THEORY OF COMPUTING, Volume 6 (2010), pp. 291–308
www.theoryofcomputing.org

RESEARCH SURVEY

Monotone Expanders: Constructions and Applications

Zeev Dvir* Avi Wigderson*

Received: February 4, 2010; published: December 30, 2010.

Abstract: The main purpose of this work is to formally define monotone expanders and motivate their study with (known and new) connections to other graphs and to several computational and pseudorandomness problems. In particular we explain how monotone expanders of constant degree lead to:

1. constant-degree dimension expanders in finite fields, resolving a question of Barak, Impagliazzo, Shpilka, and Wigderson (2004);
2. $O(1)$-page and $O(1)$-pushdown expanders, resolving a question of Galil, Kannan, and Szemerédi (1986) and leading to tight lower bounds on simulation time for certain Turing Machines.

Recently, Bourgain (2009) gave a rather involved construction of such constant-degree monotone expanders. The first application (1) above follows from a reduction due to Dvir and Shpilka (2007). We sketch Bourgain's construction and describe the reduction.

The new contributions of this paper are simple. First, we explain the observation leading to the second application (2) above, and some of its consequences. Second, we observe that

*Research partially supported by NSF grants CCF-0832797 and DMS-0835373.

ACM Classification: F.1.3, G.2.2

AMS Classification: 68Q15, 68R10

Key words and phrases: expander, zig-zag, k-page graphs, pushdown graphs

 DOI: 10.4086/toc.2010.v006a012

a variant of the Zig-Zag graph product preserves monotonicity, and use it to give a simple alternative construction of monotone expanders, with near-constant (c-times iterated log for any c) degree.

1 Introduction

Expander graphs are families of highly connected sparse graphs. These combinatorial objects have found numerous applications in diverse areas of mathematics and computer science and have drawn an enormous amount of attention (see [14] for a survey). Many of the applications require explicit constructions of such graphs, where "explicit" means graphs that can be constructed by an algorithm that runs in polynomial time in the size of the graph. Some applications require a more restrictive notion of explicitness in which the i-th neighbor of a vertex can be computed in time polylogarithmic in the size of the graph. Such constructions are called "strongly explicit."

It is easy to show that a random sparse graph is an expander, but proving that some explicit graph is an expander is considerably harder. Today there are many known constructions of expander graphs ranging from group theoretic constructions (e. g., [19, 22, 15]) to purely combinatorial ones [26, 2].

The question of whether restricted classes of graphs can be expanders of constant degree has also received attention, and there are many negative examples for natural classes, e. g., planar graphs (and graphs with other excluded minors) [18, 3] and Cayley graphs of Abelian and near-Abelian groups [16, 20]. More relevant to us are the classes of k-page graphs and k-pushdown graphs (which we define later) that arise as computation graphs of Turing machines, for which the expansion question remained open and is key to resolving some complexity questions [12, 27].

The focus of this paper are *monotone* graphs and their expansion properties. Monotone graphs are defined by monotone mappings. Throughout the paper the vertex set of graphs will be $[n]$, the first n integers with their natural ordering. A partial monotone function $f : [n] \to [n]$ satisfies $f(x) > f(y)$ for all pairs $x > y$ for which the function is defined. Such a function defines a 1-monotone graph whose edges are all pairs $(i, f(i))$ for all $i \in \mathrm{Dom}(f)$. Similarly, d monotone partial functions $f_1, \ldots, f_d$ define a d-monotone graph. This graph is the union of the d 1-monotone graphs defined by the functions $f_1, \ldots, f_d$. Note that such graphs have in-degree, as well as out-degree, at most d. The most natural way to think of these graphs is as bipartite directed graphs with n left vertices and n right vertices and edges going from left to right.[1] In this setting a graph is expanding if every set of size $t \le n/2$ of left vertices has at least $(1+\alpha)\cdot t$ neighbors for some constant $\alpha > 0$. Monotonicity (with degree d) is equivalent to saying that the set of edges can be partitioned into d disjoint monotone matchings (that is, in each matching the edges do not cross).

Unlike the question in general graphs, there is no obvious way of even proving the *existence* of d-monotone expanders for small d. Attempting the probabilistic method one is faced with the choice of distribution on monotone mappings, and then with the analysis. One fundamental problem seems to be that there are only $\exp(O(n))$ partial monotone mappings on $[n]$, whereas there are $\exp(n \log(n))$ unrestricted mappings. While it is trivial to prove that $O(1)$ random mappings create an expander with high probability, we have no analogous result for monotone mappings. To give an example of the difficulty

[1] One can easily make the transition to the usual undirected case by including the inverse functions as well.

of analyzing a random monotone construction consider the following natural way of sampling a monotone mapping: pick two sets $S,T \subset [n]$ of size $n/2$ uniformly at random and map S onto T in a one-to-one way (mapping the i-th element of S to the i-th element of T). It is easy to see that the set $[1,t]$ will not expand with high probability for $t = \Omega(n)$ since this set will have all of its neighbors in the interval $[1, t + O(\sqrt{n})]$ with high probability.

Let us return to explicit constructions (which are more interesting for applications anyway). The first construction of monotone expanders was given in [11] in connection with dimension expanders; we shall elaborate on this connection below. This construction has logarithmic degree and is composed mainly of shift maps (that is, maps of the form $f(x) = x + i$). This construction was recently significantly improved by Bourgain in [6] where he constructs optimal $O(1)$-monotone expanders. In this work, we construct $O(\log^{(c)} n)$-monotone expanders for every integer c (with $\log^{(c)}(\cdot)$ denotes the c-times iterated logarithm). Bourgain's construction is quite involved, using in particular the recent breakthrough on the "Tits Alternative" by Breuillard [8], and its analysis is even more involved, extending work on spectral gaps on the unitary group $\mathsf{SU}(2)$ by Bourgain and Gamburd [7] to the group $\mathsf{SL}_2(\mathbb{R})$ (the reference [6] contains only sketches of the construction and analysis). In Section 6 we provide some more details on the workings behind this theorem.

Theorem 1.1 (Bourgain [6])**.** *There exists a strongly-explicit family of constant-degree monotone expanders.*

We will give our (suboptimal) construction here for two reasons. First, it is simple: it uses an iterated replacement product [26], observing that with appropriate ordering of vertices it preserves monotonicity of its components. Second, it shows that any (even nonconstructive) *existence* proof of $O(1)$-monotone expanders can be used as a base graph (in the style of [2]) to make our construction a strongly-explicit one of $O(1)$-monotone expanders.

1.1 Monotone expanders and dimension expanders

Monotone graphs, and the question of their expansion for small d arose implicitly in the paper of Dvir and Shpilka [11]. They reduce the problem of constructing degree-d *dimension expanders* (proposed in [4]) to the construction of $O(d)$-monotone expanders, and give an explicit construction of $O(\log n)$-monotone expanders of size n, leaving possible improvements as an open question. Since this connection was never given explicitly, we sketch it below.

A degree-d dimension expander is a set of d linear mappings $T_1, \dots, T_d : \mathbb{F}^n \to \mathbb{F}^n$ such that for every linear subspace $V \subset \mathbb{F}^n$ with $\dim(V) \le n/2$ we have

$$\dim\left(\sum_{i=1}^{d} T_i(V)\right) \ge (1+\alpha)\cdot \dim(V)\,.$$

Here, $\mathbb{F}$ is a field, possibly finite, and α is a positive constant independent of n. The probabilistic method shows that families of constant-degree dimension expanders exist. An explicit construction over fields of characteristic zero was given in [21].[2] Here, by "explicit" we mean that the matrices computing the linear

[2]The same result was obtained independently in [13] in the context of *quantum expanders* which imply dimension expanders over characteristic zero.

maps can be described as the output of an algorithm which runs in time polynomial in n (the notion of a "strongly-explicit" dimension expander does not make sense). In [11] an approach toward constructing dimension expanders over arbitrary fields was given. This approach involved applying a monotone expander graph on the coordinates (that is, permute the coordinates using d monotone mappings).

Theorem 1.2 ([11]). *If there exists an explicit construction of d-monotone expander graphs than there is an explicit construction of degree-d dimension expanders over any field $\mathbb{F}$.*

Proof. Let $e_1,\ldots,e_n \in \mathbb{F}^n$ denote the standard basis vectors. For each monotone partial function $f:[n] \to [n]$ in the expander we define a linear map $L_f : \mathbb{F}^n \to \mathbb{F}^n$ as follows: $L_f(e_i) = e_{f(i)}$ if $f(i)$ is defined and $L_f(e_i) = 0$ otherwise. To see why these linear maps are a dimension expander consider a subspace $V \subset \mathbb{F}^n$ of dimension $t \le n/2$. For a non-zero vector $v \in \mathbb{F}^n$ denote by $\pi(v) \in [n]$ the largest index of a non-zero coordinate of v. Similarly, let $\pi(V) = \{\pi(v) \mid v \in V\}$. Observe that $|\pi(V)| = \dim(V) = t$. Monotonicity implies that

$$\pi(L_f(V)) \supseteq f(\pi(V)),$$

where, for a set S, $f(S)$ is defined as the set of all images of f on elements of S on which f is defined. So, using expansion we obtain that

$$\left|\pi\left(\sum_{i=1}^{d} L_{f_i}(V)\right)\right| \ge (1+\alpha)\cdot t$$

giving the required bound on the dimension. □

This theorem combined with Bourgain's construction gives explicit constant-degree dimension expanders over any field.

Corollary 1.3. *Over any field $\mathbb{F}$, there exists an explicit family of constant degree dimension expanders.*

1.2 Monotone graphs and multi-pushdown graphs

The second contribution of this paper is the observation of a simple connection between d-monotone graphs and d-pushdown graphs: if the former are expanding then so are the latter (for the same d). This is of consequence since the question of whether $O(1)$-pushdown graphs have small separators (and thus cannot be expanders) is intimately related (and in some cases *equivalent*) to several questions in Turing machine complexity. With this observation, Bourgain's result simultaneously proves some conjectures and refutes others in one shot. The fundamental connection to complexity arises from the basic fact [24, 23] that computation graphs of certain Turing machines are $O(1)$-pushdown graphs. We describe this connection and its consequences below.

A d-pushdown graph [24, 23] is a graph on an ordered set of vertices such that, if we order the vertices along the spine of a book, the edges can be drawn on d pages of the book such that on each page, the edges are disjoint (they do not even share a vertex). These graphs come up naturally as the computation graphs of Turing machines with d tapes and are also a natural subclass of d-page graphs [9]. For a formal definition of d-pushdown graphs see Section 5.

Let us recall the definition of a separator. A separator S is a subset of the vertices of a graph G on n vertices such that the vertices outside S can be partitioned into two disjoint sets A and B each of size at most $2n/3$ and such that there are no edges between A and B. Observe that a graph with a sublinear-size separator is not an expander. The planar separator theorem [17] says that a planar graph has a $O(\sqrt{n})$-size separator. Since d-pushdown graphs are a generalization of planar graph it is natural to ask whether or not such graphs have $o(n)$ separators. This question (conjectured to be true in [24]) turns out to be related to the time needed to simulate a deterministic TM by a nondeterministic one.[3] A "segregator" theorem (proving the existence of a weaker object than a separator) is the combinatorial "heart" of the celebrated separation [23] of nondeterministic linear time from deterministic linear time (see also [27] for more recent results in this spirit).

In [12] it was shown that there exist 3-pushdown graphs which are "almost" expanders, in the sense that every separator must be of size $\Omega(n/\log^{(c)}(n))$ for any constant c. This is probably the earliest occurrence of what is now referred to as an iterative "Zig-Zag" construction. Our construction of degree-$\log^{(c)}(n)$ monotone expanders is very similar to theirs. In this paper we observe that d-monotone expanders can easily be transformed into d-pushdown expanders. Combining this observation with Bourgain's result we obtain that there exist (explicit) d-pushdown graphs which are expanders, settling an old open problem. We prove the following theorem in Section 5.

Theorem 1.4. *If there exist (strongly-explicit) d-monotone expanders than there exist (strongly-explicit) d-pushdown expanders.*

In [27] the assumption that the class of d-pushdown graphs have sub-linear separators was used to derive several complexity theoretic results. In particular, it was shown in [27] that this assumption implies the separation

$$\mathrm{NTIME}(t) \neq \Sigma_4\mathrm{-TIME}(t)$$

for all time bounds t. The existence of expanding d-pushdown graphs shows that this approach to prove such a separation cannot succeed.

Lower bounds on simulation time It was shown in [12] that the question of whether d-pushdown graphs are separable or not (i. e., if these graphs have sublinear-size separators) is equivalent to a question regarding the simulation time of certain Turing machines. More formally, let $t(n)$ denote the time it takes a 1-tape online nondeterministic TM to simulate a two tape real-time nondeterministic TM.[4] One can easily show that $t(n) = O(n^2)$. The question of whether or not $t(n) = o(n^2)$ was shown in [12] to be *equivalent* to whether or not d-pushdown graphs have small (sublinear) separators. Combining Bourgain's result with Theorem 1.4 above we obtain the following corollary.

Corollary 1.5. *In the notation above, we have $t(n) = \Theta(n^2)$.*

1.3 Organization

In Section 2 we give formal definitions and notation that will be used later on. In Section 3 we give the analysis of the replacement product for monotone graphs. In Section 4 we describe our iterative construction of near-constant-degree monotone expanders. In Section 5 we explain the connection between

[3] These results very strictly depend on the sequential access in a multi-tape Turing machine. They do not apply even if we replace the linear tape by a 2-dimensional grid, let alone with random access.

[4] A *real time* TM reads a new symbol at each step and an *on-line* TM is such that the input tape is one-way.

monotone and multi-pushdown graphs. Section 6 contains a brief outline of Bourgain's construction of monotone expanders. We conclude in Section 7 with some open problems and directions for future research.

2 Preliminaries and notation

We denote $[n] = \{1, 2, \ldots, n\}$. All logarithms are base 2.

Let V be a finite totally ordered set. We denote by $\mathbf{Part}[V]$ the set of partial functions $f : V \to V \cup \{\bot\}$ on the set V; here $f(x) = \bot$ means that f is undefined at x. We say that $f \in \mathbf{Part}[V]$ is *monotone* if, whenever f is defined at two distinct points $x < y \in V$, we have $f(x) < f(y)$. (In this paper we use "monotone" to mean "strictly increasing.") Notice that if f is monotone it is also injective and so there exists a (partial) inverse $f^{-1} \in \mathbf{Part}[V]$ which is also monotone. Also, if $f, g \in \mathbf{Part}[V]$ are monotone then we can define their composition $f \circ g$ which is also monotone (the composition is defined on those points x where $g(x) \neq \bot$ and $f(g(x)) \neq \bot$).

An *ordered directed graph* is a pair $G = (V, (f_1, \ldots, f_d))$ with V a finite totally ordered set and $f_i \in \mathbf{Part}[V]$ where we think of $f_i(x)$ as mapping x to its i-th neighbor (if one exists). In the following we will refer to these simply as "graphs." We will call d the *degree* of the graph. A graph $G = (V, (f_1, \ldots, f_d))$ is *monotone* if for all $i \in [d]$, f_i is monotone (with respect to the ordering of V). Notice that if G is monotone then for all $x \in V$, $\deg_{\text{in}}(x) \leq d$ (since the functions f_i are injective). Let $G = (V, (f_1, \ldots, f_d))$ be a monotone graph. We say that G is *inverse-closed* if d is even and for all $i \in [d/2]$, $f_{2i} = f_{2i-1}^{-1}$ (that is, G is composed of $d/2$ neighbor functions and their $d/2$ inverses).

For a graph $G = (V, (f_1, \ldots, f_d))$ and a subset $S \subset V$ we denote the *boundary* of S in G as

$$\partial_G S \triangleq \{(x, i) \mid x \in S,\, f_i(x) \in V \setminus S\}.$$

(We omit the subscript G if it is clear from the context.) The *edge-expansion* of G is denoted by

$$h(G) \triangleq \min_{\substack{S \subset V \\ 1 \leq |S| \leq \frac{1}{2}|V|}} \frac{|\partial_G S|}{d \cdot |S|}.$$

Another notion of expansion is vertex-expansion. For $S \subset V$ let

$$\Gamma_G(S) \triangleq \{y \in V \mid (\exists x \in S,\, i \in [d])(f_i(x) = y)\}.$$

The *vertex expansion* of G, denoted $\mu(G)$, is[5]

$$\mu(G) \triangleq \min_{\substack{S \subset [n] \\ 1 \leq |S| \leq \frac{1}{2}|V|}} \frac{|\Gamma_G(S) \setminus S|}{|S|}.$$

Claim 2.1. *If G is monotone then $\mu(G) \geq h(G)$.*

[5]Notice that this definition is slightly different from the way monotone expanders were defined in the Introduction. However, the two definitions are equivalent up to a constant factor.

Proof. Let $|S| \leq |V|/2$. Then S has at least $h(G) \cdot d \cdot |S|$ edges leaving it. Since G is monotone, the in-degree of a vertex is at most d and so there have to be at least $h(G) \cdot |S|$ neighbors of S that are not in S. ☐

We will require the following simple observation.

Claim 2.2. *If $G = (V, (f_1, \dots, f_d))$ is a monotone inverse-closed graph, then for all sets $S \subset V$ we have*

$$|\partial_G S| \geq h(G) \cdot d \cdot \min\{|S|, |V| - |S|\} .$$

Proof. The inequality follows from the definition of $h(G)$ and from the fact that, in an inverse-closed graph, the number of edges from any set S to its complement is equal to the number of edges in the opposite direction. ☐

3 The replacement product of monotone graphs

Let V_1, V_2 be two finite totally ordered sets. The *reverse lexicographic ordering* of the set $V_1 \times V_2$ is defined as follows: $(a_1, a_2) > (b_1, b_2)$ if $a_2 > b_2$ or, $a_2 = b_2$ and $a_1 > b_1$.

Let $G_1 = (V_1, (f_1, \dots, f_D))$ and $G_2 = (V_2, (g_1, \dots, g_d))$ be two graphs such that $|V_2| = D$. The *replacement product* $G_1 \circ G_2$ is a graph with vertex set $V_1 \times V_2$, ordered according to reverse lexicographic ordering and with $2d$ neighbor functions $s_1, \dots, s_d, t_1, \dots, t_d \in \mathbf{Part}[V_1 \times V_2]$ defined as follows: For $i \in [d]$,

$$s_i(a_1, a_2) = (a_1, g_i(a_2))$$

(if $g_i(a_2) = \perp$ then $s_i(a_1, a_2) = \perp$). The functions $t_1, \dots, t_d$ are all equal to the same function

$$t(a_1, a_2) = (f_{a_2}(a_1), a_2) ,$$

where the set V_2 is identified in some arbitrary one-to-one way with $[D]$ (again, if $f_{a_2}(a_1) = \perp$ then $t(a_1, a_2) = \perp$). It is clear from the definitions that, if G_1 and G_2 are monotone, then so is their product $G_1 \circ G_2$. The reason for including many parallel edges in the definition will make sense later when we argue about the expansion properties of the replacement product of two expanders (this is necessary to avoid small cuts).

The proof of the following lemma, bounding the edge-expansion of the replacement product, is essentially the same as the proof for undirected graphs appearing in [2]. Since our definitions are more involved we retrace the argument below.

Lemma 3.1 (Replacement product of two monotone expanders). *Let $G_1 = (V_1, (f_1, \dots, f_D))$ and $G_2 = (V_2, (g_1, \dots, g_d))$ be two monotone inverse-closed graphs such that $|V_2| = D$. Let $H = G_1 \circ G_2$. Then H is a monotone graph (with respect to reverse lexicographic ordering) and*

$$ah(H) \geq \frac{1}{80} \cdot h(G_1)^2 \cdot h(G_2) .$$

Proof. As was observed before, if G_1 and G_2 are monotone then so is $G_1 \circ G_2$. We are thus concerned only with bounding the edge expansion.

Let us denote $n = |V_1|$, $\delta_1 = h(G_1)$, $\delta_2 = h(G_2)$. Let $S \subset V_1 \times V_2$ be such that

$$|S| \le \frac{1}{2}|V_1 \times V_2| = \frac{1}{2} \cdot nD.$$

Since the degree of H is $2d$ we need to show that $|\partial S| \ge (1/80)\delta_1^2\delta_2 \cdot 2d \cdot |S|$.

For $x \in V_1$ we define $S_x = S \cap (\{x\} \times V_2)$. Let

$$I' = \{x \in V_1 \mid |S_x| \le (1 - \delta_1/4)D\}$$

and let $I'' = V_1 \setminus I'$. We partition the set S into two parts, $S' = \bigcup_{x \in I'} S_x$ and $S'' = S \setminus S'$.

We separate the analysis into two cases. The first is when $|S'| \ge (1/10)\delta_1|S|$. In this case we will get expansion using the mappings that act on the disjoint copies of V_2. For every $x \in I'$ we have (using Claim 2.2) that

$$|\partial_{G_2} S_x| \ge \delta_2 \cdot d \cdot \min\{|S_x|, D - |S_x|\} \ge \frac{1}{4}\delta_1\delta_2 \cdot d|S_x|,$$

(we abuse notation and treat S_x as a subset of V_2). Therefore, using the bound on $|S'|$, we obtain that

$$|\partial_H S| \ge \frac{1}{4}\delta_1\delta_2 \cdot d \cdot |S'| \ge \frac{1}{80} \cdot \delta_1^2\delta_2 \cdot 2d \cdot |S|.$$

We now turn to the case when $|S'| < (1/10)\delta_1|S|$. In this case we have $|S''| \ge (1 - \delta_1/10) \cdot |S|$. We will get expansion using the d identical copies of the map $t(x,y) = (f_y(x), y)$. Since for all $x \in I''$ we have $|S_x| > (1 - \delta_1/4) \cdot D$ we obtain that

$$\frac{|S''|}{D} \le |I''| \le \frac{|S''|}{(1 - \frac{1}{4}\delta_1) \cdot D}.$$

In particular, since $|S''| \le |S| \le (1/2) \cdot nD$, we have $|I''| \le (2/3) \cdot n$. Therefore, by Claim 2.2, we have

$$M = |\partial_{G_1} I''| \ge \frac{1}{2}\delta_1 \cdot D \cdot |I''|.$$

Consider the corresponding $d \cdot M$ edges in H. Of these $d \cdot M$ edges at most $(1/4)\delta_1 dD \cdot |I''|$ come from outside S'' and so there are at least $(1/4)\delta_1 dD \cdot |I''|$ edges from S''. Among these edges, at most $d \cdot |S'|$ can land in S' (here we rely on the fact that G_1 is monotone and so the mappings acting on the copies of V_1 are injective). We can bound this number of edges by

$$d \cdot |S'| \le \frac{1}{10}\delta_1 \cdot d \cdot |S| \le \frac{1}{6}\delta_1 \cdot dD|I''|.$$

We can therefore conclude that the number of edges from S'' to the complement of S is at least

$$\frac{1}{4}\delta_1 \cdot dD \cdot |I''| - \frac{1}{6}\delta_1 \cdot dD \cdot |I''| = \frac{1}{12}\delta_1 \cdot dD \cdot |I''|.$$

As $|I''| \ge |S''|/D$ and $|S''| \ge (1/2)|S|$ we have at least $(1/48)\delta_1 \cdot 2d \cdot |S|$ edges in H leaving S. $\square$

4 An iterative construction with near optimal degree

In this section we describe a simple iterative construction of monotone expanders with almost constant degree. We give our construction in two parts. The first (Section 4.1) gives a construction of a monotone expander with polylogarithmic degree. The second (Section 4.2) shows how to iterate the construction, using the tools from Section 3, and reduce the degree to $\log^{(c)}(n)$ for any constant c.

4.1 The base graph

In this section we describe a construction of a monotone expander graph with polylogarithmic degree which will be the basis of the full construction. The graph we will use is similar to the one used in [11]. However, since we are shooting for a strongly explicit graph, we will refrain from using the base graph from [29] (which is not strongly explicit) and will use the explicit expanders implicit in [1, 25] instead. The degree of these graphs is polylogarithmic (instead of logarithmic as in [29]) but this difference will "disappear" in the recursion done in the next section.

Theorem 4.1 (Expanders for $\mathbb{Z}_n$ [1, 25])**.** *There exists a constant $h_0 > 0$ and a strongly explicit family of graphs*

$$A_n = (\{0,1,\ldots,n-1\},(f_1,\ldots,f_d))$$

with $d = \log(n)^{O(1)}$, $h(G) \geq h_0$ and such that for each i there exists an integer a_i such that $f_i(x) = x + a_i \mod n$.

We now turn the above graph into a monotone expander in a manner similar to [11]. In fact, the proof of the following theorem implies that *any* Cayley expander for $\mathbb{Z}_n$ with degree d gives a monotone expander with degree $2d$.

Theorem 4.2 (Monotone expander with polylog degree)**.** *There exists a constant $h_1 > 0$ and a strongly explicit family of monotone, inverse-closed graphs*

$$B_n = (\{0,1,\ldots,n-1\},(g_1,\ldots,g_d))$$

with $d = \log(n)^{O(1)}$ and $h(G) \geq h_1$.

Proof. Without loss of generality suppose n is even (otherwise we can run the construction on $n-1$ vertices and then connect a single vertex arbitrarily). Let $m = n/2$ and let

$$A_m = (\{0,1,\ldots,m-1\},(f_1,\ldots,f_{d'}))$$

be the graph given by Theorem 4.1. Let $a_1,\ldots,a_{d'}$ be integers such that, for $0 \leq x \leq m-1$,

$$f_i(x) = x + a_i \mod m\,.$$

We define the graph B_n on vertex set $\{0,1,\ldots,n-1\}$ to have $d = 2d'$ neighbor functions. The first d' functions, call them $g_1,\ldots,g_{d'}$ will be defined as

$$g_i(x) = \begin{cases} x + a_i & x \leq m-1; \\ \perp & \text{otherwise.} \end{cases}$$

Since we can assume without loss of generality that the integers a_i are smaller than m we have that the mappings g_i, $i \in [d']$ are indeed monotone. We now add to B_n another d' mappings $g_{d'+1}, \ldots, g_{2d'}$ which will all be the same and will be defined as

$$g_i(x) = \begin{cases} x - m & x \geq m; \\ \perp & \text{otherwise.} \end{cases}$$

It is clear that the graphs B_n are monotone, have degree $\log(n)^{O(1)}$, and are strongly explicit. We can also assume without loss of generality that B_n is inverse closed simply by adding all the inverses (this will decrease the edge expansion by at most half). We now bound the edge expansion of B_n.

Let $S \subset \{0, 1, \ldots, n-1\}$ be such that $|S| \leq n/2$. We will show that the number of edges leaving S is at least $(1/16) \cdot h_0 \cdot d \cdot |S|$. Define $S_1 = S \cap \{0, 1, \ldots, m-1\}$ and $S_2 = S \setminus S_1$. We separate the analysis into two cases based on the size of the set

$$I = S_2 \setminus (S_1 + m).$$

If $|I| \geq (h_0/8) \cdot |S|$ then there will be at least $d' \cdot |I| \geq (h_0/16) \cdot d \cdot |S|$ edges of the form $x \mapsto x - m$ from S_2 to the outside of S_1 and so we are done.

We now deal with the case when $|I| < (h_0/8) \cdot |S|$. In this case we must have

$$|S_1| \geq \left(\frac{1}{2} - \frac{h_0}{8} \right) \cdot |S|,$$

for otherwise $|I|$ can be bounded from below by $|S_2| - |S_1| > (h_0/4) \cdot |S|$. We now use the expansion of A_m to claim that there are at least $h_0 \cdot d' \cdot |S_1| \geq h_0 \cdot (d/2) \cdot (1/2 - h_0/8) \cdot |S|$ edges from S_1 to the complement of $S_1 \cup (S_1 + m)$. Of these edges, at most $d' \cdot |I| \leq (d/2) \cdot (h_0/8) \cdot |S|$ can land in S_2. Therefore, there are at least

$$\frac{1}{2} \cdot \left[h_0 \cdot \left(\frac{1}{2} - \frac{h_0}{8} \right) - \frac{h_0}{8} \right] \cdot d \cdot |S| \geq \frac{h_0}{16} \cdot d \cdot |S|$$

edges from S to its complement in this case. This concludes the proof of the theorem. □

4.2 The iterative construction

We now combine Lemma 3.1 with Theorem 4.2 to give a construction of monotone expanders with degree close to constant. We denote by $\log^{(c)}(n)$ the log function iterated c times.

Theorem 4.3 (Monotone expanders with degree $\log^{(c)}(n)$)**.** *For every $c > 0$ there exists a strongly explicit family of monotone graphs $M_k = (V_k, (f_1, \ldots, f_{d_k}))$ such that*

1. $|V_k| = \Theta(k)$,
2. $d_k \leq O(\log^{(c)}(k))$,
3. $h(M_k) \geq \Omega\left(e^{-e^c}\right)$.

Proof. We describe an algorithm for producing M_k in c iterations. We start with a graph G_1 that has degree $\log(k)^{O(1)}$ and at each iteration decrease the degree to the logarithm of the previous degree using the replacement product.

Set G_1 to be B_k, the graph given by Theorem 4.2 on input k. Let D_1 be the degree of G_1, so $D_1 = \log(k)^{O(1)}$. Let B_{D_1} be given again by Theorem 4.2, this time on D_1 vertices and with degree $D_2 = \log(D_1)^{O(1)}$. We can take the replacement product

$$G_2 = G_1 \circ B_{D_1} .$$

From Lemma 3.1 we see that G_2 is a monotone graph on $k \cdot D_1$ vertices with degree $2D_2 = (\log\log(k))^{O(1)}$ and

$$h(G_2) \geq \frac{1}{80} \cdot h(G_1)^2 \cdot h(B_{D_1}) \geq \frac{1}{80} \cdot h_1^3 ,$$

where $h_1 > 0$ is the constant given by Theorem 4.3.

We can continue in this manner c times. At the j-th iteration we are given a graph G_j with degree $D_j = \mathrm{poly}(\log^{(j)}(k))$ and we take its replacement product with B_{D_j}. If we denote by h_j the edges expansion at the j-th iteration we see that

$$h_j \geq \frac{1}{80} h_{j-1}^2 \cdot h_1 \geq (h_1/80)^{3^j}$$

and so, after c iterations we will have expansion at least $\Omega(\exp\exp(c))^{-1}$.

Tracing the growth of the vertex set size we conclude that the size of the final graph is some explicit function of k of the form $\approx k \cdot \mathrm{poly}(\log(k)) \cdot \mathrm{poly}(\log\log(k)) \cdots \mathrm{poly}(\log^{(c)}(k))$. We can choose a starting integer k', slightly smaller than k, so that the final graph will have size $\Theta(k)$.

The part of the theorem claiming strong explicitness can be easily verified by induction on the number of iterations (since the base graph is strongly explicit). □

From this last proof we see that, if we had an existence proof for constant-degree monotone expanders, we could transform it into an explicit construction in the following manner: start with two iterations of the replacement products as we did above, then, do an exhaustive search for a constant-degree monotone expander on $\mathrm{poly}(\log\log(n))$ vertices (this can be done in $\mathrm{poly}(n)$ time) and use it in the last replacement product. This approach (introduced in [2] to give a simple explicit construction of expander graphs) can be summarized in the next corollary.

Corollary 4.4. *If there exist constant-degree monotone expanders then they can be constructed in a strongly-explicit way.*

Notice that the only reason this last corollary is of any interest is that it does not rely on Bourgain's proof (which shows independently that there is an explicit construction). We hope that a simple existence proof can be found and used in conjunction with this corollary to give a simple explicit construction.

5 Connection to multi-pushdown graphs

In this section we deal with both monotone ordered directed graphs (as defined in Section 2) and with undirected graphs (in the usual sense). Our goal is to show that the existence of degree-d monotone expanders imply the existence of expanders that are d-pushdown graphs. We start by giving a formal definition of these graphs, which are a special case of d-page graphs. For more on this interesting family of graphs and its applications see [5, 10].

Definition 5.1 (d-page graphs)**.** A 1-page graph is an undirected graph with ordered vertex set $V = [n]$ such that for every pair of edges $(a,b),(c,d) \in [n]^2$ in the graph, we have that $c \in [a,b]$ iff $d \in [a,b]$. In other words, if we write down the vertices in a vertical ordered line, we could draw all the edges on the right side of this line without having intersections between edges. A d-page graph is a union of at most d 1-page graphs on the same set of vertices under the same ordering.

A d-pushdown graph is a d-page graph such that in each page the degree of each vertex is at most one. It is easy to see where these graphs get their name from—they describe a sequence of insertions/deletions from d pushdown stacks ("first in last out").

Definition 5.2 (d-pushdown graphs)**.** A 1-pushdown graph is a 1-page graph in which the degree of each vertex is at most one. A d-pushdown graph is a union of at most d 1-pushdown graphs (on the same set of vertices, under the same ordering).

The next claim shows how a monotone graph of degree d can be transformed into a d-pushdown graph with roughly the same expansion (the vertex expansion of an undirected graph is defined in a similar way to the directed case).

Claim 5.3. *Let $G = ([n], \{f_1, \ldots, f_d\})$ be a monotone inverse-closed graph with $f_1 = id$. Define H to be an undirected graph on vertex set $[2n]$ as follows: for every $i \in [d]$ and every $a \in [n]$ such that $f_i(a) \neq \perp$, H contains the undirected edge $(a, 2n+1-f_i(a))$. Then*

1. *H is a d-pushdown graph,*
2. *$\mu(H) \geq \frac{1}{4} \cdot \mu(G)$.*

Proof.

1. Each set of edges in H coming from a single f_i will give us a 1-pushdown graph since two edges $(a, 2n - f_i(a))$ and $(b, 2n - f_i(b))$ with $a < b$ will satisfy $a < b < 2n - f_i(b) < 2n - f_i(a)$ and so the edges will not cross each other.
2. Let $\alpha = \mu(G)$. Let $S \subset [2n]$ be a set of vertices of size $k \leq n$. We will show that S has at least $|S| \cdot (1 + \alpha/2)$ neighbors (including vertices in S). This will prove that $\mu(H) \geq \alpha/2$ as was required. We will rely on the fact that the identity mapping belongs to the graph G. Let $S_1 = S \cap [n]$ and $S_2 = S \setminus S_1$. Let $k_1 = |S_1|$ and $k_2 = |S_2|$ so that $k = k_1 + k_2$. Assume without loss of generality that $k_1 \geq k_2$. Notice that the neighbors of S_1 belong to the set $[n+1, 2n]$ and that the neighbors of S_2 are in $[n]$. This means that $|\Gamma(S)| \geq \max\{2k_1, k + \alpha k_2\}$, since k_2 expands (it is smaller than $n/2$) and k_1 is copied by the identity map. If $k_2 \geq k/4$ then $k + \alpha k_2 \geq (1 + \alpha/4)k$ and if $k_2 < k/4$ then $2k_1 \geq (1 + \alpha/4)k$ because $\alpha \leq 1$. This completes the proof.

□

Combining Claim 5.3 with Bourgain's construction of constant-degree monotone expanders [6] we obtain the following corollary.

Corollary 5.4. *There exist an integer d, a positive constant α, and a strongly-explicit family of n-vertex undirected d-pushdown graphs G_n, such that $\mu(G_n) \geq \alpha$ for all n.*

6 Bourgain's monotone expanders

We give here a brief outline of Bourgain's construction of monotone expanders. Let $\mathsf{SL}_2(\mathbb{R})$ denote the group of 2×2 real matrices with determinant 1. This group acts[6] on the projective line $\mathbb{P}^1 = \mathbb{R} \cup \{\infty\}$ in the following way: with each matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

we associate the Moebius transformation

$$\psi_A(x) = \frac{ax+b}{cx+d}$$

(the inclusion of ∞ allows for division by zero). Furthermore, the derivative of this mapping is given by

$$\psi_A'(x) = \frac{1}{(cx+d)^2}$$

so this is a monotone increasing function on any interval not containing $-d/c$.

Bourgain's construction proceeds to find (explicitly) a finite subset of $\mathsf{SL}_2(\mathbb{R})$ (in fact, with rational entries) that, roughly speaking, satisfies the following two conditions:

1. The matrices in the set are all close to the identity matrix and so their associated mappings do not move any point in $\mathbb{P}^1$ by much.

2. They satisfy a so called "restricted spectral gap" property. This property ensures that applying their associated maps to "nice" subsets in $\mathbb{P}^1$ will expand their measure by a bounded factor.

Combining these two properties and limiting our attention to a specific interval (which is possible due to Property 1) one gets the following continuous analog of monotone expanders.

Theorem 6.1 ([6])**.** *There exists $\alpha > 0$ and an explicit finite set Ψ of smooth increasing maps $\psi : [0,1] \to [0,1]$ such that for any measurable subset A of $[0,1]$, if $|A| < 1/2$ we have*

$$\max_{\psi \in \Psi} \left| \psi(A) \setminus A \right| \geq \alpha |A| .$$

[6] A group action on a space S is a homomorphism from the group to the group of automorphisms of S.

The final step in the construction is to discretize it by dividing the interval $[0,1]$ into n intervals of length $1/n$ and associating with each smooth mapping a discrete mapping from $[n]$ to $[n]$ in a natural way so that expansion in measure is transformed into expansion in set size. The property of "strong" monotonicity (no collisions) is obtained by observing that, since the derivatives of the smooth mappings ψ used in the construction are bounded from below, one does not have more than a constant number of edges mapping to a single vertex. This allows one to "break up" each weakly monotone mapping into a constant number of strongly monotone (partial) mappings, while preserving expansion.

7 Conclusions and open problems

This paper wishes to popularize some facts we find remarkable: explicit constant-degree expanders exist, whose graph structure is extremely restricted: the vertices are ordered, and edges decompose into few monotone maps, or few legal parenthesis sequences. In particular, these graphs are "nearly planar" in a precise sense. It would be interesting to explore the limitations of the expansion of these graphs. For example, can a constant-degree monotone graph be a lossless expander? a Ramanujan graph? a unique-neighbor expander? (Lossless expanders are expanders of degree d with expansion factor close to d (so that the expansion is "maximal"). Unique-neighbor expanders are expanders in which, for every set S of vertices, there are "many" neighbors of S that have only one neighbor in S.

Consequences of these constructions include new explicit pseudorandom objects (dimension expanders) as well as a better understanding of the computation graphs of various Turing machines. We believe that more applications of these expanders will be found. Specifically, algorithms on restricted models, especially operating with limited access to input, may be able to utilize these new expanders.

Another remarkable feature of these expanders is that while they have an explicit construction, no known direct (and simpler) existence proof is known. Few pseudorandom structures are known which have an explicit construction but whose existence does not follow from some application of the probabilistic method. We find the question of providing a simple *existence* proof of constant-degree monotone expanders very appealing mathematically. Here we also motivate it by showing how any such proof (even a highly nonconstructive one) directly implies a simple, strongly explicit construction. This reduction uses the Zig-Zag graph product adapted to monotone graphs, further revealing the generality of this paradigm.

In a different direction, while constant-degree monotone expanders lead to constant-degree dimension expanders via the reduction of Dvir-Shpilka [11], in some sense this construction is not very natural. A possibly more natural construction was conjectured by Wigderson in [28], and we conclude this section with a formal statement of it. Recall the definition of dimension expanders from the introduction.

Conjecture 7.1 ([28])**.** *Let G be a finite group, $S = \{g_1, \dots, g_k\}$ a symmetric set of generators, and assume the associated Cayley graph is an expander; for concreteness, assume the second normalized eigenvalue of its adjacency matrix is $1/2$. Let F be a field of characteristic that does not divide $|G|$. Let ρ be an irreducible representation of dimension n over F. Then $\rho(g_1), \dots, \rho(g_k) : F^n \to F^n$ form a dimension expander.*

We note that the paper of Lubotzky and Zelmanov [21] mentioned above constructs constant-degree dimension expanders over fields of characteristic 0 precisely by proving the conjecture above for such fields (and then using any group with a constant number of expanding generators and high dimensional irreducible representations, e. g., $\mathsf{SL}_2(p)$). The same paper gives purely algebraic motivations for resolving this conjecture for finite fields.

Acknowledgements

We thank Noga Alon and Jean Bourgain for helpful conversations. We thank Dieter van Melkebeek and Rahul Santhanam for very helpful comments on earlier drafts of this paper.

References

[1] MIKLÓS AJTAI, HENRYK IWANIEC, JÁNOS KOMLÓS, JÁNOS PINTZ, AND ENDRE SZEMERÉDI: Construction of a thin set with small Fourier coefficients. *Bull. Lond. Math. Soc.*, 22:583–590, 1990. [doi:10.1112/blms/22.6.583] 299

[2] NOGA ALON, ODED SCHWARTZ, AND ASSAF SHAPIRA: An elementary construction of constant-degree expanders. *Combin. Probab. Comput.*, 17(3):319–327, 2008. [doi:10.1017/S0963548307008851] 292, 293, 297, 301

[3] NOGA ALON, PAUL SEYMOUR, AND ROBIN THOMAS: A separator theorem for graphs with an excluded minor and its applications. In *Proc. 22nd STOC*, pp. 293–299, New York, NY, USA, 1990. ACM Press. [doi:10.1145/100216.100254] 292

[4] BOAZ BARAK, RUSSELL IMPAGLIAZZO, AMIR SHPILKA, AND AVI WIGDERSON: Definition and existence of dimension expanders, 2004. Discussion (no written record). 293

[5] FRANK BERNHART AND PAUL C. KAINEN: The book thickness of a graph. *J. Combin. Theory Ser. B*, 27(3):320–331, 1979. [doi:10.1016/0095-8956(79)90021-2] 302

[6] JEAN BOURGAIN: Expanders and dimensional expansion. *C. R. Math.*, 347(7–8):357–362, 2009. [doi:10.1016/j.crma.2009.02.009] 293, 303

[7] JEAN BOURGAIN AND ALEX GAMBURD: On the spectral gap for finitely-generated subgroups of $\mathsf{SU}(2)$. *Invent. Math.*, 171:83–121, sep 2007. [doi:10.1007/s00222-007-0072-z] 293

[8] EMMANUEL BREUILLARD: A strong Tits alternative. Technical Report arXiv:0804.1395, ArXiv e-print repository, April 2008. [arXiv:0804.1395v1] 293

[9] JONATHAN F. BUSS AND PETER W. SHOR: On the pagenumber of planar graphs. In *Proc. 16th STOC*, pp. 98–100, New York, NY, USA, 1984. ACM Press. [doi:10.1145/800057.808670] 294

[10] FAN R. K. CHUNG, FRANK THOMSON LEIGHTON, AND ARNOLD L. ROSENBERG: Embedding graphs in books: A layout problem with applications to VLSI design. *SIAM J. Algebr. Discrete Methods*, 8(1):33–58, 1987. [doi:10.1137/0608002] 302

[11] ZEEV DVIR AND AMIR SHPILKA: Towards dimension expanders over finite fields. In *Proc. IEEE 23rd Ann. Conf. Comput. Complex. (CCC)*, pp. 304–310, Washington, DC, USA, 2008. IEEE Comp. Soc. Press. [doi:10.1109/CCC.2008.19] 293, 294, 299, 304

[12] ZVI GALIL, RAVI KANNAN, AND ENDRE SZEMERÉDI: On nontrivial separators for k-page graphs and simulations by nondeterministic one-tape Turing machines. In *Proc. 18th STOC*, pp. 39–49, New York, NY, USA, 1986. ACM Press. [doi:10.1145/12130.12135] 292, 295

[13] ARAM HARROW: Quantum expanders from any classical Cayley graph expander. *Quantum Inf. Comput.*, 8(8/9):715–721, 2008. QIC Volume 8. 293

[14] SHLOMO HOORY, NATHAN LINIAL, AND AVI WIGDERSON: Expander graphs and their applications. *Bull. Amer. Math. Soc. (N.S.)*, 43:439–561, 2006. [doi:10.1090/S0273-0979-06-01126-8] 292

[15] MARTIN KASSABOV, ALEXANDER LUBOTZKY, AND NIKOLAY NIKOLOV: Finite simple groups as expanders. *Proc. Natl. Acad. Sci. USA*, 103(16):6116–6119, 2006. [doi:10.1073/pnas.0510337103] 292

[16] MARIA M. KLAWE: Limitations on explicit constructions of expanding graphs. *SIAM J. Comput.*, 13(1):156–166, 1984. [doi:10.1137/0213011] 292

[17] RICHARD J. LIPTON AND ROBERT E. TARJAN: A separator theorem for planar graphs. *SIAM J. Appl. Math.*, 36(2):177–189, 1979. [doi:10.1137/0136016] 295

[18] RICHARD J. LIPTON AND ROBERT E. TARJAN: Applications of a planar separator theorem. *SIAM J. Comput.*, 9(3):615–627, 1980. [doi:10.1137/0209046] 292

[19] ALEXANDER LUBOTZKY, RALPH PHILLIPS, AND PETER SARNAK: Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988. [doi:10.1007/BF02126799] 292

[20] ALEXANDER LUBOTZKY AND BENJAMIN WEISS: Groups and expanders. In *Expanding graphs (Princeton, NJ, 1992)*, DIMACS Ser. 10, pp. 95–109, Providence, RI, 1993. AMS. 292

[21] ALEXANDER LUBOTZKY AND EFIM ZELMANOV: Dimension expanders. *J. Algebra*, 319(2):730–738, 2008. [doi:10.1016/j.jalgebra.2005.12.033] 293, 304

[22] G. A. MARGULIS: Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. *Problemy Peredachi Informatsii*, 24(1):51–60, 1988. 292

[23] WOLFGANG J. PAUL, NICHOLAS PIPPENGER, ENDRE SZEMERÉDI, AND WILLIAM T. TROTTER: On determinism versus non-determinism and related problems. In *Proc. 24th Ann. Symp. Found. Comput. Sci. (SFCS)*, pp. 429–438, Washington, DC, USA, 1983. IEEE Comp. Soc. Press. [doi:10.1109/SFCS.1983.39] 294, 295

[24] NICHOLAS PIPPENGER: Advances in pebbling (preliminary version). In *Proc. 9th Colloq. Autom. Lang. Program. (ICALP)*, pp. 407–417, London, UK, 1982. Springer-Verlag. [doi:10.1007/BFb0012787] 294, 295

[25] ALEXANDER RAZBOROV, ENDRE SZEMERÉDI, AND AVI WIGDERSON: Constructing small sets that are uniform in arithmetic progressions. *Combin. Probab. Comput.*, 2:513–518, 1993. [doi:10.1017/S0963548300000870] 299

[26] OMER REINGOLD, SALIL VADHAN, AND AVI WIGDERSON: Entropy waves, the zig-zag graph product, and new constant-degree expanders. *Ann. of Math.*, 155(1):157–187, 2002. [JSTOR:3062153] 292, 293

[27] RAHUL SANTHANAM: On separators, segregators and time versus space. In *Proc. IEEE 16th Ann. Conf. Comput. Complex. (CCC)*, pp. 286–294, Washington, DC, USA, 2001. IEEE Comp. Soc. Press. [doi:10.1109/CCC.2001.933895] 292, 295

[28] AVI WIGDERSON: Expanders: Old and new applications and problems. (A lecture at IPAM, UCLA), February 2004. 304

[29] AVI WIGDERSON AND DAVID XIAO: Derandomizing the Ahlswede-Winter matrix-valued Chernoff bound using pessimistic estimators, and applications. *Theory of Computing*, 4(1):53–76, 2008. [doi:10.4086/toc.2008.v004a003] 299

AUTHORS

Zeev Dvir
Postdoc
School of Mathematics
Institute for Advanced Study, Princeton
dvir@ias.edu
http://www.math.ias.edu/~dvir

Avi Wigderson
Professor
School of Mathematics
Institute for Advanced Study, Princeton
avi@ias.edu
http://www.math.ias.edu/~avi

ABOUT THE AUTHORS

ZEEV DVIR is currently a postdoc in the school of mathematics at the IAS in Princeton NJ. He got his Ph. D. from the Weizmann Institute in Israel in 2008. His advisors were Ran Raz and Amir Shpilka. He is interested mainly in questions in computational complexity that have a connection with pure mathematics. He likes to play the guitar and do yoga.

AVI WIGDERSON was born in Haifa, Israel in 1956, and received his Ph. D. in 1983 at Princeton University under Dick Lipton. He enjoys and is fascinated with studying the power and limits of efficient computation, and the remarkable impact of this field on understanding our world. Avi's other major source of fascination and joy are his three kids, Eyal, Einat, and Yuval.