.9) and it is a chain. Since the chains of this formula are pairwise disjoint we have

$$n = |\mathscr{R}| = \sum_{k_0<i\leqq\alpha+1} 2^i N(S^{\alpha+1,i}) + 2^{k_0} N(K) +$$

$$+ 2^{k_0-1} N(C_2^{k_0-1}) + 2^{k_0-2} N(C_2^{k_0-2}).$$

n is a power of $2, n\geqq 4$, $k_0\geqq 2$, therefore $2|N(C_2^{k_0-2})$ and $2|N(C_2^{k_0-1}) + 1/2\,N(C_2^{k_0-2})$ which implies (7.1) and (7.2).

Now we prove that (i) and (ii) hold for all $0\leqq i\leqq\alpha$ by induction on α.

For $\alpha=0$, $i=0$, $N(S^{0,0})=n$ implies (i) and (ii). Suppose that our assertion is true for α and we prove it for $\alpha+1$.

By the definition of CH

$$N(C_1^i) = 4[(\tfrac{1}{4})g \cdot N(S^{\alpha,i})] \tag{7.4}$$

$$N(C_2^i) = N(S^{\alpha,i}) - 4[(\tfrac{1}{4})g N(S^{\alpha,i})] \tag{7.5}$$

therefore

$$N(D^\alpha) = 2[\tfrac{1}{4} g N(S^{\alpha,\alpha})] + [\tfrac{1}{4} g N(S^{\alpha,\alpha-1})]$$

(for $\alpha=0$ the second term is omitted).

The definition of $W(D^\alpha, k)$ and Lemma 2 imply together that for all $k_0\leqq k<\alpha$

$$q_1^{\alpha+1-k} 2^{-\alpha-2} n \leqq N\big(W(D^\alpha, k)\big) \leqq q_1^{\alpha+1-k} 2^{-\alpha-2} n + 2. \tag{7.6}$$

We may estimate the other terms of (2.8) and (2.9) using (7.4) and (7.5) and the inductive hypothezis, the definition of π_i and $1-g \ll q_1$, $1 \ll c_1$.

$$N\big(\pi_{-1}(C_2^{k+1})\big) \leqq 2\big(N(S^{\alpha,k+1}) - 4(\tfrac{1}{4} g N(S^{\alpha,k+1}) - 1)\big) \leqq$$

$$\leqq 2(1-g) N(S^{\alpha,k+1}) + 8 \leqq 2(1-g)\, q_1^{\alpha-k-1} 2^{-\alpha} n + 8 \leqq$$

$$\leqq \frac{1}{20} q_1^{\alpha+1-k} 2^{-\alpha-2} n + \frac{1}{20} c_1 \leqq \frac{1}{10} q_1^{\alpha+1-k} 2^{-\alpha-2} n +$$

$$+ \frac{1}{20} q_1^{\alpha+1-k} 2^{-\alpha-2} n \leqq \frac{1}{20} q_1^{\alpha+1-k} 2^{-\alpha-2} n.$$

$$N(\pi_2 C_1^{k-2}) \leqq \tfrac{1}{4} 4[\tfrac{1}{4} g N(S^{\alpha,k-2})] \leqq \tfrac{1}{4} N(S^{\alpha,k-2}) \leqq$$

$$\leqq \tfrac{1}{4} q_1^{\alpha-k+2} 2^{-\alpha} n \leqq \tfrac{1}{4} q_1^{\alpha+1-k} 2^{-\alpha-1} n$$

Therefore for $k_0<k\leqq\alpha$ we have

$$N(S^{\alpha+1,k}) \leqq q_1^{\alpha+1-k} 2^{-\alpha-1} n.$$

For $k=k_0$ the remaining two terms can be estimated as follows:

$$N(C_2^{k_0}) \leqq (1-g)N(S^{\alpha,k_0}) \leqq (1-g)\,q_1^{\alpha-k_0}2^{-\alpha}n \leqq$$
$$\leqq \tfrac{1}{10}\,q_1^{\alpha+1-k_0}2^{-\alpha-1}n.$$
$$N\big(\pi_1(C_2^{k_0-1})\cup\pi_1 C_2^{k_0-2}\big) \leqq \tfrac{1}{2}\big((1-g)N(S^{\alpha,k_0-1})+$$
$$+\tfrac{1}{2}(1-g)N(S^{\alpha,k_0-2})\big) \leqq \tfrac{1}{10}\,q_1^{\alpha+1-k_0}2^{-\alpha-1}n$$

that is

$$N(S^{\alpha+1,k_0}) \leqq q_1^{\alpha+1-k_0}2^{-\alpha-1}n.$$

Since $S^{\alpha,k}(t)=0$ for all $k<k_0$, $l(t)=k$ we proved (i) for $0\leqq k\leqq\alpha$.

(ii) is an immediate consequence of (7.6) and the definition of $S^{\alpha,k}$ for $0\leqq k\leqq\alpha$. $|\bigcup S^{\alpha+1,\alpha+1}|\leqq n$ and $|S^{\alpha+1,\alpha+1}|=2^{\alpha+1}$ implies (i) for $i=\alpha+1$, and in this case (ii) is a consequence of

$$\Big|\bigcup_{0\leqq i\leqq\alpha+1}(\bigcup S^{\alpha+1,i})\Big| = n \quad \text{and}$$
$$\Big|\bigcup_{0\leqq i<\alpha+1}(\bigcup S^{\alpha+1,i})\Big| \leqq \sum_{0\leqq i\leqq\alpha} q_1^{\alpha+1-i}2^{-\alpha}2^i n \leqq \tfrac{1}{2}n.$$

6. The relation Q and the operation IMP

The assertions contained in the following Lemmas are consequences of the inductive hypothesis.

Lemma 8. *For all* $0\leqq i\leqq\alpha$ *we have*

$$Q_1^{F_1^\alpha}(C_1^i,\, q_2,\, q_2^3 q_1^{\alpha-i}2^{-\alpha}n) \tag{8.1}$$

$$Q_1^{F_1^\alpha}(C_2^i,\, q_2,\, q_1^{\alpha-i}2^{-\alpha}n) \tag{8.2}$$

$$Q_2^{F_1^\alpha}(\pi_1 C_1^i,\, q_2,\, q_2^2 q_1^{\alpha-i}2^{-\alpha}n) \tag{8.3}$$

$$Q_3^{F_1^\alpha}(\pi_2 C_1^i,\, q_2,\, q_2 q_1^{\alpha-i}2^{-\alpha}n) \tag{8.4}$$

$$Q_1^{F_1^\alpha}(\pi_{-1} C_2^i,\, q_2,\, q_2 q_1^{\alpha-i}2^{-\alpha}n). \tag{8.5}$$

Proof 8.1. We may suppose that $N(S^{\alpha,i})\neq 0$. Let $\lambda\geqq 1$. We have to prove that

$$|G^{F_1^\alpha}(t,\, 2^{-i}2^\lambda,\, C_1^i)| \leqq q_2^3 q_1^{\alpha-i}2^{-\alpha}n q_2^\lambda$$

for all $l(t)=i$. ($|H^{F_1^\alpha}\ldots|\leqq\ldots$ can be proved analogously).

$$G^{F_1^\alpha}(t,\, 2^{-i}2^\lambda,\, C_1^i) = \bigcup_{t'\geqq t}\big\{x\in \operatorname{Cont}_{F_1^\alpha}(C_1^i(t'))\big| \tag{8.6}$$
$$\big|s(t)-p(x) > 2^{-i}2^\lambda+2^{-i-1}\big\}.$$

According to the inductive hypothesis $Q_1^{F^\alpha}(S^{\alpha,i}, q_1, q_1^{\alpha-i}2^{-\alpha}n)$, hence for all $t\in T$, $\lambda\geqq 1$, $l(t)=l(t')=i$ we have

$$\text{(8.7)}\qquad \sum_{t'\geqq t}\left|\left\{x\in \mathrm{Cont}_{F^\alpha}(S^{\alpha,i}(t'))\,\middle|\,s(t)-p(x)>2^{-i}2^{\lambda}+2^{-\alpha-1}\right\}\right| \leqq$$
$$\leqq q_1^{\alpha-i}2^{-\alpha}nq^{\lambda}.$$

Let us denote by $M_1(t')$ the set in (8.6) corresponding to t' and by $M_2(t')$ the set defined in the corresponding term of (8.7). Clearly $M_2(t')$ is a lower section in $S^{\alpha,i}(t')$. (8.7), $|N(S^{\alpha,i})|\geqq q_1^{\alpha-i}2^{-\alpha-1}n$, $q_2\ll 1-g$ and Lemma 5 implies that

$$|M_1(t')| = \left|M_2(t')\cap \mathrm{Cont}_{F_1^\alpha}(C_1^i(t'))\right| \leqq \varepsilon_1|M_1(t')|.$$

Thus by $\varepsilon_1\ll q_2$ (8.6) follows from (8.7). (8.2) is a trivial consequence of $Q_1^{F^\alpha}(S^{\alpha,i}, q_2, q_1^{\alpha-i}2^{-\alpha}n)$. (8.3) and (8.4) easily follow from (8.1) and (8.5) from (8.2). ▮

Lemma 8′. *Suppose C is a chain, F is a position and $Q_j^F(C, q, M)$ for some $j, q, M, \varepsilon>0$ and $F'=\mathrm{IMP}\,(C, \varepsilon)(F)$, then $Q_j^{F'}(C, q, M)$ holds as well.*

Proof. Let $t\in \mathrm{Dom}\,(C)$, μ a real number, then according to the definition of $\mathrm{IMP}\,(C, \varepsilon)$ we have $|G^F(t, \mu, C)|\geqq|G^{F'}(t, \mu, C)|$ and $|H^F(t, \mu, C)|\geqq|H'(t, \mu, C)|$, which implies our assertion. ▮

Definition 8.1. Suppose that $A\subseteqq L$ and $A=\{a_0, \dots, a_m\}$ where $i_1<i_2$ implies $a_{i_1}<a_{i_2}$ and let β be a positive real number. Then let

$$A^{-\beta} = \{a_{[\beta]}, a_{[\beta]+1}, \dots, a_{m-[\beta]}\}.$$

If G is a position C is a chain $t_1, t_2\in \mathrm{Dom}\,(C)$, $t_1<t_2$ then let us denote by $R_G^B(t_1, t_2)$ the following statement: *for all* $x\in\overline{\mathrm{Cont}_G(C(t_1))}^{\beta}$, $y\in\overline{\mathrm{Cont}_G(C(t_2))}^{\beta}$ *we have* $x<y$.

Lemma 9. *For all $\varepsilon>0, j\geqq 1$ there exists a $b_0>0$ such that if C is a chain, F is a position $0<q<\frac{1}{4}$, $M<2N(C)$, $b>b_0$, $0<\delta\ll\varepsilon$, $F'=(\mathrm{IMP}^b\,(C, \delta))(F)$ and $Q_j^F(C, q, M)$ then for all $t_1, t_2\in \mathrm{Dom}\,(C), t_1<t_2$ implies $R_{F'}^{\varepsilon N(C)}(t_1, t_2)$.*

The following definitions and lemmas are necessary for the proof of Lemma 9.

Definition 9.1. Suppose that G is a position $A\subseteqq L$ and $P\subseteqq \mathrm{Dom}\,(C)\times \mathrm{Dom}\,(C)$. Then let

$$X_{A,P}^G = \{\langle x_1, x_2\rangle | x_1, x_2\in A \quad \text{and} \quad \exists\langle r_1, r_2\rangle\in P,\quad r_1 < r_2$$
$$\text{and}\quad x_i\in \mathrm{Cont}_G(C(r_i))\ \ i = 1, 2 \quad\text{and}\quad x_1 > x_2\}$$

If $P=\mathrm{Dom}\,(C)\times \mathrm{Dom}\,(C)$ then we will write X_A^G instead of $X_{A,P}^G$.

Lemma 10. *Suppose G is a position, E is an elementary step included in $\mathrm{IMP}\,(C, \delta)$, $G'=E(G)$, $A\subseteqq L$. Then $|X_A^G|\geqq|X_A^{G'}|$.*

Proof. If $G'=G$ our assertion is trivial. Suppose $G'\neq G$. Since E is included in $\mathrm{IMP}\,(C, \delta)$, there are consecutive

$$t_1, t_2\in \mathrm{Dom}(C),\quad t_1 < t_2,\quad R_1\in C(t_1),\quad R_2\in C(t_2)$$

such that $G'(R_1)=G(R_2)$, $G'(R_2)=G(R_1)$, $G'(R_1)<G'(R_2)$ and $G'(R)=G(R)$ for all $R\neq R_1$, $R\neq R_2$. If we count the pairs in $X_A^G, X_A^{G'}$ containing $G'(R_1)$ or $G'(R_2)$ we get the required assertion. ▮

Lemma 11. *Suppose* t_1, t_2 *are consecutive elements of* Dom(C), G *is a position,* $G'=\mathrm{IMP}\,(C, \delta)(G)$, $A\subseteq L$, $P=\{t_1, t_2\}$. *Then*

$$|X_A^G|-|X_A^{G'}| \geqq |X_{A,P}^G|-\delta^2(N(C))^2-2\delta N(C).$$

Proof. First we prove the following assertion. If the last element t_1 is i, $G''=\mathrm{IMP}_i(C, \delta)(G)$, $G'''=\mathrm{IMP}_{1-i}(C, \delta)(G)$ and $P=\{t_1, t_2\}$ then we have

$$(11.1)\qquad |X_{A,P}^G|-|X_{A,P}^{G''}| \geqq |X_{A,P}^G|-\delta^2(N(C))^2-2\delta N(C)$$

$$(11.2)\qquad |X_{A,P}^{G'''}| \geqq |X_{A,P}^G| \quad\text{and}$$

$$(11.3)\qquad |X_A^G|-|X_A^{G''}| \geqq |X_{A,P}^G|-|X_{A,P}^{G''}|.$$

To prove (11.1) we have to show that $|X_{A,P}^{G''}|\leqq\delta^2(N(C))^2+2\delta N(C)$. This inequality easily follows from Lemma 4.

(11.2) is a consequence of the fact that for any $a\in C(t_1)$, $b\in C(t_2)$: $G'''(a)\geqq G(a)$ and $G'''(b)\leqq G(b)$.

In order to prove (11.3) let us write Dom$(C)\times$Dom(C) in the form $P\cup Q\cup Y\cup Z$ where $Y=(V\times\{t_1, t_2\})\cup(\{t_1, t_2\}\times V)$. Here $V=\{t\in\mathrm{Dom}\,(C)|t<t_1\}$, $Z=(W\times\{t_1, t_2\})\cup(\{t_1, t_2\}\times W)$ where $W=\{t\in\mathrm{Dom}\,(C)|t>t_2\}$, $Q=(\mathrm{Dom}\,(C)-\{t_1, t_2\})\times(\mathrm{Dom}\,(C)-\{t_1, t_2\})$.

By the definition of IMP_i, $|X_{A,V}^G|=|X_{A,V}^{G''}|$ and $|X_{A,W}^G|=|X_{A,W}^{G''}|$ and therefore

$$|X_A^G|-|X_A^{G''}| = |X_{A,P}^G|-|X_{A,P}^{G''}|+|X_{A,Q}^G|-|X_{A,Q}^{G''}|.$$

We can prove the inequality $|X_{A,Q}^G|-|X_{A,Q}^{G''}|\geqq 0$ using the same argument as in the proof of Lemma 10 so we have (11.3).

Now we prove the Lemma. If the last element of t_1 is 0 then $G'=\mathrm{IMP}_1\times(C, \delta)(G'')$ where $G''=\mathrm{IMP}_0(C, \delta)(G)$ so (11.1), (11.3) and Lemma 10 implies the required inequality.

If the last element of t_1 is 1 then $G'=\mathrm{IMP}_1(C, \delta)(G''')$ where $G'''=\mathrm{IMP}_0\times(C, \delta)(G)$ hence Lemma 10, (11.3), (11.1) and (11.2) implies our assertion. ▮

Lemma 12. (*a*) *Suppose* C *is a chain* G *is a position* $\beta>0$, $t_1, t_2\in\mathrm{Dom}\,(C)$, $t_1<t_2$ *and* $\neg R_G^\beta(t_1, t_2)$. *Then there are consecutive* $t_1', t_2'\in\mathrm{Dom}\,(C)$ *with* $t_1\leqq t_1'<t_2'\leqq t_2$ *and* $\neg R_G^\beta(t_1', t_2')$.

(*b*) *Suppose* $t_1, t_2\in\mathrm{Dom}\,(C)$, $t_1<t_2$ *and* $|X_{A,\{\langle t_1, t_2\rangle\}}^G|>\lambda(N(C))^2$ *for some* $\lambda>0$, $A\subseteq L$. *Then there exist consecutive* $t_1', t_2'\in\mathrm{Dom}\,(C)$, $t_1'<t_2'$ *with* $|X_{A,\{\langle t_1', t_2'\rangle\}}^G|>\frac{1}{4}\lambda^2(N(C))^2$.

Proof. (*a*) Let t_1' be a maximal element of Dom(C) with the following properties: $R_G^\beta(t_1, t_1')$, $t_1\leqq t_1'<t_2$. If t_2' is the element of Dom(C) which covers t_1' then $\neg R_G^\beta(t_1', t_2')$.

(*b*) $|X_{A,\{\langle t_1, t_2\rangle\}}^G|>\lambda(N(C))^2$ implies that $\neg R^{\lambda/2N(C)}(t_1, t_2)$. Applying (*a*) we have $\neg R_G^{\lambda/2N(C)}(t_1', t_2')$ for some consecutive t_1', t_2', $t_1\leqq t_1'<t_2'\leqq t_2$, and hence $|X_{A,\{\langle t_1', t_2'\rangle\}}^G|\geqq\lambda^2/4N(C)^2$. ▮

Proof of Lemma 9. Suppose that there exist $t_1, t_2 \in \mathrm{Dom}(C)$, $t_1 < t_2$ with $\neg R_{F'}^{\varepsilon N(C)}(t_1, t_2)$. According to Lemma 12 (a) we may suppose that t_1, t_2 are consecutive elements of $\mathrm{Dom}(C)$. $h_s(\varepsilon, j)$, $s=1, 2, \dots$ will denote sufficiently large positive constants depending only on ε and j. Let

$$A = \{x \in L | s(t_1) - 2^{h_1(\varepsilon, j) - l(t_1)} \leqq p(x) \leqq s(t_2) + 2^{h_1(\varepsilon, j) - l(t_2)}\}.$$

Lemma 10 implies that if $F^k = (\mathrm{IMP}^k(C, \delta))(F)(F^0 = F)$, then $|X_A^{F^k}|$ is a monotone decreasing function in k. $Q_j^F(C, q, M)$ and Lemma 8′ implies that $\left||X_{L,P}^{F^k}| - |X_{A,P}^{F^k}|\right| \leqq \frac{\varepsilon^2}{2}(N(C))^2$ where $P = \{\langle t_1, t_2 \rangle\}$. $|X_{A,P}^{F^k}| \leqq |X_A^{F^k}|$ so it is sufficient to prove that there exists a b_0 (depending only on ε and j) with the following property: $k > b_0$ implies $|X_A^{F^k}| < \varepsilon^2/_2(N(C))^2$.

We will prove the following stronger assertion: for all k

(12.1) if $|X_A^{F^k}| > \varepsilon^2(N(C))^2$ then $|X_A^{F^k}| - |X_A^{F^{k+1}}| > \frac{1}{h_2(\varepsilon, j)}(N(C))^2$,

(12.2) $$|X_A^{F^0}| < h_3(\varepsilon, j)(N(C))^2.$$

(12.2) is a consequence of $Q_j^F(C, q, M)$ and the definition of A. Indeed,

$$|X_A^{F^0}| \leqq |A|^2 \leqq \Big(\sum_{t \in \mathrm{Dom}(C)} \big|\{x | x \in \mathrm{Cont}_F(C(t)) \text{ and } x \in A\}\big|\Big)^2$$

(12.3) $$\leqq 2^{h_4(\varepsilon, j)} N(C) + \sum_{t \in H} \big|\{x \in A | x \in \mathrm{Cont}_F(C(t)\}\big|)^2,$$

where $H = \{t \| s(t) - s(t_1)| \geqq 2^{h_5(\varepsilon, j)} 2^{-l(t_1)}\}$. $Q_j^F(C, q, M)$, $M \leqq 2N(C)$, $q < \frac{1}{4}$ and the definitions of A and H imply that the second term of (12.3) is less than $2Mq^j < N(C)$ that is

$$|X_A^{F^0}| \leqq 2^{h_6(\varepsilon, j)}(N(C))^2.$$

Now suppose that $|X_A^{F^k}| > \varepsilon^2/_2(N(C))^2$. Lemma 8′ implies that $Q_j^{F^k}(C, q, M)$. According to the definition of A there is a $h_g(\varepsilon, j)$ so that if $\gamma > h_g(\varepsilon, j)$ and

$$W(\gamma) = \{t \| s(t) - s(t_1)| \leqq 2^{\gamma - l(t_1)},\ l(t) = l(t_1)\}$$

then $\Big|\bigcup_{t \notin W(\gamma)} A \cap \mathrm{Cont}_{F^k}(C(t))\Big| < N(C)$, and so $|A| < h_{10}(\varepsilon, j) N(C)$. Therefore there is a $h_{11}(\varepsilon, j)$ so that if $\gamma > h_{11}(\varepsilon, j)$ then

$$\Big|\bigcup_{t \notin W(\gamma)} A \cap \mathrm{Cont}_{F^k}(C(t))\Big| < \frac{1}{|A|}\frac{\varepsilon^2}{4} N(C)^2.$$

Hence if $|X_A^{F^k}| > \varepsilon^2/_2(N(C))^2$ then

$$|X_{A, W(\gamma) \times W(\gamma)}^{F^k}| > \frac{\varepsilon^2}{4} N(C)^2,$$

and therefore there exist $r_1, r_2 \in W(\gamma)$ with

$$|X_{A, \{\langle r_1, r_2 \rangle\}}^{F^k}| > \frac{1}{h_7(\varepsilon, j)} N(C)^2.$$

According to Lemma 12 (b) there exist consecutive r_1', r_2' with

$$|X^{F^k}_{A,\{\langle r_1', r_2'\rangle\}}| > \frac{1}{h_8(\varepsilon, j)}(N(C))^2,$$

and therefore Lemma 11 implies the conclusion of (12.1). ▌

Corollary 9. *For all* $j \geqq 1, 0<q<\frac{1}{4}\ \exists b_0, \delta_0>0$ *such that, for all* $b>b_0, 0<\delta<\delta_0$ *if* C *is a chain,* F *is a position,* $\frac{1}{2}N(C) \leqq M < 2N(C)$, $Q_j^F(C, q, M)$, $F'= =(\mathrm{IMP}^b(C, \delta))(F)$ *and* $|p(x)-p_C^{F'}(x)|<\frac{1}{2}|C|^{-1}$ *for all* $x \in \mathrm{Cont}_F(C)$, *then we have* $Q_1^{F'}(C, q, M)$.

Proof. First we prove the following assertion: For any $\gamma>0$ if b is sufficiently large and $\delta>0$ is sufficiently small and $t \in \mathrm{Dom}\,(C)$ then

$$\text{(C.1)} \qquad \left|\{x \in \mathrm{Cont}_{F'}(C(t)) \big| |p(x)-s(t)| > 2|C|^{-1}\}\right| < \gamma N(C)$$

Let $1>\eta>0$. We claim that there exists a $\beta_0>0$ (depending on η, j, q) such that for all $0<\beta<\beta_0$ we have: $x \in \overline{\mathrm{Cont}_{F'}(C(t))}^\beta$ implies that

$$\text{(C.2)} \qquad \left|\{y > x \big| \exists t' < t,\ y \in \mathrm{Cont}_{F'}(t)\}\right| < \eta N(C)$$

Indeed, $Q_j^{F'}(C, q, M)$ implies that

$$\left|\{y > x \big| \exists t' \colon s(t') < s(t)-h_1|C|^{-1},\ y \in \mathrm{Cont}_{F'}(C(t))\}\right| < \frac{\eta}{2} N(C),$$

where $h_1>0$ may depend on η, j, q. Applying Lemma 9 with a sufficiently small ε we get

$$\left|\{y > x \big| \exists t' \colon s(t)-h_1|C|^{-1} \leqq s(t') < s(t),\ y \in \mathrm{Cont}_{F'}(C(t))\}\right| < \frac{\eta}{2} N(C),$$

which implies (C.2).

Now we prove (C.1). According to (C.2) if $x \in \overline{\mathrm{Cont}_{F'}(C(t)}^\beta$, then

$$p_C^{F'}(x) \geqq 2^{-i}(N(C))^{-1}(-\eta N(C) + \sum_{t'<t} N(C)) \geqq s(t)-|C|^{-1}.$$

Similarly, we get $p_C^{F'}(x) \leqq s(t)+|C|^{-1}$, so $|p_C^{F'}(x)-p(x)|<\frac{1}{2}|C|^{-1}$ implies (C.1). Suppose now that $1 \leqq \lambda \leqq j$, and F' satisfies (C.1) with $\gamma \ll q^j$. $G^{F'}(t, |C|^{-1}2^\lambda, M)= =\bigcup_{t' \geqq t} M(t')$, where

$$M(t') = \{x \in \mathrm{Cont}_{F'}(C(t')) \big| s(t)-p(x) > |C|^{-1}(2^\lambda+\tfrac{1}{2})\}$$

$Q_j^F(C, q, M)$ implies that $\sum_{s(t')>s(t)+h_2|C|^{-1}} |M(t')| \leqq \frac{1}{4}q^jM$, where h_2 is sufficiently large compared to j, and according to (C.1)

$$\sum_{s(t) \leqq s(t') \leqq s(t)+h_2|C|^{-1}} |M(t')| \leqq \tfrac{1}{4}q^jN(C) \leqq \tfrac{1}{2}q^jM,$$

so we have $|G^{F'}(t, |C|^{-1}2^\lambda, M)| \leqq q^j M \leqq q^\lambda M$. ▌

7. The proof of Lemma 7 (iii)

Lemma 13. *For all* $x \in L$, $|p(x) - p^{F_2^\alpha}_{D^\alpha}(x)| < \frac{1}{100} 2^{-\alpha-1}$.

Proof. Clearly,

$$p(x) = \frac{1}{n}\Big(|\cup D^\alpha| p^{F_2^\alpha}_{D^\alpha}(x) + |\cup C_2^\alpha| p^{F_2^\alpha}_{C_2^\alpha}(x)$$

$$+ |\cup C_2^{\alpha-1}| p^{F_2^\alpha}_{C_2^{\alpha-1}}(x) + \sum_{0 \leqq i < \alpha - 1} |\cup S^{\alpha,i}| p^{F_2^\alpha}_{S^{\alpha,i}}(x)\Big).$$

$p^{F^\alpha}_{S^{\alpha,i}}(x) = |\cup S^{\alpha,i}|^{-1} M(x)$, where $M(x) = \{y \in \mathrm{Cont}_{F^\alpha}(S^{\alpha,i}) | p(y) \leqq p(x)\}$. Here $M(x) = M_1(x) \cup M_2(x)$, where

$$M_1(x) = \big\{y \in M(x) | \exists t \in \mathrm{Dom}(S^{\alpha,i})\colon s(t) \leqq p(x) + 3 \cdot 2^{-i},\ y \in \mathrm{Cont}_{F^\alpha}\big(S^{\alpha,i}(t)\big)\big\},$$

$$M_2(x) = \big\{y \in M(x) | \exists t \in \mathrm{Dom}(S^{\alpha,i})\colon s(t) > p(x) + 3 \cdot 2^{-i},\ y \in \mathrm{Cont}_{F^\alpha}\big(S^{\alpha,i}(t)\big)\big\}.$$

$Q_1^{F^\alpha}(S^{\alpha,i}, q_2, q_1^{\alpha-i} 2^{-\alpha} n)$, $q_2 < \frac{1}{6}$, and Lemma 7 (ii) implies that $|M_2(x)| \leqq N(S^{\alpha,i})$, that is

$$\begin{aligned} p^{F^\alpha}_{S^{\alpha,i}}(x) &\leqq |\cup S^{\alpha,i}|^{-1}\big(M_1(x) + N(S^{\alpha,i})\big) \\ &\leqq \big(2^i N(S^{\alpha,i})\big)^{-1}\big(N(S^{\alpha,i}) + \Sigma\{N(S^{\alpha,i}) | s(t) \leqq p(x) + 3 \cdot 2^{-i}\}\big) \\ &\leqq p(x) + 5 \cdot 2^{-i}. \end{aligned}$$

Similarly, using that

$$1 - p^{F^\alpha}_{S^{\alpha,i}}(x) = |\cup S^{\alpha,i}|^{-1} |\{z \in \mathrm{Cont}_{F^\alpha}(S^{\alpha,i}) | p(z) > p(x)\}|,$$

we get $p^{F_2^\alpha}_{S^{\alpha,i}}(x) = p^{F^\alpha}_{S^{\alpha,i}}(x) \geqq p(x) + 5 \cdot 2^{-i}$, so we have $p^{F_2^\alpha}_{S^{\alpha,i}}(x) = p(x) + R_i(x)$, where $|R_i(x)| < 10 \cdot 2^{-i}$, $p^{F_2^\alpha}_{C_2^\alpha}(x) = p^{F_1^\alpha}_{C_2^\alpha}$ and $Q_1^{F_1^{\alpha-j}}(C_2^i, q_2, q_1^{\alpha-j-1} 2^{-\alpha} n)$. Therefore, by the same argument as above we get that $p^{F_2^\alpha}_{C_2^\alpha}(x) = p(x) + R'_j(x)$, where $|R'_j(x)| \leqq 10 \cdot 2^{-\alpha+j}$.

Hence

$$p(x) = \frac{1}{n}\Big(|\cup D^\alpha| p^{F_2^\alpha}_{D^\alpha}(x) + \sum_{j=0,1} |\cup C_2^{\alpha-j}|\big(p(x) + R'_j(x)\big)$$

$$+ \sum_{0 \leqq i < \alpha - 1} \big(p(x) + R_i(x)\big) |\cup S^{\alpha,i}|,$$

that is,

$$\frac{1}{n} |\cup D^\alpha| p(x) = \frac{1}{n} |\cup D^\alpha| p^{F_2^\alpha}_{D^\alpha}(x)$$

$$+ (1-g)\big(R'_0(x) + R'_1(x)\big) + \sum_{0 \leqq i < \alpha - 1} q_1^{\alpha-i} R_i(x)$$

and so $p(x) = p^{F_2^\alpha}_{D^\alpha}(x) + R(x)$, where

$$|R(x)| \leqq (1 + q_1)\big((1-g) 10 \cdot 2^{-\alpha} + q_1 2^{-\alpha}\big) < \frac{1}{100} 2^{-\alpha-1}. \quad ∎$$

Lemma 14. $Q_1^{F_2^\alpha}(D^\alpha, q_2, 2^{-\alpha-1}n)$ *and* $Q_1^{F^{\alpha+1}}(S^{\alpha+1,\alpha+1}, q_2, 2^{-\alpha-1}n)$.

Proof. The first assertion implies the second since $S^{\alpha+1,\alpha+1}(t)\subseteqq D^\alpha(t)$ for all $t\in\mathrm{Dom}\,(D^\alpha)$. The definition of D^α, (8.3) and (8.4) imply $Q_3^{F_1^\alpha}(D^\alpha, q_2, 2q_2 2^{-\alpha}n)$, and so $Q_3^{F_1^\alpha}(D^\alpha, q_2, 2^{-\alpha-1}n)$.

$d_1\gg\dfrac{1}{q_2}$, $\varepsilon_1\ll q_2$, therefore Corollary 9 and Lemma 13 imply

$$Q_1^{F_2^\alpha}(D_\alpha, q_2, 2^{-\alpha-1}n). \quad \blacksquare$$

Lemma 15. *For all* $0\leqq i\leqq\alpha$

$$Q_1^{F^{\alpha+1}}(S^{\alpha+1,i}, q_2, q_1^{\alpha+1-i}2^{-\alpha-1}n). \tag{15.1}$$

Proof. If $i<k_0$, then $N(S^{\alpha+1,i})=0$, hence (15.1) trivially holds in this case. Suppose $k_0<i\leqq\alpha$. By (2.8)

$$S^{\alpha+1,i}=W(D^\alpha, i)\cup\pi_{-1}C_2^{i+1}\cup\pi_2C_1^{i-2}. \tag{15.2}$$

$W(D^\alpha, i)$ is a chain, and for all t with $l(t)=i$ we have

$$|W(D^\alpha, i)(t)\subseteqq\bigcup_{\substack{t'\prec t\\ l(t')=\alpha+1}} D^\alpha(t')$$

Therefore, for all $\lambda\geqq1$, $l(t)=i$,

$$G^{F_2^\alpha}(t, |W|^{-1}2^\lambda, W)\subseteqq\bigcup_{\substack{t'\prec t\\ l(t')=\alpha+1}} G^{F_2^\alpha}(t', |W|^{-1}2^\lambda-\tfrac{1}{2}|W|^{-1}+2^{-\alpha-1}, D^\alpha),$$

where $t_0=\langle t, 0, \dots, 0\rangle$, $l(t_0)=\alpha+1$, and hence $s(t)=s(t_0)+1/2\,|W|^{-1}-2^{-\alpha-1}$. Therefore, for $\lambda\geqq2$,

$$G^{F_2^\alpha}(t, |W|^{-1}2^\lambda, W|)\subseteqq G^{F_2^\alpha}(t_0, |W|^{-1}2^{\lambda-\frac{1}{2}}, D^\alpha)$$

$$=G^{F_2^\alpha}(t_0, |D^\alpha|^{-1}2^{\lambda+\alpha-i+\frac{1}{2}}, D^\alpha).$$

By Lemma 14 and $q_2\ll q_1$, we have

$$|G^{F_2^\alpha}(t, |W|^{-1}2^\lambda, W)|\leqq 2^{-\alpha-1}nq_2^{\lambda+\alpha-i+\frac{1}{2}}$$

$$\leqq 2^{-\alpha-1}nq_1^{\alpha-i}q_2^\lambda\left(\frac{q_2}{q_1}\right)^{\alpha-i}\leqq 2^{-\alpha-1}nq_1^{\alpha+1-i}q_2^\lambda,$$

and similar inequality holds with H. So we have

$$Q_2^{F_2^\alpha}(W(D^\alpha, i), q_2, 2^{-\alpha-1}nq_1^{\alpha+1-i}). \tag{15.3}$$

According to (8.5) and the definition of P_α^2

$$Q_1^{F_2^\alpha}(\pi_{-1}C_2^{i-1}, q_2, q_2q_1^{\alpha-i-1}2^{-\alpha}n) \tag{15.4}$$

holds. By (8.4),

$$Q_3^{F_2^\alpha}(\pi_2C_1^{i-2}, q_2, q_2q_1^{\alpha-i+2}2^{-\alpha}n). \tag{15.5}$$

(15.3), (15.4) and (15.5) imply that

$$Q_3^{F_2^\alpha}(S^{\alpha+1,i},\, q_2,\, q_1^{\alpha+1-i}2^{-\alpha}n). \tag{15.6}$$

To prove $Q_1^{F^{\alpha+1}}(\dots)$ we may use the same argument as in the proof of Lemma 14. Let x be an arbitrary element of L

$$|p(x)-p_{S^{\alpha+1,i}}^{F_2^\alpha}(x)| \leqq$$

$$\left|p(x)-\frac{1}{N(S^{\alpha+1,i})}\right| P_{W(D^\alpha),i}(x)\cup P_{\pi^{-1}C_2^{i+1}}(x)\cup P_{\pi_2 C_1^{i-2}}(x), \tag{15.7}$$

where $P_C(x)=\{y\in \operatorname{Cont}_{F_2^\alpha}(C)\,|\,y\leqq x\}$,

$$P_{W(D^\alpha),i}(x) = \bigcup_{l(t)=\alpha+1} \{y\in \operatorname{Cont}(D^\alpha(t)\cap W(D^\alpha, i))\}$$

and $D^\alpha(t)\cap[\cup(W(D^\alpha, i))]$ is a chain (as a function of t), therefore Lemma 13, 14 and $q_1\ll 1$ imply

$$|P_{w(D^\alpha,i)}(x)| = p(x)|\cup W(D^\alpha, i)|+M_1(x)$$

where $M_1(x)\leqq 1/10\, 2^{-\alpha-1}n$. (15.4) and (15.5) imply

$$|P_{\pi_{-1}C_2^{i+1}}(x)| = p(x)|\cup \pi_{-1}C_2^{i+1}|+M_2(x)$$

$$|P_{\pi_2 C_2^{i-2}}(x)| = p(x)|\cup \pi_2 C_2^{i-1}|+M_3(x),$$

where $M_2(x)<1/10\, N(\pi_{-1}C_2^{i+1})$, $M_3(x)=1/10\, N(\pi_2 C_2^{i-1})$. Thus we have

$$|p(x)-p_{S^{\alpha+1,i}}^{F_2^\alpha}(x)| \leqq$$

$$(N(S^{\alpha+1,i}))^{-1}(M_1(x)+M_2(x)+M_3(x)) \leqq \tfrac{1}{3}2^{-i}.$$

Hence Corollary 9 implies that $Q_1^{F^{\alpha-1}}(S^{\alpha+1,i},\, q_2,\, q_1^{\alpha+1-i}2^{-\alpha}n)$. ▮

References

[1] O. Gabber and Z. Galil, Explicit constructions of linear size superconcentrators, *Proc. 20st Annual Symposium on Foundations of Computer Science* (1979).

[2] D. E. Knuth, *The art of computer programming Volume* 3, *Sorting and Searching*, Addison—Wesley (1973).

[3] G. A. Margulis, Effective construction of expander graphs (in Russian), *Probl. Pered. Inf.* **9** (4), 71—80.

M. Ajtai, J. Komlós, E. Szemerédi

Mathematical Institute of the
Hungarian Academy of Sciences
Budapest, Hungary, H-1053