SIAM J. COMPUT.
Vol. 13, No. 1, February 1984


0097-5397/84/1301-0011 $01.25/0



# LIMITATIONS ON EXPLICIT CONSTRUCTIONS OF EXPANDING GRAPHS*

MARIA KLAWE†

**Abstract.** Expanding graphs are the basic building blocks in constructions of many types of graphs with special connectivity properties which arise in a variety of applications including switching networks, sorting networks and establishing time-space trade-offs for numerous computational problems. Only one explicit method of constructing arbitrarily large expanding graphs with a linear number of edges is known (Margulis [13], Gabber and Galil [8]), but the number of edges used is much greater than the number known to be sufficient via probabilistic arguments. In this paper we show that various other constructions which have been proposed to obtain expanding graphs, including one-dimensional analogues of the Gabber–Galil construction and some pseudorandom constructions, cannot ever yield expanding graphs.

**Key words.** network, expander, superconcentrator

**1. Introduction.** For any bipartite graph, whose two vertex sets are called inputs and outputs, if $X$ is a subset of inputs we will use $\Gamma X$ to denote the neighborhood of $X$, i.e. the set of outputs which are adjacent to some input in $X$. Moreover, we will denote the cardinality of any set $A$ by $|A|$. For the purposes of this paper, we will call a bipartite graph with $n$ inputs and $n$ outputs an expanding graph, if there exist positive constants $\alpha$ and $\delta$, such that for any subset $X$ of inputs with $|X| \leqq \alpha n$ we have $|\Gamma X| \geqq (1+\delta)|X|$. (There are many slight variations in the definitions of expanding graphs in the applications we will mention, but the basic idea is always that every set in some class of subsets of inputs is guaranteed to expand by some fixed amount.)

It is obvious that expanding graphs exist since the complete bipartite graph is an expanding graph for any $\alpha$ and $\delta$ with $(1+\delta)\alpha \leqq 1$. What is more surprising is that there are families of expanding graphs with only a linear number of edges. In fact, for any $\alpha$ and $\delta$ such that $(1+\delta)\alpha < 1$, there is some constant $k$ such that for every $n$ there is a bipartite graph with $n$ inputs, $n$ outputs and at most $kn$ edges, which is an expanding graph with respect to $\alpha$ and $\delta$. Pinsker [19] gave a fairly simple probabilistic proof of this for a particular $\alpha$, $\delta$ and $k$ in 1973; similar arguments have been used in subsequent papers to prove this fact for other combinations of $\alpha$ and $\delta$, and it not hard to see that these probabilistic arguments succeed in general.

Over the past ten years expanding graphs with a linear number of edges have been used as building blocks in constructions of graphs appearing in a broad spectrum of applications. As motivation for the importance of obtaining good explicit constructions, and consequently for the significance of the results in this paper, we give a brief survey of these applications.

The study of the complexity of graphs with special connectivity properties originated in switching theory, motivated by problems of designing networks able to connect many disjoint sets of users, while only using a small number of switches. An example of this type of graph is a superconcentrator, which is an acyclic directed graph with $n$ inputs and $n$ outputs such that given any pair of subsets $A$ and $B$ of the same size, of inputs and outputs respectively, there exists a set of disjoint paths joining the inputs in $A$ to the outputs in $B$. Some other examples are concentrators, nonblocking connectors and generalized connectors (see [6], [21] for more details). There is a large body of work searching for optimal constructions of these graphs (Pinsker [19],

* Received by the editors July 14, 1982, and in revised form February 8, 1983.
† Computer Science Department, IBM Research, San Jose, California 95193.

Bassalygo and Pinsker [3], Cantor [5], Ofman [15], Masson and Jordan [14], Pippenger [20], [21], Chung [6]). So far all optimal explicit constructions depend on expanding graphs of some sort.

Superconcentrators have also proved to be useful in theoretical computer science. By showing that the computation graphs of straight line programs for problems such as polynomial multiplication, the Fourier transform and matrix inversion must be superconcentrators, it has been possible to establish nonlinear lower time bounds and time-space trade-offs for these problems assuming certain models of computation (Valiant [25], Abelson [1], Ja'Ja' [9], Tompa [24]).

These space-time trade-offs are obtained via a game known as pebbling which is played on acyclic directed graphs and mimics the storage of temporary results during a straight-line computation. In considering the problem of pebbling an arbitrary acyclic directed graph, expanding graphs have been used in several instances to construct graphs which are (in some sense) hardest to pebble, hence establishing lower bounds in space-time trade-offs (Lengauer and Tarjan [12], Paul and Tarjan [17], Paul, Tarjan and Celoni [18], Pippenger [22]).

Expanding graphs have also been used to construct sparse graphs with dense long paths (Erdos, Graham and Szemeredi [7]). Interest in sparse graphs with dense long paths stems from studying the complexity of Boolean functions, and more recently from problems of designing fault-tolerant microelectronic chips. Paul and Reischuk strengthened this result by constructing (still using expanding graphs) sparse graphs of bounded in-degree with dense long paths, which is of interest since computation graphs have bounded in-degree.

Perhaps the most practical applications of expanding graphs occur in the two most recent results. Ajtai, Komlos and Szemeredi [2] have announced the construction of an oblivious sorting network using $O(n \log n)$ comparators, and having depth $O(\log n)$. Again, expanding graphs form the basic components, and of course, the explicit construction of the sorting network depends on the explicit construction of expanding graphs. The problem of constructing such a sorting network has been open for twenty years [4], which perhaps illustrates best the unexpected power of expanding graphs. Finally, expanding graphs have been used by Karp and Pippenger [10] to design an algorithm which can be applied to virtually all the well-known Monte-Carlo algorithms to reduce the number of uses of a randomization resource (i.e. coin-flips or calls to a random number generator) while still maintaining polynomial running time.

In several of the applications mentioned above the usefulness of expanding graphs depends on the existence of an explicit construction of expanding graphs with a linear number of edges. In 1973 Margulis [13] gave an explicit construction, but, although he was able to prove that the constant $\delta$ was greater than zero, he was not able to bound $\delta$ strictly away from zero. In 1979, after slightly modifying Margulis's construction, Gabber and Galil [8] were able to obtain a positive lower bound for $\delta$, and thus obtained the first usable explicit construction, which we now present for future reference. Let $Z_m$ denote the integers mod $m$, and let $f_i$ for $i = 0, 1, \cdots, 6$ be the functions on $Z_m \times Z_m$ defined by

$$f_0(s, t) = (s, t),$$

$$f_1(s, t) = (s, 2s + t) \bmod m,$$

$$f_2(s, t) = (s, 2s + t + 1) \bmod m,$$

$$f_3(s, t) = (s, 2s + t + 2) \bmod m,$$

$$f_4(s,t) = (s+2t, t) \bmod m,$$
$$f_5(s,t) = (s+2t+1, t) \bmod m,$$
$$f_6(s,t) = (s+2t+2, t) \bmod m.$$

The graph $G(m)$ is defined as the bipartite graph with inputs $\{x(s,t)\colon 1 \leqq s,\ t \leqq m\}$ and outputs $\{y(s,t)\colon 1 \leqq s,\ t \leqq m\}$ such that $x(s,t)$ is adjacent to $y(f_i(s,t))$ for $i = 0, 1, \cdots, 6$.

There are two aspects of this construction which make it less than completely satisfactory. The first, and most important, is that the combination of $\alpha$ and $\delta$ for which Gabber and Galil are able to prove that $G(m)$ expands is significantly worse than those combinations which can be proved to exist by probabilistic methods. As a result, for example, the best construction of superconcentrators using their expanding graphs has $261.5n$ edges, which compares unfavorably with the fact that it is known (via probabilistic methods) that superconcentrators exist with $(38.5n + O(\log n))$ edges (Chung [6]). The second is that the proof that their construction succeeds is fairly sophisticated mathematically. One might hope for a more elementary and intuitively satisfying proof. Consequently the search has continued for explicit constructions of expanding graphs with a linear number of edges.

The most obvious approach is to look for some variant of the Gabber–Galil construction which would either yield a better combination of $\alpha$, $\delta$ and $k$, or at least yield a simpler proof of expansion. Another possibility which has occurred to many people, is that since it can be shown that for any $\alpha$ and $\delta$ there exists $k$ such that almost all random bipartite graphs with $kn$ edges expand with respect to $\alpha$ and $\delta$, one could use pseudorandom number generators to construct a bipartite graph with $kn$ edges. Then, presumably with high probability, this graph should be an expanding graph with respect to $\alpha$ and $\delta$. We will refer to this type of construction as a pseudorandom construction. Yet another direction has been proposed by Tanner [23]. He observed that if $\lambda_1$ and $\lambda_2$ are the two largest eigenvalues of $MM^T$, where $M$ is the incidence matrix of a regular bipartite graph $G$, then $G$ is an expanding graph with respect to $\alpha$ and $(\lambda_1/(\alpha\lambda_1 + (1-\alpha)\lambda_2)) - 1$. Thus it suffices to construct regular bipartite graphs with a linear number of edges such that the two largest eigenvalues of $MM^T$ are widely separated. Tanner also showed that a class of graphs known as generalized $n$-gons have this property, but unfortunately generalized $n$-gons only exist for finitely many $n$.

The results in this paper show that at least the most obvious examples of the first two above approaches cannot succeed. We will define a class of constructions which both is a natural variant of the Gabber–Galil construction, and includes all the graphs which can be obtained by pseudorandom constructions when linear congruential pseudorandom number generators are used in the following fashion. Given a finite set $\{f_i\}$ of pseudorandom number generators, the edges of the pseudorandom graph are all pairs of the form $(x, f_i(x))$ where $1 \leqq x \leqq n$.

Notice that each $f_i$ in the Gabber–Galil construction is the restriction mod $m$ of a two-dimensional linear function, all of whose coefficients are either 0, 1 or 2. In an analogous manner, for any finite set $F = \{a_i x + b_i\colon 1 \leqq i \leqq k\}$ of one-dimensional linear mappings, we can define a bipartite graph $G(n, F)$ with inputs $\{x(i)\colon 1 \leqq i \leqq n\}$ and outputs $\{y(i)\colon 1 \leqq i \leqq n\}$ such that $x(i)$ is adjacent to $y(j)$ if and only if $j = \lfloor f(i) \rfloor \bmod n$ for some $f$ in $F$. By choosing the coefficients $a_i$ to be integers, it is easy to see that this class includes all graphs which could be obtained by pseudorandom constructions using linear congruential pseudorandom number generators. Suppose $0 < \alpha < 1$ and

let $F$ be a finite family of one-dimensional linear functions with rational coefficients. The main result of this paper is the following.

THEOREM. *There exist functions $N(\alpha, |F|)$ and $\delta(\alpha, F, n)$ such that the limit of $\delta(\alpha, F, n)$ as $n$ goes to infinity is* 0, *and such that for each $n \geqq N(\alpha, |F|)$ there is a subset $X$ of the inputs of $G(n, F)$ with $\alpha n/2 < |X| \leqq \alpha n$ and $|\Gamma X| < (1+\delta(\alpha, F, n))|X|$.*

Since $\lim_{n\to\infty} \delta(\alpha, F, n) = 0$, there is no $\delta > 0$ such that $G(n, F)$ is an expanding graph with respect to $\alpha$ and $\delta$ for all $n$. Moreover, if the coefficients of the functions in $F$ are integers, we can prove a stronger result. Namely that $\delta(\alpha, F, n)$ depends only on $\alpha$, $|F|$ and $n$. This strengthening is particularly important when applying the result to pseudorandom constructions using linear congruential number generators since it means that even if the multipliers are chosen as a function of $n$, expanding graphs cannot be obtained.

The theorem above is proved by explicitly constructing a nonexpanding subset $X$, and establishing a number of its properties. In an earlier version of this paper [11], we proved similar results using an entirely different construction of nonexpanding subsets. There are two ways in which this paper's construction improves upon the previous one. First of all, the old construction did not yield the stronger result for integer coefficients. The second improvement is that in the new construction the size of the nonexpanding subset can be specified fairly precisely, whereas previously the size of the nonexpanding subset was $O(n^{2/3})$ and thus could not be applied to situations where one is only interested, for example, in the expansion of sets of approximately half the inputs. We should, however, point out one aspect in which the old construction may dominate the new one. Let $F$ be the family $\{(p_i/q_i)x + b_i : 1 \leqq i \leqq k\}$. The $\delta$ function in the old construction is $(\sum_{1\leqq i\leqq k} \log p_i + \log q_i)(\sum_{1\leqq i\leqq k} |p_i/q_i| + |b_i|)/\log n$, whereas the $\delta$ function in the new construction (for rationals) is $\sum_{1\leqq i\leqq k} ((3+q_i)/s + (q_i(p_i^2+1))/\tau)$ where

$$s = \lfloor (\log \alpha n / \log\log \alpha n)^{1/(3k+2)} \rfloor \quad \text{and} \quad \tau = \lfloor (s/\alpha)^{(k+1)s^{k+2}} \rfloor.$$

It is not hard to see that for some sets $F$ and choices of $\alpha$ and $n$ the value of the old $\delta$ function is much smaller than the value of the new $\delta$ function, and hence in those cases the old construction would give a stronger nonexpansion result. The new $\delta$ function for integers is $3k/s$, and again in some cases the old $\delta$ function is less than this.

There are two major questions about one-dimensional linear constructions which remain unsettled. The first is whether it is possible to obtain expanding graphs using real coefficients, and the second is whether it is possible to extend the stronger integer result to rational coefficients. Of course a positive answer to the second would also imply a negative answer to the first, since for any fixed $n$ and finite set $F$ of one-dimensional linear mappings with real coefficients there is a set $F'$ with rational coefficients such that $G(n, F) = G(n, F')$. However, as $n$ increases so must the numerators and denominators in the rational coefficients in $F'$, and so the kind of result for rational coefficients given in this paper has no implication for real coefficients.

The next section describes the construction of the nonexpanding subset $X$ and establishes sufficiently many of its properties to prove the result for integer coefficients. In § 3, we continue to explore the properties of $X$, finally achieving the result for rational coefficients. We are also able to apply this construction to shuffle-exchange graphs, thus proving that shuffle-exchange graphs cannot be expanding graphs either.

**2. Integer coefficients.** Given integers $a_i$ and $b_i$ for $1 \leqq i \leqq k$ for each $i$ let us define a mapping $f_i$ on $Z_n$ by $f_i(x) = a_i x + b_i \bmod n$. For sets $A$ and $B$ we use $A \backslash B$ to denote the difference set of elements which are in $A$ but not $B$. This section is devoted to proving the following theorem.

THEOREM 2.1. *For each real number $\alpha$ between 0 and 1 there is a constant $N$ depending only on $\alpha$ and $k$, such that for each $n \geqq N$, there exists a subset $X$ of $Z_n$ with $\alpha n/2 \leqq |X| \leqq \alpha n$, and $|f_i(X)\backslash X| < 3|X|/\lfloor(\log \alpha n/\log\log \alpha n)^{1/(3k+2)}\rfloor$ for $1 \leqq i \leqq k$.*

We begin by introducing some notation and conventions that we will use. For any numbers $x$ and $p$ in $Z_n$, unless otherwise noted we will understand $px$ and $x+p$ to mean $px \bmod n$ and $(x+p) \bmod n$ respectively. The greatest common divisor of $p$ and $x$ is denoted by $(p, x)$, and if $X$ is a subset of $Z_n$ then $p^{-1}X$ is the subset of $Z_n$ defined by $p^{-1}X = \{z : pz \in X\}$. For subsets $X$ and $Y$ we will use $XY$ to denote the product subset, i.e. $XY = \{z : z = xy$ for some $x$ in $X$ and $y$ in $Y\}$. Similarly $\prod_{1 \leqq i \leqq j} X_i$ denotes the product set $X_1X_2 \cdots X_j$. Finally, let $s$ denote $\lfloor(\log \alpha n/\log\log \alpha n)^{1/(3k+2)}\rfloor$, let $\tau$ denote $\lfloor(s/\alpha)^{(k+1)s^{k+2}}\rfloor$, let $\nu = \max\{4k+4, (1/\alpha)^{3k+2}\}$, and let $N = 2^{2^\nu}/\alpha$. For the remainder of this section we will assume that $n$ and $t$ are integers satisfying $n \geqq N$ and $\tau \leqq t \leqq n$. The next lemma states the inequalities involving these numbers which we will require in the remainder of this section.

LEMMA 2.2.

(i) $s/\alpha \geqq s \geqq 2$.

(ii) $\alpha^{3k+2} \log\log \alpha n \geqq 1$.

(iii) $\tau \geqq (2s(s-1)(s/\alpha)^s)/(s-2)$ *for* $s \geqq 3$.

(iv) $\tau \geqq 2s^k(s/\alpha)^{sk}2^{(k+1)s^k}$.

(v) $s^k(s/\alpha)^{sk}\tau^{(k+1)s^k} \leqq (s/\alpha)^{(k+2)s^{3k+2}}$.

(vi) $(s/\alpha)^{(k+2)s^{3k+2}} \leqq \alpha n$.

*Proof.* (i) and (ii) are consequences of our assumption that $n \geqq N$, $k \geqq 1$ and $\alpha < 1$. (iii), (iv) and (v) can be established in a straightforward manner by applying (i) and the inequalities $k \geqq 1$ and $k+1 \leqq s^k$ in a variety of circumstances. Finally (vi) follows from (ii) and the identity $\alpha n = (\log \alpha n)^{(\log \alpha n/\log\log \alpha n)}$. □

We are now ready to describe the basic ideas in our construction. We will construct a set $X$ with the following properties:

*Property* 2.3.1. $\alpha n/2 \leqq |X| \leqq \alpha n$.

*Property* 2.3.2. For each $i$, $|(X+b_i)\backslash X| < |X|/s$.

*Property* 2.3.3. For each $i$ such that $(a_i, n) \leqq s/\alpha$, $|a_iX\backslash X| < 2|X|/s$.

For any subset $X$ of $Z_n$ and $a \in Z_n$ we have $|aX\backslash X| \leqq |aX| \leqq |aZ_n| = n/(a, n)$. Thus Property 2.3.1 also implies the following additional property:

*Property* 2.3.4. If $(a_i, n) > s/\alpha$ then $|a_iX\backslash X| < 2|X|/s$.

Finally $|(a_iX+b_i)\backslash X| \leqq |((a_iX \cap X)+b_i)\backslash X| + |(a_iX\backslash X)+b_i| \leqq |(X+b_i)\backslash X| + |a_iX\backslash X|$, and hence the above properties imply the following property, as desired:

*Property* 2.3.5. For each $i$, $|f_i(X)\backslash X| < 3|X|/s$.

Let $P = \{a_i : (a_i, n) \leqq s/\alpha\}$, and let $Q$ be the subset $\prod_{p \in P}\{1, p, \cdots, p^{s-1}\}$. For each $p$ in $P$ and $0 \leqq i \leqq s-1$, let $Q(p, i)$ be the subset $p^i \prod_{q \in P\backslash\{p\}}\{1, q, \cdots, q^{s-1}\}$. Thus $Q$ is the set of elements of $Z_n$ which can be written as a product of powers of elements of $P$ in which the exponent of any element is at most $s-1$, and $Q(p, i)$ is the subset of elements of $Q$ which can be so expressed with the exponent of $p$ equal to $i$.

Next for each $t$ with $\tau \leqq t \leqq n$ we define another subset $A(t)$ of $Z_n$ by $A(t) = \{\sum_{z \in QB} a(z)z : a$ maps $QB \to \{0, 1, \cdots, t-1\}\}$, where $B = \{1, b_1, \cdots, b_k\}$. Now, finally, we define $X(t)$ as $X(t) = \bigcup_{q \in Q} q^{-1}A(t)$. We will show that $X(t)$ has Properties 2.3.2 and 2.3.3 for $t$ in the range $\tau \leqq t \leqq n$. Moreover we will show that for some $t$ in this range $X(t)$ also satisfies Property 2.3.1.

Before continuing with the proof we will attempt to provide some intuition as to why $X(t)$ has these properties. First of all, in order for any set $X$ to have Property 2.3.2, it is clear that for each $b_i$ it must be true that most of the elements of $X$ can be arranged into long sequences of the form $x, x+b_i, x+2b_i, \cdots$, or in other words,

into long arithmetic progressions with period $b_i$. The set $A(t)$ is constructed so that for each $q$ in $Q$, the set $q^{-1}A(t)$ (and hence also $X(t)$) can be arranged into arithmetic progressions with period $b_i$ and of length at least $t$. This and its consequences are more formally presented in Lemmas 2.6 and 2.7.

Next let us consider why $X(t)$ should satisfy Property 2.3.3. The set $Q$ is constructed so that $|Q(p, 0)|$ is small relative to $|Q|$ for each $p$ in $P$. Moreover for any set $A$ and $i>0$, if $x$ is in $\cup_{q\in Q(p,i)} q^{-1}A$ then $px$ is in $\cup_{q\in Q(p,i-1)} q^{-1}A$. Thus if $|q^{-1}A|\simeq|A|$ for each $q$ in $Q$, one could hope that $(|pX\backslash X|/|X|)\simeq(|Q(p, 0)|/|Q|)$. In general $|q^{-1}A|$ may be much smaller than $|A|$ ($q^{-1}A$ could be empty, for example), but one kind of set $A$ which has $|q^{-1}A|\simeq|A|$ for every $q$ is a long interval, i.e. $\{x, x+1, x+2, \cdots, x+j\}$ for sufficiently large $j$. This is expressed more precisely in Lemma 2.8. Examining the definition of $A(t)$ shows that $A(t)$ has been constructed so that it is the union of intervals of length at least $t$ and so has the desired property. Since the sets $q^{-1}A(t)$ are not disjoint in general, the proof that $|pX\backslash X|$ is small is still quite complicated, and depends heavily on the fact that each set $q^{-1}A(t)$ is also the union of long intervals.

Finally we consider Property 2.3.1. It is obvious that $|X(t)|$ increases with $t$, and that for $t$ large enough ($t=n$ for example) $X(t)$ is all of $Z_n$. What is harder to prove is that $|X(t)|$ increases slowly enough in the appropriate range so that there is some $t$ with $\alpha n/2\leqq|X(t)|\leqq\alpha n$, and it is precisely for this reason that $t$ is chosen to be so much larger than $s$.

We begin the proof by establishing some upper bounds on the size of our sets in terms of $s$, $t$ and $k$.

LEMMA 2.4.

(i) $|Q|\leqq s^k$.

(ii) $|A(t)|\leqq t^{(k+1)s^k}$

(iii) *For each* $q$ in $Q$, $|q^{-1}A(t)|\leqq(s/\alpha)^{sk}|A(t)|$.

(iv) $|X(t)|\leqq s^k(s/\alpha)^{sk}t^{(k+1)s^k}$.

*Proof.* (i) is obvious since $|P|\leqq k$, and (ii) follows directly from (i) since clearly $|A(t)|\leqq t^{|Q||B|}$. For the proof of (iii) note that for any subset $Y$ of $Z_n$ and any $q$ in $Z_n$ we have $|q^{-1}Y|\leqq(q, n)|Y|$. Moreover, it is easy to see that for any $q$ in $Q$ we have $(q, n)\leqq(s/\alpha)^{sk}$, which completes the proof of (iii). Finally (iv) follows in an obvious way from (i), (ii) and (iii). □

COROLLARY 2.5. $|X(\tau)|\leqq\alpha n$.

*Proof.* This follows immediately from inequalities (v) and (vi) of Lemma 2.2 and (iv) of Lemma 2.4. □

In order to prove that $X(t)$ has the properties that we desire we will need the following lemma describing the structure of $X(t)$ in terms of $b$-intervals. If $b\in Z_n$ and $Y$ is a subset of $Z_n$, then we say $Y$ is a $b$-interval of length $m$ if the elements of $Y$ are the elements of an arithmetic progression in $Z_n$ of length $m$ and of period $b$. Note that the actual cardinality of a $b$-interval will be less than its length if its length exceeds $n/(b, n)$, but if $m\leqq n$ then a 1-interval of length $m$ is simply an interval of length $m$ in the usual sense except that it is interpreted mod $n$. A $b$-block of a subset $Y$ is a $b$-interval which is maximal with respect to containment in $Y$.

LEMMA 2.6. *For each* $q$ *in* $Q$, $b$ *in* $B$, *and* $x$ *in* $q^{-1}A(t)$ *there is a* $b$*-interval* $Y$ *of length* $t$ *such that* $z\in Y$ *and* $Y\subset q^{-1}A(t)$.

*Proof.* Let $a$ map $QB\to\{0, 1, \cdots, t-1\}$ such that $qx=\sum_{z\in QB} a(z)z$. Then it is easy to check that the set $Y=\{x+jb: -a(qb)\leqq j\leqq t-1-a(qb)\}$ has the desired properties. □

COROLLARY 2.7. *For each* $b$ *in* $B$ *we have* $|(X(t)+b)\backslash X(t)|\leqq|X(t)|/t$.

*Proof.* Let $X_1, \cdots, X_d$ be the $b$-blocks of $X(t)$. By Lemma 2.6 each $X_i$ is a $b$-interval of length at least $t$, and it is easy to see that this implies that for any $i$ such that $|X_i| < t$ we must have $(X_i + b) \subset X_i$. Consequently $|(X(t)+b)\backslash X(t)| \leqq |\{i: |X_i| \geqq t\}| \leqq |X(t)|/t$ since the $X_i$ are disjoint. □

In proving a similar result about $|pX(t)\backslash X(t)|$ for each $p \in P$, we will use the following observation, whose proof we omit since it is almost trivial.

LEMMA 2.8. *If $Y$ is a 1-interval, then for any $r \in Z_n$ we have* $|r^{-1}Y| \geqq |Y| - ((r, n) - 1)$.

PROPOSITION 2.9. *If $p \in P$ then $|pX(t)\backslash X(t)| < 2|X(t)|/s$.*

*Proof.* This clearly holds for $s = 2$ so suppose $s \geqq 3$. For $0 \leqq i \leqq s-1$ let $D_i = \bigcup_{q \in Q(p,i)} q^{-1}A(t)$, and let $D = D_0 \backslash (\bigcup_{1 \leqq i \leqq s-1} D_i)$. Then it is easy to see that for $i \geqq 1$ we have $pD_i \subset D_{i-1}$, and hence $(pX(t)\backslash X(t)) \subset pD$. Thus it suffices to show that $|D| < 2|X(t)|/s$. Let $Y_1, \cdots, Y_d$ be the 1-blocks of $D$ in increasing order with respect to size, and let $m = \max(0, \max\{i: |Y_i| < (s-2)t/(2s(s-1))\})$. We first show that $\sum_{1 \leqq i \leqq m} |Y_i| < (s-2)|X(t)|/(s(s-1))$. Since every 1-block of $D_0$ has length (and hence cardinality) at least $t$ by Lemma 2.6, if $|Y_i| < (s-2)t/(2s(s-1))$ we must have that $Y_i$ is adjacent to some 1-block of $(\bigcup_{1 \leqq j \leqq s-1} D_j)$ either on the right or on the left. Let us denote this 1-block as $b(Y_i)$. Notice that any particular 1-block of $(\bigcup_{1 \leqq j \leqq s-1} D_j)$ could be $b(Y_i)$ for at most two distinct $i$ since it can border at most one of them on the right and at most one on the left. Thus $\sum_{1 \leqq i \leqq m} |b(Y_i)| \leqq 2|\bigcup_{1 \leqq j \leqq s-1} D_j| \leqq 2|X(t)|$. Finally, since Lemma 2.6 implies that $|b(Y_i)| \geqq t$ for each such $i$, we have $|Y_i| < (s-2)|b(Y_i)|/(2s(s-1))$, which completes this part of the proof.

It now suffices to prove that $\sum_{m < i \leqq d} |Y_i| < |X(t)|/(s-1)$, since $(s-2)/(s(s-1)) + 1/(s-1) = 2/s$. For convenience, if $Z$ is a subset of $Z_n$ and $i$ is a nonnegative integer, we will use $p^{-i}Z$ to denote the subset $(p^i)^{-1}Z$. We first observe that if $0 \leqq i < j \leqq s-1$ then $p^{-i}D \cap p^{-j}D = \varnothing$, since if $x \in p^{-i}D \cap p^{-j}D$ then $p^i x \in D \cap D_{j-i}$, which contradicts the definition of $D$. Combining this with the fact that the $Y_i$ are disjoint, it is easy to see that the sets $p^{-j}Y_i$ are disjoint, and hence $|X(t)| \geqq \sum_{m < i \leqq d} \sum_{0 \leqq j \leqq s-1} |p^{-j}Y_i|$. By Lemma 2.8 $|p^{-j}Y_i| \geqq |Y_i| - (p^j, n) + 1$, and since $(p, n) \leqq s/\alpha$, clearly $(p^j, n) \leqq (s/\alpha)^j$. Combining these observations, and recalling that $s/\alpha \geqq s \geqq 3$, we see that $|X(t)| > \sum_{m < i \leqq d} (s|Y_i| - (s/\alpha)^s)$. Moreover, since $t \geqq \tau$, Lemma 2.2(iii) implies $(s/\alpha)^s \leqq (s-2)t/(2s(s-1)) \leqq |Y_i|$, and hence $|X(t)| > \sum_{m < i \leqq d} (s-1)|Y_i|$, or equivalently $\sum_{m < i \leqq d} |Y_i| < |X(t)|/(s-1)$ as promised. □

The remainder of this section is devoted to showing that for $r = \max\{t: |X(t)| \leqq \alpha n\}$, we have $\alpha n/2 \leqq |X(r)| \leqq \alpha n$. Note that Corollary 2.5 guarantees that $r \geqq \tau$.

PROPOSITION 2.10. $|A(r+1)\backslash A(r)| \leqq \alpha n/(2s^k(s/\alpha)^{sk})$.

*Proof.* Let $C = A(r+1)\backslash A(r)$, and suppose $|C| > \alpha n/(2s^k(s/\alpha)^{sk})$. For each $x$ in $C$ we can choose $a_x$ mapping $QB \to \{0, 1, \cdots, r\}$ such that $x = \sum_{z \in QB} a_x(z)z$. Also, for each such $x$ we define a subset $T(x)$ of $QB$ by $T(x) = \{z: a_x(z) = r\}$. Notice that $T(x) \neq \varnothing$ since otherwise we would have $x \in A(r)$. Finally for each nonempty subset $Z$ of $QB$ we define a subset $g(Z)$ of $C$ as $g(Z) = \{x: T(x) = Z\}$. Now since $|C| > \alpha n/(2s^k(s/\alpha)^{sk})$, there must be some nonempty subset $Z$ of $QB$ with $|g(Z)| > \alpha n/(2s^k(s/\alpha)^{sk}2^{|QB|})$. As $r \geqq \tau$ and $|QB| \leqq (k+1)s^k$, by Lemma 2.2(iv) this implies $|g(Z)| > \alpha n/r$.

For each $i$ with $1 \leqq i \leqq r$ let $y(i)$ be the element $\sum_{z \in Z} iz$. From the definition of $g(Z)$ it is easy to see that for each such $i$ we have $(g(Z) - y(i)) \subset A(r)$. Moreover, we claim that if $1 \leqq i < j \leqq r$ we have $(g(Z) - y(i)) \cap (g(Z) - y(j)) = \varnothing$, since otherwise we would have $g(Z) \cap (g(Z) - y(j) + y(i)) = g(Z) \cap (g(Z) - y(j-i)) \neq \varnothing$; yet $g(Z) \cap (g(Z) - y(j-i)) \subset C \cap A(r) = \varnothing$. Thus $|A(r)| \geqq \sum_{1 \leqq i \leqq r} |g(Z)| = r|g(Z)| > \alpha n$, and

hence $|X(r)| > \alpha n$, which contradicts the definition of $r$. Consequently we must have $|C| \leqq \alpha n/(2s^k(s/\alpha)^{sk})$. □

COROLLARY 2.11. $|X(r)| > \alpha n/2$.

*Proof.* It suffices to show that $|X(r+1)\backslash X(r)| \leqq \alpha n/2$, since by the definition of $r$ we have $|X(r+1)| > \alpha n$. By the same arguments used in the proof of Lemma 2.4(iii) we have $|q^{-1}(A(r+1)\backslash A(r))| \leqq (s/\alpha)^{sk}|(A(r+1)\backslash A(r)|$. Thus $|X(r+1)\backslash X(r)| \leqq |Q|(s/\alpha)^{sk}|A(r+1)\backslash A(r)| \leqq s^k(s/\alpha)^{sk}|A(r+1)\backslash A(r)| \leqq \alpha n/2$ by Proposition 2.10. □

If we take $X = X(r)$, combining Corollaries 2.7 and 2.11 with Proposition 2.9, we see that $X$ satisfies Properties 2.3.1, 2.3.2 and 2.3.3, thus completing the proof of Theorem 2.1.

*Remark* 2.12. It is easy to see that by choosing $s$ and $\tau$ in slightly different ways one can prove slightly different results. For example, by changing $s$ to $\lfloor \alpha(\log \alpha n/\log\log \alpha n)^{1/(3k+2)} \rfloor$, one obtains the following result:

THEOREM 2.13. *For each real number $\alpha$ between 0 and 1 and each $n \geqq 0$ there exists a subset $X$ of $Z_n$ with $\alpha n/2 \leqq |X| \leqq \alpha n$, such that for $1 \leqq i \leqq k$ we have $|f_i(X)\backslash X| < 3|X|/\lfloor \alpha(\log \alpha n \log\log \alpha n)^{1/(3k+2)} \rfloor$.*

Notice that this avoids having to choose $n$ sufficiently large at the expense of weakening the bound on $|f_i(X)\backslash X|$. Of course this theorem is trivially true for any subset $|X|$ when $s \leqq 3$, so really, when one takes Theorem 2.1 into consideration, this theorem is only interesting for $n$ (approximately) in the range defined by the inequality $(3/\alpha)^{3k+2} \leqq \log \alpha n \leqq 2^{(1/\alpha)^{3k+2}}$.

Similarly our choosing $\alpha n/2$ and $\alpha n$ as the limits on the size of $X$ were completely arbitrary. In fact if $0 < \beta < \alpha < 1$, there is a constant $N$ depending on $k$, $\alpha$ and $\beta$, and a function $g(n, \alpha, \beta, k)$ going to infinity as $n$ goes to infinity, such that for each $n \geqq N$ there exists a subset $X$ of $Z_n$ with $\beta n \leqq |X| \leqq \alpha n$ and $|f_i(X)\backslash X| \leqq 3|X|/g(n, \alpha, \beta, k)$.

**3. Rational coefficients.** The special problems, which occur in constructing non-expanding subsets for the case of rational coefficients, are basically caused by the way that the floor function $\lfloor x \rfloor$ interacts with the multiplying and taking inverses mod $n$. Our first goal in this section is to prove a result similar to Proposition 2.9. We wish to show that the subset of elements $x$ of $X(t)$ such that $p^{-1}x$ is not contained in $X(t)$ is small relative to $|X(t)|$ for each $p$ in $P$ with $p \leqq s$. This result will be proved in Proposition 3.2, but first we prove a useful technical lemma.

For any subset $Z$ of $Z_n$ let $\beta(Z)$ denote the number of 1-blocks in $Z$.

LEMMA 3.1. *Let $Z$, $V$, $W$ be subsets of $Z_n$, and let $p, t \in Z_n$ such that $0 < p < t < n$. Moreover, suppose that every 1-block in either $V$ or $W$ has length at least $t$, and that $pZ \subset V \backslash W$. Then there is a subset $h(Z)$ of $V \backslash W$ such that*

(i) $\beta(h(Z)) \leqq \beta(Z) + |h(Z)|/t$,

(ii) $|h(Z)| \geqq (|Z| - 2p\beta(Z))/(1 + (p-1)/t)$, *and*

(iii) $|h(Z)| \leqq |Z|$.

*Proof.* If $D = \{x, x+1, \cdots, y\}$ is a 1-block of $Z$, we will use $p\&D$ to denote the 1-block $\{px, px+1, \cdots, py\}$. Let $K = \cup\{p\&D : D \text{ is a 1-block of } Z\}$, and let $H = K \cap (V \backslash W)$. We first prove that in fact $H = K \cap V$. Clearly it suffices to show that for any 1-block $D$ of $Z$ we have $p\&D \cap (V \backslash W) = p\&D \cap V$. Suppose $z \in p\&D \cap V \cap W$. Since $pD \subset V \backslash W$, $z$ cannot be in $pD$ and hence for some adjacent pair $x, x+1$ in $D$, we have $px < z < p(x+1)$. This shows that the 1-block of $W$ containing $z$ has length at most $p-1$, which contradicts the assumption that every 1-block of $W$ has length at least $t$.

We next prove that $|K \backslash V| \leqq (p-1)(|H|/t + \beta(K))$. Let $Y$ be a 1-block of $K$. From the definition of $K$ and the fact that $pZ \subset V$, it is easy to see that every 1-block

of $Y\backslash V$ has length at most $p-1$. Moreover, since every 1-block of $V$ has length at least $t$ it is easy to see that $\beta(Y\backslash V)$ is at most $|Y\cap V|/t+1$. Combining these we see that $|Y\backslash V|\leqq(p-1)(|Y\cap V|/t+1)$, which yields $|K\backslash V|\leqq(p-1)(|H|/t+\beta(K))$.

To complete the proof that $H$ satisfies (ii), we will first show that $|K|\geqq|Z|-p\beta(K)$. Clearly every element of $pZ$ is a multiple of $p$, and thus from the definition of $K$ we see that every 1-block of $K$ both begins and ends with a multiple of $p$. As at most one out of any $(p,n)$ consecutive elements in 1-block can be a multiple of $p$ (and hence an element of $pZ$), this shows that $|K|\geqq(p,n)(|pZ|-\beta(K))$. Obviously $|pZ|\geqq|Z|/(p,n)$, so $|K|\geqq|Z|-p\beta(K)$ as desired. Finally, we have $|H|=|K|-|K\backslash V|\geqq|Z|-p\beta(K)-(p-1)(\beta(K)+|H|/t)$, yielding $|H|\geqq(|Z|-2p\beta(Z))/(1+(p-1)/t)$ since obviously $\beta(K)\leqq\beta(Z)$.

Let $K'$ be any subset of $K$ with $\beta(K')\leqq\beta(K)$, and let $H'=K'\cap V$. Since every 1-block of $V$ has length at least $t$, for each 1-block $Y'$ of $K'$ we must have $\beta(Y'\cap V)\leqq|Y'\cap V|/t+1$, and hence $\beta(H')\leqq\sum\{|Y'\cap V|t+1\colon Y'$ is a 1-block of $K'\}\leqq\beta(K')+|H'|/t\leqq\beta(Z)+|H'|/t$. If $|H|\leqq|Z|$ we may take $h(Z)$ to be $H$ since the preceding remark shows that $H$ satisfies (i). Otherwise take $h(Z)$ to be $K'\cap V$, where $K'$ is a subset of $K$ with $\beta(K')\leqq\beta(K)$ and $|K'\cap V|=|Z|$. To see that such a set $K'$ must exist note that it is easy to construct a family $\{K(r)\colon 1\leqq r\leqq|K|\}$ of nested subsets of $K$ with $\beta(K(r))\leqq\beta(K)$ and $|K(r)|=r$. Now combining the facts that $|K(|K|)\cap V|>|Z|$ and $|K(r)\cap V|-|K(r-1)\cap V|\leqq 1$ for each $r>1$ shows that $|K(r)\cap V|=|Z|$ for some $r$. □

For each $p\in P$ and $i$ with $0\leqq i\leqq s-1$ let $V(p,i)=\cup_{r\in Q(p,i)}r^{-1}A(t)$, and let $W(p,i)=\cup_{0\leqq j\leqq i}V(p,j)$. For convenience we also adopt the convention that $W(p,-1)=\varnothing$ for any $p$.

PROPOSITION 3.2. *For each p in P such that $p\leqq s$ we have*

$$|V(p,s-1)\backslash W(p,s-2)|\leqq\frac{2|X(t)|}{s}.$$

*Proof.* We assume $s\geqq 3$ since the proposition holds trivially for $s=2$. Let $\xi=(s-2)t/(2s(s-1))$, and let $Z(0)$ be the union of the 1-blocks of $V(p,s-1)\backslash W(p,s-2)$ which have length at least $\xi$. Then by the same argument as used in the proof of Proposition 2.9, we have $|(V(p,s-1)\backslash W(p,s-2))\backslash Z(0)|<(s-2)|X(t)|/(s(s-1))$, and hence it suffices to show that $|Z(0)|<|X(t)|/(s-1)$. Now observe that if $i\geqq 1$ then $p(V(p,i)\backslash W(p,i-1))\subset V(p,i-1)\backslash W(p,i-2)$. Moreover, by Lemma 2.6 every block in either $V(p,i)$ or $W(p,i-1)$ has length at least $t$. Thus by Lemma 3.1 we can recursively define $Z(i)=h(Z(i-1))$ such that $Z(i)\subset V(p,s-i-1)\backslash W(p,s-i-2)$, $\beta(Z(i))\leqq\beta(Z(i-1))+|Z(i)|/t$, and $\gamma(|Z(i)|-2p\beta(Z(i-1)))\leqq|Z(i)|\leqq|Z(i-1)|$ where $\gamma=1/(1+(p-1)/t)$. Since every 1-block in $Z(0)$ has length at least $\xi$, clearly $\beta(Z(0))\leqq|Z(0)|/\xi$. Also obviously $|Z(i)|/t\leqq|Z(0)|/\xi$, and hence by induction one can trivially show that $\beta(Z(i))\leqq 3^i|Z(0)|/\xi$. Using this, again by induction it is easy to show that $|Z(i)|\geqq\gamma^i|Z(0)|-3^ip|Z(0)|/\xi$. Since the sets $V(p,s-i-1)\backslash W(p,s-i-2)$ are disjoint for $0\leqq i\leqq s-1$, the sets $Z(i)$ are disjoint, and hence $|X(t)|\geqq\sum_{0\leqq i\leqq s-1}|Z(i)|\geqq|Z(0)|\sum_{0\leqq i\leqq s-1}(\gamma^i-3^ip/\xi)$. Now $\gamma^i=(1/(1+(p-1)/t))^i$, and it is easy to verify that $(1/(1+(p-1)/t))^i\geqq 1-i(p-1)/t$. This shows that $|X(t)|\geqq|Z(0)|(s-s^2(p-1)/t-3^sp/\xi)$. Finally it can easily be checked that $s^2(p-1)/t+3^sp/\xi<1$ since $t\geqq\tau$, $s\geqq 3$, $s\geqq p$ and $k\geqq 1$. □

Proposition 3.2 yields the following corollary which will be useful for proving the nonexpansion of shuffle-exchange graphs, as well as of $G(n,F)$ when the mappings in $F$ have rational coefficients.

COROLLARY 3.3. *For each $p$ in $P$ such that $p \leqq s$ we have*

$$|\{x \in X(t): \{\lfloor x/p \rfloor + jn/(p,n): 0 \leqq j < (p,n)\} \backslash X(t) \neq \varnothing\}| < \left(\frac{2}{s} + \frac{p}{t}\right)|X(t)|.$$

*Proof.* Let $W$ be the set of elements of $W(p, s-2)$ which are among the first $p$ elements of their 1-block in $W(p, s-2)$. We claim that for each $x$ in $W(p, s-2) \backslash W$ we have $\{\lfloor x/p \rfloor + jn/(p,n): 0 \leqq j < (p,n)\} \subset X(t)$. First note that since $x - p\lfloor x/p \rfloor \leqq p-1$ we have $p\lfloor x/p \rfloor \in W(p, s-2)$ and hence $p^{-1}(p\lfloor x/p \rfloor) \subset X(t)$. However, $p^{-1}(p\lfloor x/p \rfloor) = \{\lfloor x/p \rfloor + jn/(p,n): 0 \leqq j < (p,n)\}$. Thus $|\{x \in X(t): \{\lfloor x/p \rfloor + jn/(p,n): 0 \leqq j < (p,n)\} \backslash X(t) \neq \varnothing\}| \leqq |X(t) \backslash W(p, s-2)| + |W|$. Clearly $X(t) \backslash W(p, s-2) = V(p, s-1) \backslash W(p, s-2)$ so we have $|X(t) \backslash W(p, s-2)| < 2|X(t)|/s$ by Proposition 3.2. Moreover, since every 1-block of $W(p, s-2)$ has size at least $t$, we have $|W| \leqq p|W(p, s-2)|/t \leqq p|X(t)|/t$, which completes the proof. □

Let $X_1 = \{x \in X(t): \lfloor x/q \rfloor$ is not in $X(t)\}$, $X_2 = \{x \in X(t): px$ is not in $X(t)\}$, and $X_3 = \{x \in X(t): \{x, x+1, \cdots, x+p-1\} \backslash X(t) \neq \varnothing\}$. In the following corollary we will use $*$ to distinguish real multiplication from multiplication mod $n$. Thus for $p$ and $x$ in $Z_n$ $p * x$ denotes the product of $p$ and $x$ regarded as real numbers, whereas $px$ denotes the product mod $n$.

COROLLARY 3.4. *If $p, q \in P$ and $q \leqq s$ then* $|(\lfloor p * X(t)/q \rfloor \bmod n) \backslash X(t)| \leqq (2*(q+1)/s + q*(p*p+1)/t)|X(t)|$.

*Proof.* We first show that $|(\lfloor p * X(t)/q \rfloor \bmod n) \backslash X(t)| \leqq |X_1| + q*|X_2| + p*q*|X_3|$. Let $Y = \{x \in X(t): \{\lfloor x/q \rfloor\} \cup \{p\lfloor x/q \rfloor, p\lfloor x/q \rfloor + 1, \cdots, p\lfloor x/q \rfloor + p - 1\} \subset X(t)\}$. It is not hard to see that for any $x$ we have $\lfloor p * x/q \rfloor \bmod n \in \{p\lfloor x/q \rfloor, p\lfloor x/q \rfloor + 1, \cdots, p\lfloor x/q \rfloor + p - 1\}$, and hence we see that $\lfloor p * Y/q \rfloor \bmod n \subset X(t)$. This shows that $|\lfloor p * X(t)/q \rfloor \backslash X(t)| \leqq |X(t) \backslash Y|$. Now clearly $|X(t) \backslash Y| \leqq |X_1| + |\{x: \lfloor x/q \rfloor \in X_2\}| + |\{x: p\lfloor x/q \rfloor \in X_3\}|$, from which it is easy to see that $X|(t) \backslash Y| \leqq |X_1| + q*|X_2| + p*q*|X_3|$.

The proof is completed by giving appropriate upper bounds for $|X_1|$, $|X_2|$ and $|X_3|$. From Corollary 3.3 we have $|X_1| < (2/s + q/t)|X(t)|$, and from the proof of Proposition 2.9 it is easy to see that $|X_2| < (2/s)|X(t)|$. Finally, since every 1-block in $X(t)$ has length at least $t$, one easily concludes that $|X_3| < (p/t)|X(t)|$. □

Combining this corollary with the results of the previous section yields the following theorem.

THEOREM 3.5. *Let $F$ be the family $\{p_i x/q_i + b_i: 1 \leqq i \leqq k\}$ and let $0 < \alpha < 1$. Then there exists a constant $N$ depending only on $\alpha$ and $k$ such that for each $n \geqq N$ there exists a subset $X$ of inputs of $G(n, F)$ with $\alpha n/2 < |X| \leqq \alpha n$ and $|\Gamma X| < (1 + \delta(\alpha, F, n))|X|$, where $\delta(\alpha, F, n)$ is the function $\sum_{1 \leqq i \leqq k} ((3+q_i)/s + (q_i(p_i^2+1))/\tau)$ where*

$$s = \lfloor (\log \alpha n / \log\log \alpha n)^{1/(3k+2)} \rfloor \quad \text{and} \quad \tau = \lfloor (s/\alpha)^{(k+1)s^{k+2}} \rfloor.$$

If $d$ is a divisor of $n$, the perfect $d$-shuffle rearranges the numbers 1 to $n$ into the sequence

$$1, (n/d)+1, \cdots, ((d-1)n/d)+1,$$
$$2, (n/d)+2, \cdots, ((d-1)n/d)+2, \cdots,$$
$$(n/d), (n/d)+(n/d), \cdots, n$$

which corresponds to partitioning the numbers 1 to $n$ into $d$ segments of equal length and performing a perfect shuffle. Suppose $D$ is a subset of the divisors of $n$. If a graph has inputs $x(i)$ and outputs $y(i)$ for $1 \leqq i \leqq n$, we say that it is a $D$-shuffle-exchange graph if $x(i)$ and $y(j)$ are adjacent whenever for some $d$ in $D$ the perfect $d$-shuffle

places $i$ in the $j$th position, or $j$ in the $i$th position. By this definition, the usual shuffle-exchange graph is simply a $\{2\}$-shuffle-exchange graph. It is not hard to see that the $D$-shuffle-exchange graph is a partial subgraph of $G(n, F(D))$ where $F(D)$ is the family $\{dx+b: d \in D, 0 \leqq b \leqq d-1\} \cup \{x/d + jn/d + 1: d \in D, 0 \leqq j \leqq d-1\}$. If we take $P = D$ and $B = \{1\}$, then it is not hard to see from Lemma 2.6 and Corollary 3.3 that, regarding $X(t)$ as a subset of inputs in $G(n, F(D))$, if $d \leqq s$ for each $d$ in $D$ we have $|\Gamma X(t)| < (1 + \sum_{d \in D} (4/s + 2d/\tau))|X(t)| < (1 + 5|D|/s)|X(t)|$ since $d \leqq s$ obviously implies $2d/\tau < 1/s$. This shows that as long as the divisors used are small enough relative to $n$, shuffle exchange graphs cannot be expanding graphs.

**Acknowledgment.** I would like to thank Nick Pippenger for many illuminating discussions.

## REFERENCES

[1] H. ABELSON, *A note on time-space tradeoffs for computing continuous functions*, Inform. Process. Lett., 8 (1979), pp. 215–217.

[2] M. AJTAI, J. KOMLOS AND E. SZEMEREDI, *An $O(n \log n)$ sorting network*, in Proc. 15th Annual ACM Symposium on the Theory of Computing, Association for Computing Machinery, New York, 1983.

[3] L. BASSALYGO AND M. PINSKER, *Complexity of an optimum nonblocking switching network without reconnections*, Problemy Peredachi Informatsii, 9, 1 (1973), pp. 84–87; Problems Inform. Transmission, 9, 1 (1974), pp. 64–66.

[4] R. C. BOSE AND R. J. NELSON, *A sorting problem*, J. Assoc. Comput. Mach., 9 (1962), pp. 282–296.

[5] D. CANTOR, *On nonblocking switching networks*, Networks, 1 (1971), pp. 367–377.

[6] F. R. K. CHUNG, *On concentrators, superconcentrators, and nonblocking networks*, Bell System Tech. J., 58 (1979), pp. 1765–1777.

[7] P. ERDOS, R. L. GRAHAM AND E. SZEMEREDI, *On sparse graphs with dense long paths*, Comput. Math. Appl., 1 (1975), pp. 365–369.

[8] O. GABBER AND Z. GALIL, *Explicit constructions of linear size superconcentrators*, Proc. 20th Annual Symposium on the Foundations of Computer Science, 1979, pp. 364–370.

[9] J. JA'JA', *Time-space tradeoffs for some algebraic problems*, Proc. 12th Annual ACM Symposium on the Theory of Computing, 1980, pp. 339–350.

[10] R. KARP AND N. PIPPENGER, *A time-randomness trade-off*, in preparation.

[11] M. KLAWE, *Nonexistence of one-dimensional expanding graphs*, Proc. 22nd Annual Symposium on the Foundations of Computer Science, Nashville, TN, 1981.

[12] T. LENGAUER AND R. TARJAN, *Asymptotically tight bounds on time-space trade-offs in a pebble game*, J. Assoc. Comput. Mach., 29 (1982), pp. 1087–1130.

[13] G. MARGULIS, *Explicit constructions of concentrators*, Problemy Peredachi Informatsii, 9(4) (1973), pp. 71–80; Problems Inform. Transmission, 10 (1975), pp. 325–332.

[14] G. MASSON AND B. JORDAN JR., *Generalized multi-stage connection networks*, Networks, 2 (1972), pp. 191–209.

[15] JU. P. OFMAN, *A universal automaton*, Trans. Moscow Math. Soc., 14 (1965), pp. 200–215.

[16] W. PAUL AND R. REISCHUK, *On Alternation* II—*a graph theoretic approach to determinism versus nondeterminism*, Acta Inform., 14 (1980), pp. 391–403.

[17] W. PAUL AND R. TARJAN, *Time-space trade-offs in a pebble game*, Acta Inform., 10 (1978), pp. 111–115.

[18] W. PAUL, R. TARJAN AND J. CELONI, *Space bounds for a game on graphs*, Math. Systems Theory, 10 (1979), pp. 239–251.

[19] M. PINSKER, *On the complexity of a concentrator*, in 7th International Teletraffic Conference, Stockholm, June 1973, pp. 318/1–318/4.

[20] N. PIPPENGER, *Superconcentrators*, SIAM J. Comput., 6 (1977), pp. 298–304.

[21] ———, *Generalized connectors*, SIAM J. Comput., 7 (1978), pp. 510–514.

[22] ———, *Pebbling with an auxiliary pushdown*, J. Comput. System Sci., 23 (1981), pp. 151–165.

[23] R. M. TANNER, *Explicit concentrators from generalized N-gons*, SIAM J. Alg. Discr. Meth., 5 (1984), to appear.

[24] M. TOMPA, *Time-space tradeoffs for computing functions, using connectivity properties of their circuits*, J. Comput. System Sci., 20 (1980), pp. 118–132.

[25] L. VALIANT, *Graph theoretic properties in computational complexity*, J. Comput. System Sci., 13 (1976), pp. 278–285.