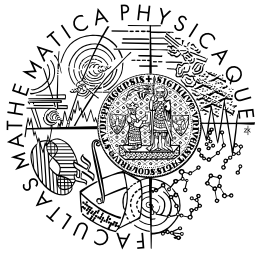

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

**BACHELOR THESIS**

Tomáš Domes

# Constructions of Bounded-depth Superconcentrators

Computer Science Institute of Charles University

Supervisor of the bachelor thesis: Michal Koucký

Study programme: Computer Science

Study branch: General Computer Science

Prague 2021

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date .....  .....

Author's signature

Na tomto místě bych rád poděkoval těm, kteří mi s vypracováním této práce pomohli. Předně svému vedoucímu Michalu Kouckému za nabídku zajímavého tématu, za trpělivé vysvětlování základních konceptů a za spousty hodin konzultací vznikající práce. Dále Martinu Dvořákovi, Kubovi Tětkovi a Janě Kopfové za jejich cenné korektury. Medvědovi za vytvoření této skvělé LaTeXové šablony. A konečně své rodině, která měla pochopení pro to, že jsem se jim v průběhu psaní příliš nevěnoval a domů jezdil přibližně jednou za čtvrt roku.

Title: Constructions of Bounded-depth Superconcentrators

Author: Tomáš Domes

Institute: Computer Science Institute of Charles University

Supervisor: Michal Koucký, Computer Science Institute of Charles University

Abstract: In the thesis, we summarize known results regarding different types of expanders, upper and lower bounds on their sizes, and their explicit constructions. From the expanders, we construct bounded-depth superconcentrators of optimal size for every depth, and we show some explicit bounded-depth superconcentrator constructions from the explicit expanders. Apart from few minor generalizations, we do not bring any new results, but we present several known bounded-depth superconcentrator constructions in one place together with all the tools needed for the constructions. As far as we know, no such survey has existed before.

Keywords: superconcentrator constructions, expanders

# Contents

# Introduction

## Superconcentrators

A *superconcentrator* was defined by Valiant [1975] as a variant of *concentration networks*, also called *concentrators*. Concentrators were originally studied as a telephone network model – such a network has inputs, crosspoints, and outputs, all of them connected by wires. By the original definition, a concentrator is a network with $n$ inputs and $m$ outputs, such that any $k \leq m$ inputs can be connected to some $k$ outputs, while every wire or crosspoint can be used only for one connection. In the language of graph theory, the network can be viewed as a graph, in which we connect input and output vertices by vertex-disjoint paths.

A superconcentrator is a network with $n$ input vertices and $n$ output vertices, such that for any set $S$ of $k \leq n$ input vertices and any set $T$ of $k$ output vertices, there are $k$ vertex-disjoint paths between $S$ and $T$. One can easily imagine an application in computer networks – we have $k$ requests on the inputs (from $k$ clients), and we need to route the requests to some $k$ servers while utilizing the network evenly. Valiant's goal was to use superconcentrators for proving lower bounds on the running time of algorithms for certain arithmetic problems. By this, he (along with others) started a new era of using concentrators, superconcentrators, and other related networks in computational complexity theory.

By the *size* of a superconcentrator, we mean the number of its edges with respect to the number $n$ of the input vertices. Valiant [1975] proved the existence of a superconcentrator of linear size, and many authors later tried to achieve better and better constants in size. However, in many applications, the *depth* (longest path from an input to an output vertex) of the superconcentrator is also a relevant parameter. In our thesis, as the title suggests, we focus on the tradeoff between the size and the depth of superconcentrators.

Most of the time, we talk about the *existence* of superconcentrators of appropriate size and depth. However, for some applications, one needs to have an efficient algorithm for finding such a superconcentrator. Such superconcentrators with an algorithm are called explicit, and we dedicate the final part of the thesis to them.

## Structure of the thesis

As far as we know, the only tool for superconcentrator constructions are graphs called *expanders*. Generally, in expanders, subsets of vertices have many neighbours. That's why they are useful in superconcentrator constructions – if the vertices with requests in them have enough neighbours, we can route the requests to other vertices and consequently find the required vertex-disjoint paths. However, there are many different definitions of expanders, so we spend the first chapter defining different kinds of expanders and examining their properties (mostly the tradeoff between the average degree and the expansion properties).

In the second chapter, we stay with the expanders and look closely at the relationships between different kinds of them – we prove that if a graph is an expander

of one type, it is usually to some extent also an expander of another type, and we also show some techniques of constructing one type of an expander from another.

In the third chapter, we finally get to the superconcentrators. Using the expanders from the first chapter, we construct a bounded-depth superconcentrator of asymptotically optimal size for every depth.

After that, in chapter four, we again come back to the expanders, particularly to the explicit constructions. We also use there the relationships from chapter two to get explicit expanders of one kind from explicit expanders of another one.

In the last chapter, we use the explicit expanders to construct explicit superconcentrators, and we state some open problems concerning mostly the explicit expander constructions.

# Basic definitions and notation

We state a few notes to the notation.

- In the whole thesis we usually denote reals by greek letters $(\alpha, \beta, \gamma, \dots)$, integers by lowercase letters $(a, b, c, \dots)$ and sets by capitals $(A, B, C, \dots)$.
- For integer $x$, we denote the set $\{1, 2, \dots, x\}$ by $[x]$. We denote the vertices in a graph by numbers $1, 2, \dots n$, so the set of all vertices of a graph is $[n]$.
- By multigraph, we mean an undirected graph, in which we allow multiple edges and loops (unless we explicitly state "directed multigraph").
- By biregular multigraph, we mean a bipartite multigraph with all left vertices of degree $d$ and all right vertices of degree $d'$ for some integers $d, d'$.
- For multigraph $G(E, V)$ and $X \subseteq V$, we denote the set of all neighbours of $X$ by $\mathsf{N}(X) \stackrel{\text{def}}{=} \{v \mid \exists u \in V : \{v, u\} \in E\}$. Note that the intersection $X \cap \mathsf{N}(X)$ can be nonempty.
- We denote the natural logarithm of $\alpha$ by $\log \alpha$ and the Euler's number by $e$.

# 1. Building blocks – expanders

*Expander graphs*, shortly *expanders* are the key (and maybe only) building block of superconcentrator constructions. They have various applications in many different fields, which in turn require different versions of expanders and different settings of parameters. Below, we provide an overview of several expander-like graphs, which are useful for us. We define all the expanders as undirected multigraphs (however, some authors use directed multigraphs).

We start the chapter with perhaps the most "standard" expanders – *vertex expanders*. In vertex expanders, every set $|S| \leq k$ of vertices "expands" – it has at least $\gamma |S|$ neighbours for some fixed $\gamma$.

The *k-expanding graphs* are somehow opposite to the vertex expanders – in a $k$-expanding graph, every two sets of vertices of size $k$ share an edge.

We also present a generalization of bipartite $k$-expanding graphs – *disperser graphs*.

The chapter is concluded with *spectral expanders*. These are graphs with a large *spectral gap* – the difference between the two largest eigenvalues of the adjacency matrix (in magnitude). From the definition, it is not clear why to call them expanders, but in Chapter 2, we prove that spectral expanders have properties of vertex expanders and $k$-expanding graphs (to some extent).

Of course, there are more types of expanders that we do not cover in our thesis, e.g. *boundary expanders*, in which every set $S$ of size $s \leq k$ has at least $\gamma s$ neighbours outside $S$, or *edge expanders* in which for a set of vertices of size $s \leq k$, there are at least $\gamma s$ edges leaving the set.

In Table 1.1, we summarize the dependence of the best-known sizes of these graphs on relevant parameters. These sizes are often based on so-called "probabilistic constructions" – proof that a random graph has desired property with nonzero probability. Explicit constructions of these graphs usually don't achieve these values; we discuss them in Chapter 4.

## 1.1 Vertex expanders

Informally, in expander graphs, every sufficiently large subset of vertices "expands" – in the meaning that it "has many neighbours". This is captured by the definition of *vertex expanders* below.

### 1.1.1 Definitions

**Definition 1** (Vertex expander)**.** *For positive integers $k \leq n$ and a real $\gamma > 0$, a multigraph on $n$ vertices is a vertex $(k, \gamma)$-expander, if for every set $S$ of at most $k$ vertices, $|\mathsf{N}(S)| \geq \gamma |S|$.*

It is clear that we must always have $\gamma k \leq n$; otherwise, we would require some set to have more than $n$ neighbours.

To distinguish it from bipartite versions defined below, we sometimes call it *general vertex expander*.

| | Vertex expander | $\lambda$-expander | $k$-expanding graph | Disperser graph |
|---|---|---|---|---|
| General | $\bar{d} \geq \frac{2(\gamma+2)\log\left(\frac{e^2 n}{k}\right)}{\log\left(\frac{n-k}{\gamma k}\right)}$ | $\lambda \leq \frac{2}{\sqrt{d}}$ | $\bar{d} \geq \frac{4n}{k}\log\left(\frac{en}{k}\right)$ | $\emptyset$ |
| Balanced | $d \geq \frac{(\gamma+2)\log\left(\frac{e^2 n}{k}\right)}{\log\left(\frac{n}{\gamma k}\right)}$ | $\lambda \leq \frac{2}{\sqrt{d}}$ | $d \geq \frac{2n}{k}\log\left(\frac{en}{k}\right)$ | $\emptyset$ |
| Unbalanced | $d \geq \frac{(\gamma+2)\log\left(\frac{e^2 n}{k}\right)}{\log\left(\frac{m}{\gamma k}\right)}$ | ? | $d \geq \frac{2m}{k}\log\left(\frac{e\sqrt{nm}}{k}\right)$ | $d \geq \frac{1}{\varepsilon}\log\left(\frac{en}{k}\right) + \frac{m}{k}\log\left(\frac{e}{\varepsilon}\right)$ |

Table 1.1: Existence of expanders with (left) degree $d$ or average (left) degree $\bar{d}$

We must note that there is also an alternative definition of vertex expanders, which says that $|\mathsf{N}(S) \setminus S| \geq \gamma |S|$. Some call these expanders *boundary expanders*. Theorems 2 and 10 do not hold for the boundary expanders, so we stick to our original definition. However, for the bipartite cases, the definitions coincide, so the difference is, in fact, not important for the applications in the constructions of superconcentrators (as we use the bipartite expanders in them).

We also remark that by the above definition, the complete graph is the best expander in both relevant parameters $\gamma$ and $k$ (it has for every $k$ the highest possible expansion factor $\gamma$). What interests us is usually the tradeoff between the expansion properties and the number of edges, which is typically expressed by maximal or average degree. We denote the maximal degree $d$, the average degree $\bar{d}$ and the number of vertices $n$, so the size of the expander is $\mathcal{O}(dn)$, or $\mathcal{O}(\bar{d}n)$.

By *bipartite vertex expander*, we mean any bipartite multigraph with left side of size $n$ and right side of size $m \leq n$ satisfying vertex expander property. However, we only require this property to hold for $S$ chosen from the left side. We denote the maximum left degree $d$, maximum right degree $d'$ and average left and right degree $\bar{d}$ and $\bar{d}'$. Again, we denote the sets of vertices $[n]$ and $[m]$.

**Definition 2** (Bipartite vertex expander)**.** *For positive integers $n, m, k; n \geq m; n \geq k$ and a real $\gamma > 0$, a bipartite multigraph with left side of size $n$ and right side of size $m$ is a bipartite vertex $(k, \gamma)$-expander, if for every subset $S$ of at most $k$ left side vertices, $|\mathsf{N}(S)| \geq \gamma |S|$.*

Analogously to the general case, we must always have $\gamma k \leq m$ in the bipartite case.

If the parts are of the same size, we denote by $n$ the size of each part and call the graph *balanced vertex expander*. For balanced vertex expanders, achieving $\gamma = 1$ is trivial with $d = 1$ for every $k$; we just define the graph as a matching between the two parts.

If the parts have different sizes, we call such expanders *unbalanced vertex expanders*. For unbalanced expanders (besides maximizing $k$ and $\gamma$), we usually

try to minimize $m$. Intuitively, it makes sense that the smaller $m$, the harder it is to achieve the same expansion factor, as we are expanding to a smaller space.

For $\gamma = 1$, unbalanced expanders correspond to *depth-1 concentrators*. When every set $|S| \leq k$ of left vertices has at least $|S|$ neighbours, it follows from Hall's Marriage Theorem, that for every set $|T| \leq k$ of left vertices, there is a matching from $T$ to the right side which covers $T$. Therefore, if we have some $\leq k$ "requests" on the left side, the matching will "concentrate" them to the right (smaller) side. The concentrator property is useful in the superconcentrator constructions, so in unbalanced vertex expanders, the case $\gamma = 1$ is the most interesting for us. We define the concentrators formally in Chapter 3 (Definition 16).

### 1.1.2 Upper and lower bounds

We now show a probabilistic construction of bipartite expanders. It is based on construction by Alon and Pudlák [1994]. However, the original theorem was stated only for $k \leq \frac{m}{2}$ and $\gamma = 1$; we generalized it for all $\gamma$ and we require only $\gamma k \leq m$ (which is important in the constructions later).[1]

We also note that the result is meaningless for $\gamma k$ close to $m$ (or to $n$ in the general case), as the theorems then yield arbitrarily large $d$, even though it must be always enough to have $d = m$ (or $d = n$).

**Theorem 1** (Lemma 4.2 in Alon and Pudlák [1994])**.** *Let there be three positive integers $n, m, k$ and a real number $\gamma > 0$, such that $n \geq k$ and $n \geq m > \gamma k$. If $\gamma \geq \frac{m}{en}$, there is a bipartite vertex $(k, \gamma)$-expander with left degree $d$ for every*

$$d \geq (\gamma + 1)\frac{\log\left(\frac{e^2 n}{k}\right)}{\log\left(\frac{m}{\gamma k}\right)}.$$

*If $\gamma \leq \frac{m}{en}$, there is a bipartite vertex $(k, \gamma)$-expander with left degree $d$ for every*

$$d \geq 3.$$

Note, that in Section 2.6, we will see a technique for constructing an unbalanced vertex expander from a balanced one. When $\frac{n}{m}$ is an integer, we can achieve $\gamma \leq \frac{m}{n}$ with $d = 1$ using this technique on trivial balanced vertex expander with $\gamma = 1$. For the details, see Section 2.6.

*Proof.* We construct a random multigraph $G$ on $n + m$ vertices with left degree $d$ as follows. For each vertex $v \in [n]$, we choose randomly with replacement $d$ neighbours in $m$. Let $X \subseteq [n]$, be a counterexample to the expansion property, i.e. $|X| \leq k$ and $|\mathsf{N}(X)| < \gamma |X|$. We now show, that the expected value $\mathsf{E}$ of the number of such counterexample sets in $G$ is less than one, which means, that there exists at least one multigraph with degree $d$ and no counterexample – the desired $(k, \gamma)$-expander.

So, let's first express the expected number of counterexamples as a sum of indicator random variables:

$$\mathsf{E} = \sum_{|X|=1}^{k} \binom{n}{|X|} \mathsf{P}\left[|\mathsf{N}(X)| < \gamma |X|\right]$$

[1] At least for the case $\gamma = 1$ this is not a new result, only in most articles the proof is omitted as "it can be shown by standard probabilistic argument".

Let's denote $j = |X|$. For every counterexample $X$, there are at most $\binom{m}{\lfloor \gamma j \rfloor}$ ways of choosing a set $Z$ of cardinality $\lfloor \gamma j \rfloor$ containing all the neighbours of $X$ and for every such $Z$ the probability that all the neighbours lie in $Z$ is $\left(\frac{|Z|}{m}\right)^{jd}$. That bounds $\mathsf{P}\left[|\mathsf{N}(X)| < \gamma j\right]$:

$$\mathsf{E} = \sum_{|X|=1}^{k} \binom{n}{j} \mathsf{P}\left[|\mathsf{N}(X)| < \gamma j\right] \leq \sum_{j=1}^{k} \binom{n}{j} \binom{m}{\lfloor \gamma j \rfloor} \left(\frac{\lfloor \gamma j \rfloor}{m}\right)^{jd}$$

Now, we use standard estimate on binomials and rewrite the term as a power of $e$:

$$\mathsf{E} \leq \sum_{j=1}^{k} \left(\frac{en}{j}\right)^{j} \left(\frac{em}{\lfloor \gamma j \rfloor}\right)^{\lfloor \gamma j \rfloor} \left(\frac{\lfloor \gamma j \rfloor}{m}\right)^{jd} = \sum_{j=1}^{k} e^{j \log\left(\frac{en}{j}\right) + \lfloor \gamma j \rfloor \log\left(\frac{em}{\lfloor \gamma j \rfloor}\right) - jd \log\left(\frac{m}{\lfloor \gamma j \rfloor}\right)}$$

We would also like to get rid of the floor function. As we are bounding $\mathsf{E}$ from above, we can write $-jd \log\left(\frac{m}{\gamma j}\right)$ instead of $-jd \log\left(\frac{m}{\lfloor \gamma j \rfloor}\right)$, as $-jd \log\left(\frac{m}{\gamma j}\right) \geq -jd \log\left(\frac{m}{\lfloor \gamma j \rfloor}\right)$. We would also like to write $j\gamma \log\left(\frac{em}{\gamma j}\right)$ instead of $\lfloor \gamma j \rfloor \log\left(\frac{em}{\lfloor \gamma j \rfloor}\right)$, so we need to prove, that $j\gamma \log\left(\frac{em}{\gamma j}\right) \geq \lfloor \gamma j \rfloor \log\left(\frac{em}{\lfloor \gamma j \rfloor}\right)$. That is indeed true, because function $\beta \log \frac{\alpha}{\beta}$ is non-decreasing function of $\beta$ for $\frac{\alpha}{\beta} \geq e$ (as the derivative is $\log \frac{\alpha}{\beta} - 1$). Substituting $\alpha = em$, $\beta = \lfloor \gamma j \rfloor$ (or $\gamma j$), we get the true condition $m \geq \gamma j \geq \lfloor \gamma j \rfloor$. That gives us following upper bound on $\mathsf{E}$:

$$\mathsf{E} \leq \sum_{j=1}^{k} e^{j\left(\log\left(\frac{en}{j}\right) + \gamma \log\left(\frac{em}{\gamma j}\right) - d \log\left(\frac{m}{\gamma j}\right)\right)}$$

Now, we would like to prove, that the exponent is at most $-j$. Then, we will have $\mathsf{E} \leq \sum_{j=1}^{k} e^{-j} < 1$. That means, that we only need following inequality to hold:

$$\log\left(\frac{en}{j}\right) + \gamma \log\left(\frac{em}{\gamma j}\right) - d \log\left(\frac{m}{\gamma j}\right) \leq -1 \quad \forall j \tag{1.1}$$

Now, we consider both settings of parameter $\gamma$ from the theorem statement and for both of them find appropriate $d$ for which the Inequality 1.1 holds.

Let's start with the case $\gamma \geq \frac{m}{en}$. We put $d$ on the right side and incorporate the $-1$ term to the logarithm:

$$\frac{\log\left(\frac{e^2 n}{j}\right) + \gamma \log\left(\frac{em}{\gamma j}\right)}{\log\left(\frac{m}{\gamma j}\right)} \leq d \quad \forall j$$

Now, we use the fact, that $\log\left(\frac{em}{\gamma j}\right)$ is decreasing with $\gamma$, so by substituting the minimum value of $\gamma = \frac{m}{en}$, we get true inequality $\log\left(\frac{em}{\gamma j}\right) \leq \log\left(\frac{e^2 n}{j}\right)$. So we substitute $\log\left(\frac{e^2 n}{j}\right)$ for $\log\left(\frac{em}{\gamma j}\right)$:

$$\frac{\log\left(\frac{e^2 n}{j}\right) + \gamma \log\left(\frac{e^2 n}{j}\right)}{\log\left(\frac{m}{\gamma j}\right)} = (1+\gamma) \frac{\log\left(\frac{e^2 n}{j}\right)}{\log\left(\frac{m}{\gamma j}\right)} \leq d \quad \forall j$$

And at the end, we realize, that the whole term is increasing with $j$ for $e^2 n \geq \frac{m}{\gamma}$, which is true by the assumption $\gamma \geq \frac{m}{en}$. So we only require the following inequality to hold:

$$(1+\gamma)\frac{\log\left(\frac{e^2 n}{k}\right)}{\log\left(\frac{m}{\gamma k}\right)} \leq d$$

□

For the second case, let $\gamma \leq \frac{m}{en}$. We again rearrange the Inequality 1.1:

$$\log\left(\frac{en}{i}\right) + \gamma \log\left(\frac{em}{\gamma j}\right) - d\log\left(\frac{m}{\gamma j}\right) \leq -1 \quad \forall j \qquad (\text{1.1 revisited})$$

We notice that both the second and the third term are increasing with $\gamma$ so we can substitute $\gamma = \frac{m}{n}$ to the second one (as it is more than the maximum value of $\gamma$) and $\gamma = \frac{m}{en}$ to the third one:

$$\log\left(\frac{en}{j}\right) + \frac{m}{n}\log\left(\frac{en}{j}\right) - d\log\left(\frac{en}{j}\right) \leq -1 \quad \forall j$$

$$\log\left(\frac{en}{j}\right)\left(1 + \frac{m}{n} - d\right) \leq -1 \quad \forall j$$

And as $\log\left(\frac{en}{j}\right) \geq 1$, it is clearly enough to have $d \geq 3$.

□

We would like to prove an analogous statement for the general (non-bipartite) case. However, we can't make a random $d$ regular multigraph by the technique we used for the bipartite case, as we are choosing the source vertices and the target vertices from the same set, so there can be a vertex with a large degree. We make a simple workaround – we construct oriented multigraph with all vertices of outdegree $d_0$, and we prove that the expander property holds for "oriented neighbours". In other words, $u$ is the neighbour of $v$ iff there is an oriented edge from $v$ to $u$. It is easy to see that if we later convert the graph to non-oriented by cancelling the edge orientation, the expander property is preserved, and the average degree $\bar{d} = 2d_0$. Apart from this little workaround, the proof is completely analogous, so we do not repeat it there.

**Theorem 2.** *Let there be positive integers $n, k$ and a real number $\gamma > 0$, such that $n \geq k$ and $n > \gamma k$. If $\gamma \geq \frac{1}{e}$, there is a vertex (k, $\gamma$)-expander with average degree $\bar{d} = 2d_0$ for every integer*

$$d_0 \geq (\gamma+1)\frac{\log\left(\frac{e^2 n}{k}\right)}{\log\left(\frac{n}{\gamma k}\right)}.$$

*If $\gamma \leq \frac{1}{e}$, there is a vertex (k, $\gamma$)-expander with average degree $\bar{d} = 2d_0$ for every integer*

$$d_0 \geq 3.$$

To conclude the section, we present a lower bound for bipartite expanders, which for constant $\gamma$ matches the upper bound. It was noted by Guruswami et al. [2009], and it is based on lower bound on dispersers by Radhakrishnan and Ta-Shma [2000]. We discuss it more in Section 1.3.

**Proposition 3** (Lower bounds on unbalanced vertex expanders)**.** *For every unbalanced vertex expander, if left average degree $\bar{d} \leq \frac{\gamma k}{2}$ and $\gamma k \leq m$, then*

$$d \in \Omega\left(\frac{\log\left(\frac{n}{k}\right)}{\log\left(\frac{m}{\gamma k}\right)}\right).$$

## 1.2 *k*-expanding graphs

**Definition 3** ($k$-expanding graph)**.** *For an integer $k \geq 1$, a multigraph $G$ is $k$-expanding if for every two sets $|S| \geq k$ and $|T| \geq k$ of its vertices, there is an edge connecting a vertex from $S$ with some vertex from $T$.*

The definition can be rephrased as: In multigraph on $n$ vertices, every set of size $k$ has more than $n - 2k$ neighbours. So, it means that contrary to vertex expanders, we only require sufficiently large sets to expand, but we want the expansion to be huge. It also means that $k$-expanding graphs are useful only for large $k$. For example, for $k \approx \sqrt{n}$, we still need $d \approx \sqrt{n}$, so we usually set $k = \frac{n}{c}$ for some constant $c$.

For the bipartite versions, we only require the property to hold for a set $S$ chosen from the left and set $T$ chosen from the right side (again, we talk about the balanced and unbalanced case). We then need $k \leq m$ for the definition to still make sense, so we usually set $k = \frac{m}{c}$ in the unbalanced case.

**Definition 4** (Bipartite $k$-expanding graph)**.** *For integers $n \geq m \geq k \geq 1$, a bipartite multigraph $G$ with left part $[n]$ and right part $[m]$ is $k$-expanding if for every set $|S| \geq k$ of left vertices and set $|T| \geq k$ of right vertices, there is an edge connecting a vertex from $S$ with some vertex from $T$.*

There is a simple probabilistic construction of $k$-expanding graphs by Alon and Pudlák [1994]. Later, in Section 2.4, we show that the construction yields asymptotically optimal results for both the bipartite and the general case. Again, we start with the bipartite one.

**Theorem 4** (Lemma 4.1 in Alon and Pudlák [1994])**.** *For every three integers $n \geq m \geq k$, there is a bipartite $k$-expanding graph with $n$ left and $m$ right vertices and with left degree $d$ for every*

$$d \geq \frac{2m}{k} \log\left(\frac{e\sqrt{nm}}{k}\right).$$

*Proof.* For the case $k = m$, the statement is trivially true, so let $k < m$ for the rest of the proof to avoid dividing by zero. The principle of the proof is the same as in the construction of vertex expanders. We again construct random bipartite multigraph $G$ on $n+m$ vertices, by choosing randomly with replacement

$d$ neighbours in $[m]$ for every vertex $v$ from $[n]$. Again, we show that the expected number of counterexamples in the random graph is smaller than one. There are $\binom{n}{k}\binom{m}{k}$ ways of choosing a set $|S| = k$ of left vertices and set $|T| = k$ of right vertices and for every vertex $v \in S$, the probability it has no edge in $T$ is $(1-\frac{k}{m})^d$.

So we again express the expected value as a sum of indicator random variables and use standard estimate on binomial coefficients.

$$\begin{aligned}\mathsf{E} = \binom{n}{k}\binom{m}{k}\left(\frac{m-k}{m}\right)^{kd} &\leq \left(\frac{en}{k}\right)^k \left(\frac{em}{k}\right)^k \left(\frac{m-k}{m}\right)^{kd} \\ &= \left(\frac{e\sqrt{nm}}{k}\right)^{2k} \left(\frac{m-k}{m}\right)^{kd}\end{aligned}$$

We would like to prove, that $\mathsf{E} < 1$:

$$\left(\frac{e\sqrt{nm}}{k}\right)^{2k} \left(\frac{m-k}{m}\right)^{kd} \stackrel{?}{<} 1$$

As in the construction of vertex expanders, we rearrange the inequality to find the sufficient bound on $d$:

$$\left(\frac{e\sqrt{nm}}{k}\right)^{2} < \left(\frac{m}{m-k}\right)^{d}$$

We take logarithms of both sides:

$$2\log\left(\frac{e\sqrt{nm}}{k}\right) < d\log\left(\frac{m}{m-k}\right)$$

And finally, we use the fact, that $\frac{k}{m} < \log\left(\frac{1}{1-k/m}\right) = \log\left(\frac{m}{m-k}\right)$. This is true, because $\alpha < \log\left(\frac{1}{1-\alpha}\right)$ for every $0 < \alpha < 1$, which in turn follows from a standard estimate $\alpha e^\alpha \geq e^\alpha - 1$. By substituting $\frac{k}{m}$ for $\log\left(\frac{m}{m-k}\right)$, we get the desired sufficient bound on $d$:

$$\frac{2m}{k}\log\left(\frac{e\sqrt{nm}}{k}\right) \leq d$$

□

Now, we would like to prove an analogous bound for the non-bipartite case. We use the same trick as with the vertex expanders – we construct a random directed multigraph with outdegree $d_0$ of every vertex, and after proving the expansion property in the directed case, we cancel the orientation and get $k$-expanding graph with $\bar{d} = 2d_0$. Besides that, the proof is completely the same as for the bipartite case, so we don't repeat it there.

**Theorem 5.** *For every two integers $n \geq k$, there is an $k$-expanding graph on $n$ vertices with average degree $\bar{d} = 2d_0$ for every integer*

$$d_0 \geq \frac{2n}{k}\log\left(\frac{en}{k}\right).$$

## 1.3 Disperser graph

**Definition 5** (Disperser graph)**.** *Let $G$ be a bipartite multigraph with $n$ left and $m$ right vertices and let there be integer $k \leq n$. Graph $G$ is $(k, \varepsilon)$-disperser graph, if every $k$ vertices from the left side have at least $(1-\varepsilon)m$ neighbours.*

Notice, that disperser graphs are just generalization of unbalanced $k$-expanding graphs – every $k$-expanding graph is also $(k, \frac{k}{m})$-disperser graph. That means, among other things, that also the disperser graphs have a high degree for small $k$, so again, we usually choose a $k$ as a fraction of $m$. We talk about the equivalence more in Section 2.4.

The name comes from the fact that disperser graphs are closely connected with disperser function (in fact, they are just graph-theoretic view on that function), which is in turn just a relaxed version of a seeded randomness extractor. These objects are beyond the scope of this thesis; however, only the rapid development of the theory of pseudorandomness (where they belong) in the last years has enabled the existence of explicit construction of superconcentrator of polylogarithmic degree, which we present in Chapter 5. On this topic, we highly recommend the survey *Pseudorandomness* by Vadhan [2012].

Radhakrishnan and Ta-Shma [2000] showed the following upper bound on dispersers:

**Theorem 6** (Thm. 1.10 in Radhakrishnan and Ta-Shma [2000])**.** *For all integers $1 < k \leq n$, $0 < m$ and real $\varepsilon > 0$, there exists a $(k, \varepsilon)$-disperser graph with maximum left degree $d$ for every*

$$d \geq \frac{1}{\varepsilon}\log\left(\frac{en}{k}\right) + \frac{m}{k}\log\left(\frac{e}{\varepsilon}\right).$$

The proof is again by probabilistic construction, and we don't repeat it here, as it doesn't need any modification and is explained in the article in detail. In the same article, they also provide lower bounds matching their construction up to constant factors.

These lower bounds can also be used to prove the lower bound on the unbalanced vertex expander mentioned in Section 1.1. It is easy to see that every $\left(k, \gamma = \frac{m(1-\varepsilon)}{k}\right)$ unbalanced vertex expander is also $(k, \varepsilon)$-disperser graph. That's why the lower bound on unbalanced expander is a direct consequence of the following theorem:

**Theorem 7** (Thm. 1.5 in Radhakrishnan and Ta-Shma [2000])**.** *Let $G$ be a disperser graph with $k < n$ and $\lfloor \bar{d} \rfloor \leq \frac{(1-\varepsilon)m}{2}$. If $\frac{1}{m} \leq \varepsilon \leq \frac{1}{2}$, then*

$$\bar{d} \in \Omega\left(\frac{\log\left(\frac{n}{k}\right)}{\varepsilon}\right),$$

*and if $\varepsilon > \frac{1}{2}$, then*

$$\bar{d} \in \Omega\left(\frac{\log\left(\frac{n}{k}\right)}{\log\left(\frac{1}{1-\varepsilon}\right)}\right).$$

## 1.4 Spectral expanders

**Definition 6** (Random-walk matrix)**.** *Let $G$ be a connected $d$-regular multigraph on $n$ vertices. Let's denote $E(i,j)$ the number of edges between vertices $i$ and $j$. We define the random-walk matrix of $G$ as $\mathcal{M} \in \mathbb{R}^{n \times n}$, where*

$$\mathcal{M}_{i,j} = \frac{E(i,j)}{d}.$$

We point out a few important properties of $\mathcal{M}$:

- $\mathcal{M}$ has $n$ eigenvectors, which form an orthonormal basis.
- A constant vector is an eigenvector of $\mathcal{M}$, the corresponding eigenvalue is 1, and all the other eigenvalues are strictly smaller.
- All eigenvalues of $\mathcal{M}$ have size at least $-1$. There is at most one eigenvalue of size $-1$; it occurs if and only if $G$ is bipartite and it corresponds to an eigenvector with half entries $\alpha$ and half entries $-\alpha$.

The first property follows from the spectral theorem and from the fact that $\mathcal{M}$ is symmetric. The remaining two properties follow from the connectedness of $G$ and from the fact that all the row sums of $G$ equal 1. We leave the proof as an exercise.

**Definition 7** (General spectral expander)**.** *Let $G$ be a connected non-bipartite $d$-regular multigraph and $\mathcal{M}$ be its random-walk matrix. Further, let $|\lambda_1| \geq |\lambda_2| \geq \cdots \geq |\lambda_n|$ be the eigenvalues of $\mathcal{M}$. Then, we denote $\lambda \stackrel{\text{def}}{=} |\lambda_2|$. Graph $G$ is then* spectral $\lambda$-expander*.*

We note that the smaller is the parameter $\lambda$, the better are the expansion properties. That is a bit unintuitive, so the spectral expansion is often expressed in terms of the *spectral gap* $\stackrel{\text{def}}{=} 1-\lambda$ (so the better expanders have a larger spectral gap).

At first sight, spectral expanders don't seem to have anything in common with vertex expanders, and it is not clear why to even call them expanders. However, there is a strong connection to both vertex expanders and $k$-expanding graphs, which we show in Chapter 2. The connection to vertex expanders is based on some interesting properties of spectral expanders concerning random walks – that's why $\mathcal{M}$ is called *random-walk matrix*.

From the properties of $\mathcal{M}$ above, it is clear that the definition would be meaningless for the bipartite graphs, as $\lambda_2$ always equals $-1$, so the spectral gap would always be zero. We leave the bipartite case undefined for now – we define it in Chapter 2 after explaining the connection to random walks.

Spectral expanders are also sometimes defined in the non-normalized form. We can use the adjacency matrix of $G$, so all the row sums of the matrix equal $d$ and all the eigenvalues are $d$-times larger than in our definition. The spectral gap is then defined as $d - \lambda$. We used the normalized version, as it is more suitable for the proofs in Chapter 2.

The main reason for our interest in spectral expanders is, that due to their rather algebraic definition, the situation with lower and upper bounds and explicit

constructions is quite clear. Nilli [1991] proved, that in every $d$-regular multigraph on $n$ vertices, $\lambda_2 \geq 2\frac{\sqrt{d-1}}{d} - o(1)$ (where the $o(1)$ notation is with respect do $n$). Multigraphs, for which this bound is tight, are called *Ramanujan graphs* and there are explicit constructions of these graphs for both general and balanced case (more on the constructions in Chapter 4).

The unbalanced version of spectral expanders does not often occur in literature, and we did not find the bounds anywhere, hence the question mark in the table.

# 2. Relationships between expanders

In this chapter, we introduce a few relationships between different types of expanders. The main reason for doing this is that if we can explicitly construct one type of expander, we would like to either find some way to modify it to get an expander of another type or prove it also has another "expander-like" property (as we promised we will do for spectral expanders). These conversions are hardly lossless – for example, as we mentioned earlier, we can explicitly construct the best possible spectral expanders, and we prove below that every spectral expander is also a vertex expander; however, an explicit construction of optimal vertex expanders is still unknown. The conversions between different types of expanders are summarized in Figure 2.1

## 2.1 Spectral expander → vertex expander

As promised, we now show that good spectral expanders are good vertex expanders. First, we show the connection between spectral expanders and random walks, and we define the bipartite spectral expanders, which we left undefined in Chapter 1. Then, we use the random walks to prove the vertex expander property.

### 2.1.1 Random walks

Consider that we start a walk at one vertex of a connected multigraph. At every step, we choose uniformly at random one of the incident edges, and we move to the next vertex using this edge. Now, we are interested in the number $t$ of steps needed, so the probabilities of us being at any vertex are approximately the same. This quantity $t$ is called the *mixing time* of a graph, and we usually want it to be small.[1]

First, we realize that the random-walk matrix $\mathcal{M}$ tells us for every vertex $v$ the probabilities of moving to either of its neighbours (see Definition 6). In other words, $\mathcal{M}_{i,j}$ is the probability that if we stand at vertex $i$, we will move to vertex $j$ in the next step.

After $k$ steps of a random walk, we can assign to every vertex the probability that we stand at it. That gives us probability distribution $\pi$ on $n$ vertices. If we write $\pi$ as a row vector, we can use the properties of $\mathcal{M}$ to get the distribution after next step, which is simply $\pi\mathcal{M}$, because $(\pi\mathcal{M})_j = \sum_i \pi_i \mathcal{M}_{i,j}$.

Above, we wanted for the probabilities of us being in either vertex to be approximately the same after not too many steps. This can be rephrased: we would like $\pi\mathcal{M}^k$ to converge to uniform distribution with $k$ (and the faster, the better). So we denote by $u$ the row vector with each entry $\frac{1}{n}$ – it represents the uniform distribution on $n$ vertices. Note, that $u\mathcal{M} = u$, as $u$ is constant vector with

[1] Note, that it is intuitively true, that mixing time and expansion properties are somehow connected – if every set of vertices has many neighbours, then mixing will be faster and vice versa.

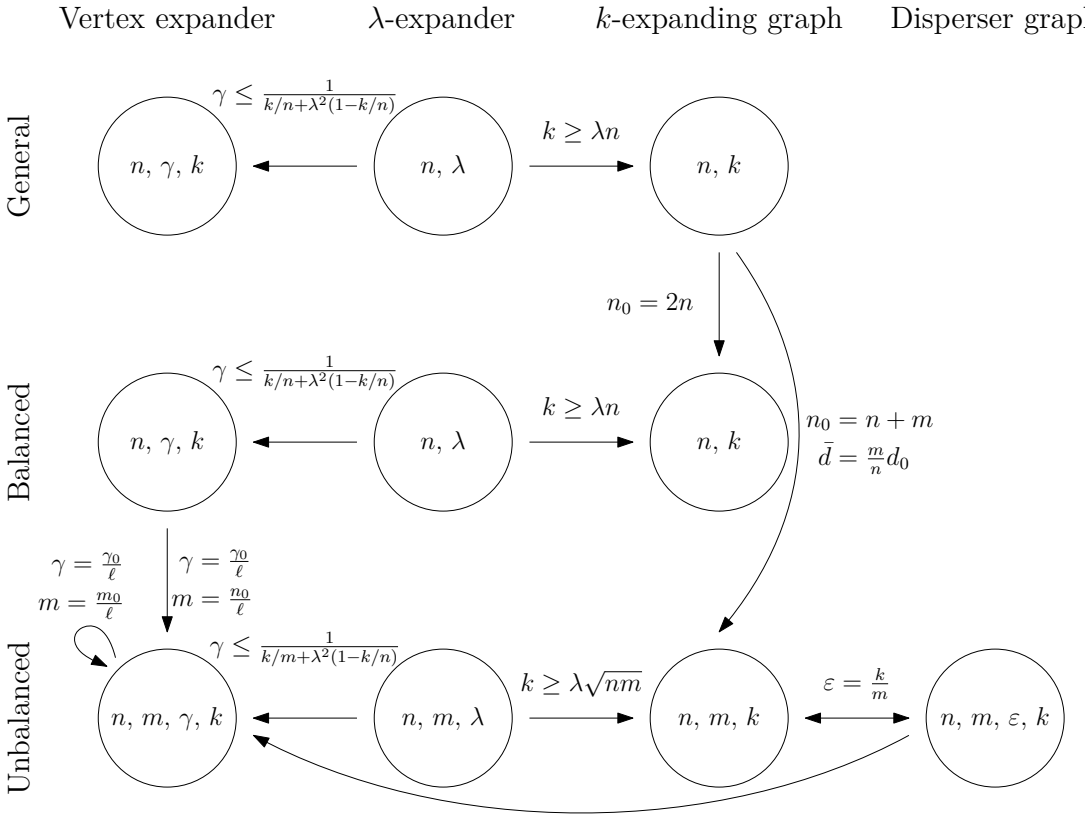


Figure 2.1: Conversions between expanders

eigenvalue 1. Now, we define the following quantity, which expresses our wish of getting closer to uniform distribution with every step (we will call it *convergence rate*).

**Definition 8** (Def. 2.50 in Vadhan [2012])**.** *For a regular multigraph $G$ and its random-walk matrix $\mathcal{M}$,*

$$\lambda(G) \stackrel{\text{def}}{=} \max_{\pi} \frac{\|\pi\mathcal{M} - u\|}{\|\pi - u\|} = \max_{x \perp u} \frac{\|x\mathcal{M}\|}{\|x\|},$$

*where $\|x\|$ is the euclidean norm, the first maximization is over all distributions $\pi$ on $n$ vertices and the second one is over all vectors $x \in \mathbb{R}^n$ orthogonal to $u$.*

The first expression says, how much closer to the normal distribution do we get in one step. To show that the second expression is equivalent, first check that for every $\pi$, $x = \pi - u$ is orthogonal to $u$, so the right maximization is over all the elements from the left one. On the other hand, for every $x \perp u$, the vector $\pi = u + \alpha x$ is a probability distribution for small enough $\alpha$, so the left maximization is over all the elements from the right side and the expressions are equal.

The notation $\lambda(G)$ is not a coincidence; we will now show that the convergence rate equals $\lambda$ from the definition of general spectral expanders (Definition 7).

**Lemma 8** (Lemma 2.55 in Vadhan [2012])**.** *For a regular multigraph $G$ and it's random-walk matrix $\mathcal{M}$,*

$$\lambda = \max_{x \perp u} \frac{\|x\mathcal{M}\|}{\|x\|} = \lambda(G).$$

*Proof.* $\mathcal{M}$ is real symmetric $n \times n$ matrix, so its eigenvectors form the orthonormal basis $v_1, v_2, \ldots, v_n$. As we mentioned earlier, a constant vector is among the eigenvectors (it corresponds to $\lambda_1 = 1$), so without loss of generality, let $v_1$ be the constant vector. Then, every vector $x \perp u$, can be expressed as $x = c_2 v_2 + \cdots + c_n v_n$, and $\langle x, x \rangle = \|x\|^2 = c_2^2 + \cdots + c_n^2$ Then:

$$\begin{aligned} \|x\mathcal{M}\|^2 &= \|\lambda_2 c_2 v_2 + \cdots + \lambda_n c_n v_n\|^2 \\ &= \lambda_2^2 c_2^2 + \cdots + \lambda_n^2 c_n^2 \leq \lambda_2^2 (c_2^2 + \cdots + c_n^2) = \lambda_2^2 \|x\|^2 \end{aligned}$$

The equality occurs for $x = v_2$. So $\lambda = |\lambda_2| = \max_{x \perp u} \frac{\|x\mathcal{M}\|}{\|x\|} = \lambda(G)$

□

**Bipartite cases**

It remains to define the bipartite versions of spectral expanders. The same definition as for general case doesn't work for several reasons. First, as we mentioned earlier, for the balanced case, $\lambda_2$ equals $-1$, so $\lambda$ would always be 1 by our first definition. Second, unbalanced graphs can't be really $d$-regular (left and right degrees must differ), so the row sums in $\mathcal{M}$ wouldn't be equal. And most importantly, the definition of $\lambda(G)$ also wouldn't make sense because it would always be at least 1; just consider uniform distribution on all vertices from one side – after one step, we get uniform distribution on the other side. Therefore we define a different version of the random-walk matrix for bipartite graphs.

**Definition 9** (Bipartite random-walk matrix)**.** *Let $G$ be a connected biregular multigraph with left part $[n]$, right part $[m]$ and left and right degree $d$ and $d'$. Again, let $E(u, v)$ denote the number of edges between vertices $u$ and $v$. For $i \in [n]$ and $j \in [m]$, we define the left bipartite random-walk matrix of $G$ as $\mathcal{A} \in \mathbb{R}^{n \times m}$, where*

$$\mathcal{A}_{i,j} = \frac{E(i,j)}{d},$$

*and the right bipartite random-walk matrix of $G$ as $\mathcal{A}' \in \mathbb{R}^{m \times n}$, where*

$$\mathcal{A}'_{j,i} = \frac{E(j,i)}{d'}.$$

We now alter a bit the rules of the random walk. We start the walk on one side of the graph, and in every step, we move to the other side. That means that after every step, we have a probability distribution on one side of the graph, so we only require to be close to the normal distribution on the current side.

The matrix $\mathcal{A}$ tells us for every vertex $v \in [n]$ the probabilities of moving to either of its neighbours and the matrix $\mathcal{A}'$ tells the same for every vertex $u \in [m]$. That means, that if se start the random walk with distribution $\pi$ on left side, the distribution after another $k$ steps is $\pi(\mathcal{A}\mathcal{A}')^{k/2}$ for even $k$ and $\pi\mathcal{A}(\mathcal{A}'\mathcal{A})^{(k-1)/2}$ for odd $k$.

For the bipartite expanders, we require only the left side of the graph to expand. That's why we define the *left convergence rate*, which expresses how much the graph "mixes" in one step from left to right.

**Definition 10** (Left convergence rate)**.** *For a biregular multigraph $G$ and its left bipartite random-walk matrix $\mathcal{A}$,*

$$\lambda_\ell(G) \stackrel{\text{def}}{=} \max_\pi \frac{\|\pi\mathcal{A} - u_m\|}{\|\pi - u_n\|} = \max_{x \perp u} \frac{\|x\mathcal{A}\|}{\|x\|},$$

*where $u_n$ and $u_m$ are uniform distributions on left and right sides.*

Now, we would like to define the bipartite $\lambda$-expander so that $\lambda$ equals $\lambda_\ell(G)$. It turns out that the right choice is to take the square root of the second eigenvalue of $\mathcal{A}\mathcal{A}^T$ in magnitude. The matrix $\mathcal{M}' \stackrel{\text{def}}{=} \mathcal{A}\mathcal{A}^T$ has similar properties as $\mathcal{M}$:

- $\mathcal{M}'$ has $n$ eigenvectors, which form an orthonormal basis.
- Constant vector is an eigenvector of $\mathcal{M}'$; the corresponding eigenvalue is $\frac{d'}{d}$, and all the other eigenvalues are strictly smaller in magnitude.

We again leave the proof of the properties as an exercise.

**Definition 11** (Tanner [1984])**.** *Let $G$ be a connected biregular multigraph with left and right degrees $d$ and $d'$ and left random-walk matrix $\mathcal{A}$. For the $n \times n$ matrix $\mathcal{A}\mathcal{A}^T$, let's denote its eigenvalues $|\lambda_1| \geq |\lambda_2| \geq \cdots \geq |\lambda_n|$. Then we denote $\lambda \stackrel{\text{def}}{=} \sqrt{|\lambda_2|}$ and we say that $G$ is bipartite spectral $\lambda$-expander.*

It remains to prove, that really $\lambda = \lambda_\ell(G)$. We do it similarly to the general case.

**Lemma 9.** *For a biregular multigraph $G$ and it's left bipartite random-walk matrix $\mathcal{A}$,*

$$\lambda = \max_{x \perp u} \frac{\|x\mathcal{A}\|}{\|x\|} = \lambda_\ell(G).$$

*Proof.* Again the eigenvectors of $\mathcal{A}\mathcal{A}^T$ form the orthonormal basis $v_1, v_2, \ldots, v_n$ with constant vector $v_1$. Then, every vector $x \perp u$, can be expressed as $x = c_2 v_2 + \cdots + c_n v_n$, and $\langle x, x\rangle = \|x\|^2 = c_2^2 + \cdots + c_n^2$ Thus:

$$\|x\mathcal{A}\|^2 = x\mathcal{A}\mathcal{A}^T x = \sum_{i=2} c_i^2 \lambda_i \leq \lambda_2(c_2^2 + \cdots + c_n^2) = \lambda_2 \|x\|^2$$

Again, the equality occurs for $x = v_2$. So $\lambda = \sqrt{|\lambda_2|} = \max_{x \perp u} \frac{\|x\mathcal{A}\|}{\|x\|} = \lambda_\ell(G)$ □

### Note about the definition of balanced spectral expanders

There is an alternative definition of balanced spectral expanders. For the balanced case, $d = d'$, so $A' = A^T$ and the random-walk matrix $\mathcal{M}$ of size $2n \times 2n$ and with eigenvalues $|\lambda_1| \geq |\lambda_2| \geq \cdots \geq |\lambda_{2n}|$ can be defined in the same way as for the general case. Then we can denote $\lambda' = \max_i\{|\lambda_i| : |\lambda_i| < 1\}$. (We already know, that it is equal to $|\lambda_3|$). This definition is usually used in literature (e. g. for the Ramanujan graphs), so the relationships between the two definitions are important to us.

It turns out, that if we define also the right convergence rate $\lambda_r(G)$ in an obvious way, then $\lambda' = \max\{\lambda_\ell(G), \lambda_r(G)\}$, so the alternative definition just expresses both-side expansion. To realize that it is true, consider the matrix $\mathcal{M}^2$. Its $2n$ eigenvalues are exactly the second powers of eigenvalues of $\mathcal{M}$ (corresponding to the same eigenvectors). At the same time, the $2n$ eigenvalues of $\mathcal{M}^2$ exactly correspond to the disjoint union of eigenvalues of $AA^T$ and $A'A'^T = A^TA$.

That means that the alternative definition is stricter, so every balanced spectral $\lambda'$-expander by the alternative definition is also balanced spectral $\lambda$-expander by our definition with $\lambda \leq \lambda'$.

### 2.1.2 Spectral expanders are vertex expanders

As promised, we now present the proof that good spectral expanders are good vertex expanders, using the equivalence between $\lambda$ and the convergence rate. We took the proof from Vadhan [2012] (as Thm. 4.6). He stated it only for the general case, for the bipartite version, see Tanner [1984] (Thm. 2.1).

**Theorem 10.** *For every multigraph $G$, if $G$ is a general spectral $\lambda$-expander, it is also a general vertex $(k, \gamma)$-expander for every $k \leq n$ and*

$$\gamma = \frac{1}{\frac{k}{n} + \lambda^2(1 - \frac{k}{n})}.$$

*If $G$ is a bipartite spectral $\lambda$-expander, it is also a bipartite vertex $(k, \gamma)$-expander for every $k \leq n$ and*

$$\gamma = \frac{1}{\frac{k}{m} + \lambda^2(1 - \frac{k}{n})}.$$

For the proof, we need a simple technical proposition. The proof of the proposition is left as an exercise.

**Definition 12** (Definition 4.7 in Vadhan [2012])**.** *For a probability distribution $\pi$, the* collision probability *of $\pi$ is defined to be the probability that two independent samples from $\pi$ are equal, namely* $\mathrm{CP}(\pi) = \sum_x \pi_x^2$*. The support of $\pi$ is* $\mathrm{Supp}(\pi) \stackrel{\text{def}}{=} \{x : \pi_x > 0\}$.

**Proposition 11** (Lemma 4.8 in Vadhan [2012])**.** *For every probability distribution $\pi \in [0,1]^n$ we have:*

$$\mathrm{CP}(\pi) = \|\pi\|^2 = \|\pi - u\|^2 + \frac{1}{n}, \tag{2.1}$$

*where $u$ is the uniform distribution on $[n]$.*

$$\mathrm{CP}(\pi) \geq \frac{1}{|\mathrm{Supp}(\pi)|}, \tag{2.2}$$

*with equality iff $\pi$ is uniform on* $\mathrm{Supp}(\pi)$.

We state the proof only for the bipartite version; the other versions are completely analogous.

*Proof of Theorem 10 (by Vadhan [2012]).* First, we use the first part of the Proposition 11 on the definition of $\lambda_\ell(G)$, together with the fact that $\lambda = \lambda_\ell(G)$ ($\pi$ is any distribution on left vertices):

$$\mathrm{CP}(\pi\mathcal{A}) - \frac{1}{m} \overset{(2.1)}{=} \|\pi\mathcal{A} - u_m\|^2 \leq \lambda^2 \|\pi - u_n\|^2 \overset{(2.1)}{=} \lambda^2 \left(\mathrm{CP}(\pi) - \frac{1}{n}\right)$$

Now, let $S$ be any subset of the left vertices of size at most $k$ and $\pi$ the uniform distribution on $S$. Then, by the second part of Proposition 11, $\mathrm{CP}(\pi) = \frac{1}{|S|}$ and $\mathrm{CP}(\pi\mathcal{A}) \geq \frac{1}{|\mathrm{Supp}(\pi\mathcal{A})|} = \frac{1}{|\mathsf{N}(S)|}$. After plugging into the inequality, we get:

$$\frac{1}{|\mathsf{N}(S)|} - \frac{1}{m} \leq \lambda^2 \left(\frac{1}{|S|} - \frac{1}{n}\right)$$

$$|\mathsf{N}(S)| \geq \frac{|S|}{|S|\left(\frac{1}{m} - \frac{\lambda^2}{n}\right) + \lambda^2}$$

and after using $k \geq |S|$, we have $|\mathsf{N}(S)| \geq \frac{|S|}{\frac{k}{m} + \lambda^2\left(1 - \frac{k}{n}\right)}$, so $\gamma \geq \frac{1}{\frac{k}{m} + \lambda^2\left(1 - \frac{k}{n}\right)}$.

□

If we now use the theorem on the known spectral expanders with $\lambda = \frac{2}{\sqrt{d}}$, after the substitution we get general or balanced vertex expanders for any

$$d \geq 2\frac{n-k}{\frac{n}{\gamma} - k} \in \Omega\left(\gamma\frac{n-k}{n-\gamma k}\right),$$

whereas from the probabilistic constructions, we got

$$d \in \Omega\left(\gamma\frac{\log n - \log k}{\log n - \log \gamma k}\right).$$

## 2.2 Spectral expander → *k*-expanding graph (Mixing lemma)

There is a well-known claim about spectral expanders called *Expander mixing lemma*, which among others implies, that spectral expanders are also $k$-expanding. We omit the proof, as it is mostly technical; it can be found in a survey by Vadhan [2012] as proof of a Lemma 4.15 (it is again stated only for the general case, but the bipartite version is completely analogous).

**Theorem 12** (Expander mixing lemma)**.** *Let $G$ be a spectral $\lambda$-expander. If $G$ is bipartite, let's take subset $S$ of left vertices, subset $T$ of right vertices and denote $\alpha = |S|/n$, $\beta = |T|/m$. If $G$ is non-bipartite, take any subsets of vertices $S$, $T$ and denote $\alpha = |S|/n$, $\beta = |T|/n$. For both cases, let $e(S,T)$ denote the number of edges between sets $S$, $T$, counting edges in intersection $S \cap T$ twice. Then, the following holds:*

$$\left|\frac{e(S,T)}{nd} - \alpha\beta\right| \leq \lambda\sqrt{\alpha(1-\alpha)\beta(1-\beta)} \leq \lambda\sqrt{\alpha\beta}$$

Note that $\alpha\beta$ is the expected fraction of all edges that goes between $S$ and $T$ in a random graph, whereas $\frac{e(S,T)}{nd}$ is the actual fraction. So the Mixing lemma says that for a good spectral expander, the expected and actual number of edges between $S$ and $T$ is somehow "close". It makes intuitively sense, as we already know, that random graphs are good expanders (for various expander definitions). Mixing lemma goes in the opposite direction – good spectral expanders are similar to random graphs. However, the word *close* is in quotes, as there is a quadratic loss due to the square root on the right side, so in fact, the terms are close only when $|S|, |T|$ are close to $n$. Then, $\alpha$ and $\beta$ are close to 1, and so the square root does not have much effect. This also makes sense in the context of $k$-expanding graphs, about which we already know, that we need $k$ to be large:

**Corollary 13** (Spectral expanders are $k$-expanding)**.** *If for a bipartite spectral $\lambda$-expander $G$ and some integer $0 \leq k \leq m$ it holds*

$$\lambda < \frac{k}{\sqrt{(n-k)(m-k)}},$$

*then $G$ is also $k$-expanding. Particularly, it suffices to have $\lambda \leq \frac{k}{\sqrt{nm}}$, so every $\lambda$ bipartite expander is also $k$-expanding for every $k \geq \lambda\sqrt{nm}$.*

*Analogously, if for a general spectral $\lambda$-expander $G$ and some integer $0 \leq k \leq n$ it holds*

$$\lambda < \frac{k}{n-k},$$

*then, $G$ is also $k$-expanding. Again, every general $\lambda$ expander is therefore $k$-expanding for every $k \geq \lambda n$.*

*Proof.* Let $|S| = |T| = k$. For $k$-expanding graphs, we require $S, T$ to be connected by edge, which is equivalent to $\frac{e(S,T)}{nd} > 0$. For the expression to be positive, it suffices to have its distance from positive number $\alpha\beta$ be smaller than $\alpha\beta$, so we only need $\left|\frac{e(S,T)}{nd} - \alpha\beta\right| < \alpha\beta$. Now, by the Mixing lemma, we just need $\lambda\sqrt{\alpha(1-\alpha)\beta(1-\beta)} < \alpha\beta$. By substitution for $\alpha$ and $\beta$ from definition, we get the corollary. For the weaker bounds $k > \lambda\sqrt{nm}$ and $k > \lambda n$ it suffices to use the rightmost part of the Mixing lemma (so $\lambda\sqrt{\alpha\beta} < \alpha\beta$).

□

If we use the corollary on the balanced spectral expander from Section 1.4, we have $k > \lambda n$ and $\lambda \leq \frac{2}{\sqrt{d}}$, so we get $k$-expanding graph for every $k > \frac{2n}{\sqrt{d}}$. That means that it suffices to have $d \geq \frac{4n^2}{k^2}$. In comparison, we have $\frac{2n}{k}\log\left(\frac{en}{k}\right)$ by the probabilistic method. That means that the degree we got from spectral expanders is less than a second power of the degree from the optimal probabilistic construction, which is quite good. However, for the unbalanced case, we get $d \geq \frac{4nm}{k^2}$, compared to $\frac{m}{k}\log\left(\frac{e\sqrt{nm}}{k}\right)$ probabilistically. So, with a small $m$, the difference can be much larger in the unbalanced case.

## 2.3 General $k$-expanding graph $\rightarrow$ bipartite $k$-expanding graph

There is a simple way of constructing any bipartite $k$-expanding graph from the general one. For a general $k$-expanding graph with $n+m$ vertices and maximum degree $d$, we just arbitrarily split the vertices into two groups of sizes $n \geq m$ (the left and right part) and remove all the edges within the groups. As we require the $k$-expanding property to hold only for $S \subseteq [n]$ and $T \subseteq [m]$, the edges which connected $S$ and $T$ in the original graph were not deleted, as they go between the groups, so we really got bipartite $k$-expanding graph. The maximum degree of the new graph is still $d$, so the average degree on the left side is $\frac{m}{n}d$.

**Proposition 14** (Lemma 4.2 in Wigderson and Zuckerman [1993])**.** *If there is a general $k$-expanding graph on $n+m$ vertices ($n \geq m$) with maximum degree $d_0$, there is also a bipartite $k$-expanding graph with $n$ left and $m$ right vertices with maximum right and left degree $d' = d = d_0$ and average left degree $\bar{d} = \frac{m}{n}d_0$.*

That means, that from the general $k$-expanding graph from Section 1.2 with $\bar{d}_0 = \frac{4n}{k}\log\left(\frac{en}{k}\right)$, we can get bipartite $k$-expanding graph with $\bar{d} = \frac{4m}{k}\log\left(\frac{en}{k}\right)$, which is asymptotically the same as the bound we got by probabilistic construction, which was $d = \frac{2m}{k}\log\left(\frac{e\sqrt{nm}}{k}\right)$.

## 2.4 Disperser graph $\leftrightarrow$ bipartite $k$-expanding graph

The connection between disperser graphs and $k$-expanding graphs is quite simple. Recall that in $(k, \varepsilon)$-disperser graph, every set $|S| \geq k$ of left vertices has at least $(1-\varepsilon)m$ neighbours. In bipartite $k$-expanding graphs, every set $|S| \geq k$ of left vertices shares an edge with every set $|T| \geq k$ of right vertices. So, in other words, $S$ has at least $m-k$ neighbours. It means that bipartite $k$-expanding graphs are just special case of disperser graphs:

**Proposition 15.** *Every bipartite $k$-expanding graph is also $(k, \varepsilon = \frac{k}{m})$-disperser graph. Every $(k, \varepsilon)$-disperser with $\varepsilon \leq \frac{k}{m}$ is also bipartite $k$-expanding graph.*

If we compare the probabilistic upper bounds for $\varepsilon = \frac{k}{m}$, the bound for $k$-expanding graphs is $\frac{2m}{k}\log\left(\frac{e\sqrt{nm}}{k}\right)$ whereas for the disperser graph we have $\frac{m}{k}\left(\log\left(\frac{en}{k}\right) + \log\left(\frac{em}{k}\right)\right) = \frac{2m}{k}\log\left(\frac{e\sqrt{nm}}{k}\right)$, so the sizes are exactly the same. This is interesting, as we already know, that the bound on disperser graphs is asymptotically optimal, so it implies, that the probabilistic construction of bipartite $k$-expanding graphs from Section 1.2 is also asymptotically optimal.

In Section 2.3, we showed that from the general $k$-expanding graph from Section 1.2, we can get bipartite $k$-expanding graph with the asymptotically same size as from the probabilistic construction, so it follows that the probabilistic construction of general $k$-expanding graph is also asymptotically optimal.

## 2.5 Disperser graph → unbalanced vertex expander

We now show a technique of constructing an unbalanced vertex expander from a disperser graph. It was invented by Wigderson and Zuckerman [1993], and it is important to us because both best known explicit a non-explicit depth-2 superconcentrator constructions are based on the same idea.

Disperser graphs are somehow opposite to unbalanced vertex expanders – for disperser graphs, every set of size *at least* $k$ expands, so it covers most of the right part, whereas, for vertex expanders, every set of size *at most* $k_v$ expands, so it gets $\gamma$ times bigger. Therefore, we need a sequence of disperser graphs with different parameters $k$ and different sizes $m$ of the right part – the resulting vertex expander will be a union of these disperser graphs. Particularly, for every $S \subseteq [n]$ of size $|S| \leq k_v$, we will need to have some disperser graph with $k \leq |S|$ and $(1-\varepsilon)m \geq \gamma |S|$. That ensures that every $S \leq k_v$ can expand $\gamma$ times through one of the disperser graphs.

### The construction

Formally, we will construct unbalanced vertex $(k_v, \gamma)$-expander $U$ with $n$ left vertices $m_v$ right vertices and maximum left degree $d_v$ as follows. Let $D_0, D_1, \ldots, D_\ell$ be sequence of disperser graphs, where $D_i$ is $(k_i, \varepsilon_i)$-disperser graph with $n$ left vertices, $m_i$ right vertices and maximum left degree $d_i$. Further, let $m_0 \leq m_1 \leq \cdots \leq m_\ell = m_v$, and let $1 = k_0 \leq k_1 \leq \cdots \leq k_\ell \leq k_v \stackrel{\text{def}}{=} k_{\ell+1}$. The resulting vertex expander $U$ is a union of all the disperser graphs $D_i$ obtained by identifying the left side of disperser $D_i$ with the left side of $U$ and the right side of $D_i$ with the first $m_i$ vertices of the right side of $U$. The set of edges of $U$ is disjoint union of all edges of all the disperser graphs (so $d_v = \sum_{i=0}^{\ell} d_i$). The construction is shown in Figure 2.2.

Now, let $S \subseteq [n]$ and $|S| \leq k_v$. There must be some $i$ so that $k_i \leq |S| \leq k_{i+1}$. We need to ensure, that $\mathsf{N}(S) \geq \gamma |S|$. By the properties of $d_i$, we know, that $\mathsf{N}(S) \geq m_i(1-\varepsilon_i)$ and because $k_{i+1} \geq |S|$, it is enough to require:

$$m_i(1-\varepsilon_i) \geq \gamma k_{i+1} \; \forall i \in \{0, \ldots, \ell\}.$$

**Proposition 16.** *If there is a sequence of disperser graphs $D_0, D_1, \ldots, D_\ell$ so that $D_i$ is a $(k_i, \varepsilon_i)$-disperser graph with $n$ right and $m_i$ left vertices and degree $d_i$ and $m_0 \leq m_1 \leq \cdots \leq m_\ell \stackrel{\text{def}}{=} m_v$, $1 = k_0 \leq k_1 \leq \cdots \leq k_\ell \leq k_v \stackrel{\text{def}}{=} k_{\ell+1}$ and*

$$m_i(1-\varepsilon_i) \geq \gamma k_{i+1} \; \forall i \in \{0, \ldots, \ell\},$$

*then, there is also an unbalanced vertex $(k_v, \gamma)$-expander with $n$ left and $m_v$ right vertices and with left degree $d_v = \sum_{i=0}^{\ell} d_i$*

### Use with optimal dispersers

Let's now try this technique with optimal disperser graphs from Chapter 1. For simplicity, we set $\gamma = 1$ and $\varepsilon_i = \varepsilon$ for all $i$ (and we also omit the ceiling function). We have:

$$d_i = \frac{1}{\varepsilon} \log\left(\frac{en}{k_i}\right) + \frac{m_i}{k_i} \log\left(\frac{e}{\varepsilon}\right)$$

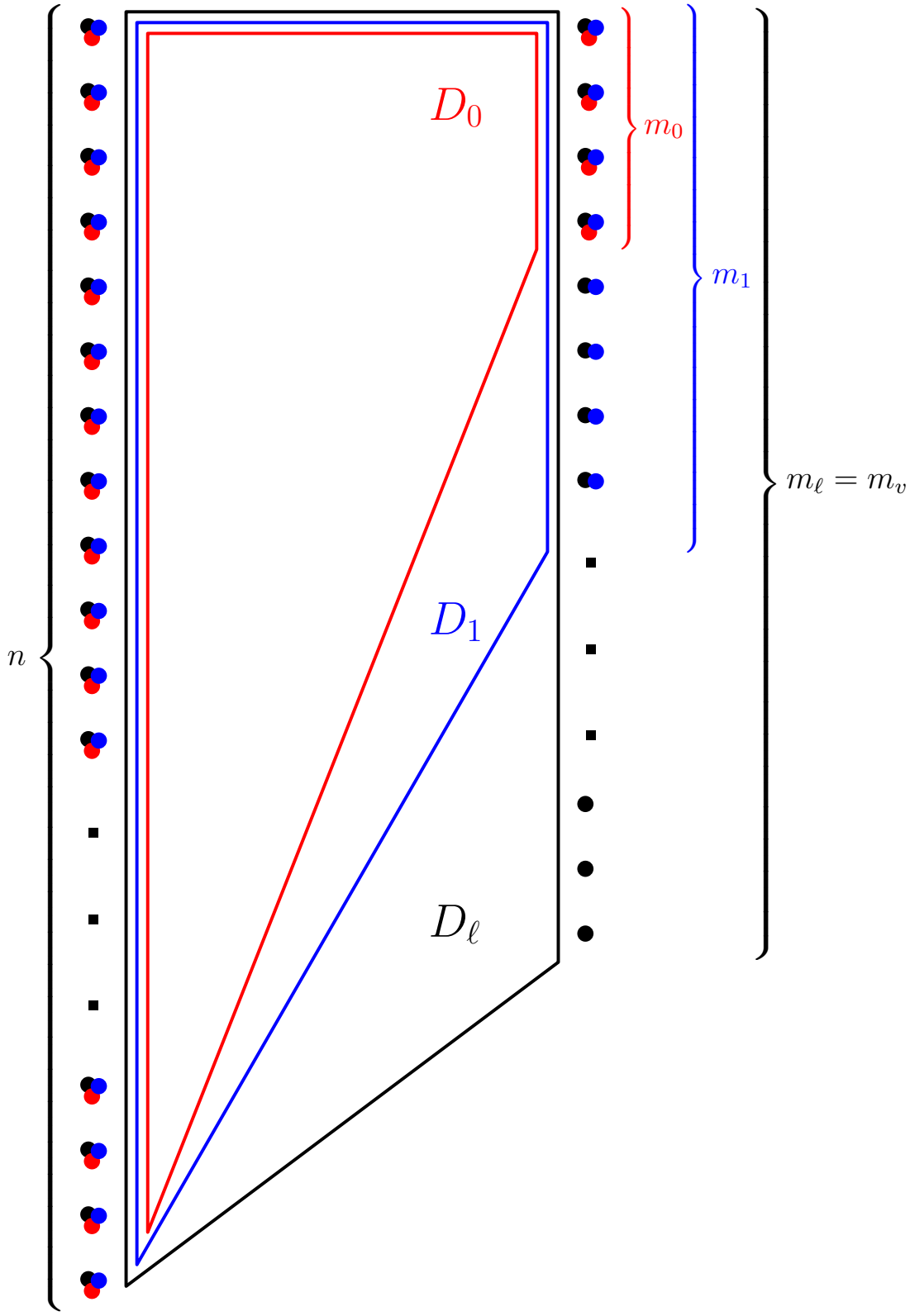


Figure 2.2: Construction of an unbalanced vertex expander from $\ell$ disperser graphs

After substitution for $m_i = \frac{k_{i+1}}{1-\varepsilon}$ (from the main condition of the proposition), we get

$$d_i = \frac{1}{\varepsilon}\log\left(\frac{en}{k_i}\right) + \frac{k_{i+1}}{k_i(1-\varepsilon)}\log\left(\frac{e}{\varepsilon}\right)$$

We now choose $k_i = \log^i(k_v)$ and substitute:

$$d_i = \frac{1}{\varepsilon}\log\left(\frac{en}{\log^i(k)}\right) + \frac{\log(k)}{1-\varepsilon}\log\left(\frac{e}{\varepsilon}\right)$$

We have $k_v = k_{\ell+1} = \log^{\ell+1}(k_v)$, so $\ell = \frac{\log(k)}{\log(\log(k))} - 1$. Then we can calculate degree $d$:

$$\sum_{i=0}^{\ell} d_i \leq \frac{\log(k)}{\log(\log(k))}\left(\frac{\log(en)}{\varepsilon} + \frac{\log(k)\log\left(\frac{e}{\varepsilon}\right)}{1-\varepsilon}\right) - \frac{\log(\log(k))}{\varepsilon}\sum_{i=0}^{\ell} i =$$
$$= \frac{\log(k)}{\log(\log(k))}\left(\frac{\log(en) - \frac{1}{2}\log(k) + \frac{1}{2}\log(\log(k))}{\varepsilon} + \frac{\log(k)\log\left(\frac{e}{\varepsilon}\right)}{1-\varepsilon}\right)$$

Assuming $\varepsilon$ is constant, we get $d \in \mathcal{O}\left(\frac{\log(k)\log(n)}{\log(\log(k))}\right)$. Note, that this is not optimal, as for $\gamma = 1$ and $\frac{m}{k}$ constant, optimal probabilistic construction from Chapter 1 yields $d \in \mathcal{O}\left(\log\frac{n}{k}\right)$.

## 2.6 Balanced vertex expander → unbalanced vertex expander

We conclude this chapter with a simple tradeoff between $\gamma$ and $m$ in bipartite vertex expanders. We just take bipartite vertex $(k_b, \gamma_b)$-expander with $n \geq m_b$ and "shrink" its right side $\ell$-times. The resulting unbalanced expander has right side of size $m = \frac{m_b}{\ell}$, expansion factor $\gamma = \frac{\gamma_b}{\ell}$ and $k = k_b$. For $m_b = n$, this can be used to construct unbalanced vertex expander from balanced vertex expanders.

Formally, let there be bipartite vertex $(k_b, \gamma_b)$-expander with left part of size $n$ and right part of size $m_b = m\ell \leq n$. Let's divide the right vertices into $m$ groups of size $\ell$ and for every group, join all its vertices into one, so the resulting graph has $m$ right vertices. And finally, let's keep all the edges, so the maximum left degree stays the same.

If we now choose set $|S| \leq k$ of left vertices, it had at least $\gamma_b |S|$ neighbours in the original graph, so by the pigeonhole principle it had some neighbour in at least $\frac{\gamma_b|S|}{\ell}$ groups, so it has at least $\frac{\gamma_b|S|}{\ell}$ neighbours in the new graph. That proves, that the new graphs with $n$ left and $m$ right vertices is unbalanced vertex $(k = k_b, \gamma = \frac{\gamma_b}{\ell})$-expander.

**Proposition 17.** *If there is a bipartite vertex $(k, \gamma)$-expander with $n$ left and $m\ell$ right vertices, there is also an unbalanced vertex $(k, \frac{\gamma}{\ell})$-expander with $n$ left and $m$ right vertices.*

We note that we took this construction from article *Self-routing superconcentrators* (Pippenger [1996]); however, Pippenger, instead of shrinking one bipartite

expander, composes $\ell$ bipartite expanders by identifying the right sides and taking a disjoint union of the left sides. This method results in $\ell$-times smaller $k$ than in our construction. It is probably because he only needed $\ell = 2$, so the difference was not important.

Let's again try to use this construction to get unbalanced vertex expander with $\gamma = 1$ from the balanced vertex expander from Section 1.1. Recall that there is balanced expander for every $d \geq \frac{(\gamma_b+1)\log(en/k)}{\log(n/\gamma_b k)}$. We will construct unbalanced expander with $\gamma = 1$ and $m = \frac{n}{\ell}$, so we need to set $\gamma_b = \ell$. After substitution, we get $d \geq (\ell + 1)\frac{\log(en/k)}{\log(m/k)}$, which is $(\ell + 1)$ times worse then the probabilistic construction. From that, we can see, that the construction works fine for constant $\ell$ and is useless for $\ell$ close to $n$.

# 3. Non-explicit superconcentrator constructions

In this chapter, we present known constructions of bounded-depth superconcentrators of asymptotically optimal size for every depth $h$ and also a construction of a linear-size superconcentrator of asymptotically optimal depth. In all the constructions, we use upper bounds on sizes of expanders from Chapter 1, which were mostly achieved by non-explicit methods, and so the superconcentrator constructions are also non-explicit.

We start the chapter with definitions of networks and some functions needed for determining the sizes of the superconcentrators. In the second section, we present the lower bounds for the sizes of all bounded-depth superconcentrators. In the third section, we recall some useful expanders from previous chapters and then, in section 3.4 we finally present the constructions.

To keep the constructions simple and clear, we determine the sizes of superconcentrators only asymptotically, and we also omit the ceiling function in this and the next chapter.

## 3.1 Definitions

### 3.1.1 Networks

**Definition 13** (Network)**.** *An $(n : m)$-network is a directed acyclic multigraph with $n$ vertices with zero indegree labeled as inputs and $m$ vertices with zero outdegree labeled as outputs.*

We sometimes refer to the vertices in a network that are not labeled as inputs or outputs as *middle vertices*. It is also sometimes useful to think of the network as layered. For us, *level* of a vertex $v$ will be the length of the *longest* directed path from some input to $v$. We refer to all the vertices of a certain level as a *layer*. The *depth* of a network is the length of the longest directed path in the network, so it corresponds to the highest layer. The *size* of a network is the number of its edges.

In all networks in this thesis, the inputs have always level 0 (so there are no paths between them), and the outputs are always all on the highest level.

Following Pinsker [1973], we define some operations on networks (see Figure 3.1):

**Inversion**
: The inversion $\overline{X}$ of a network $X$ is obtained by reversing the direction of all the edges and switching inputs and outputs.

**Multiplication**
: Let $X$ and $Y$ be networks of depths $h_x$, $h_y$ and sizes $s_x$ $s_y$, where the number of outputs of $X$ equals the number of inputs of $Y$ (and $X, Y$ has no common vertices). Then, $Z \stackrel{\text{def}}{=} X \times Y$ is the network of depth $h_x + h_y$ and size $s_x + s_y$

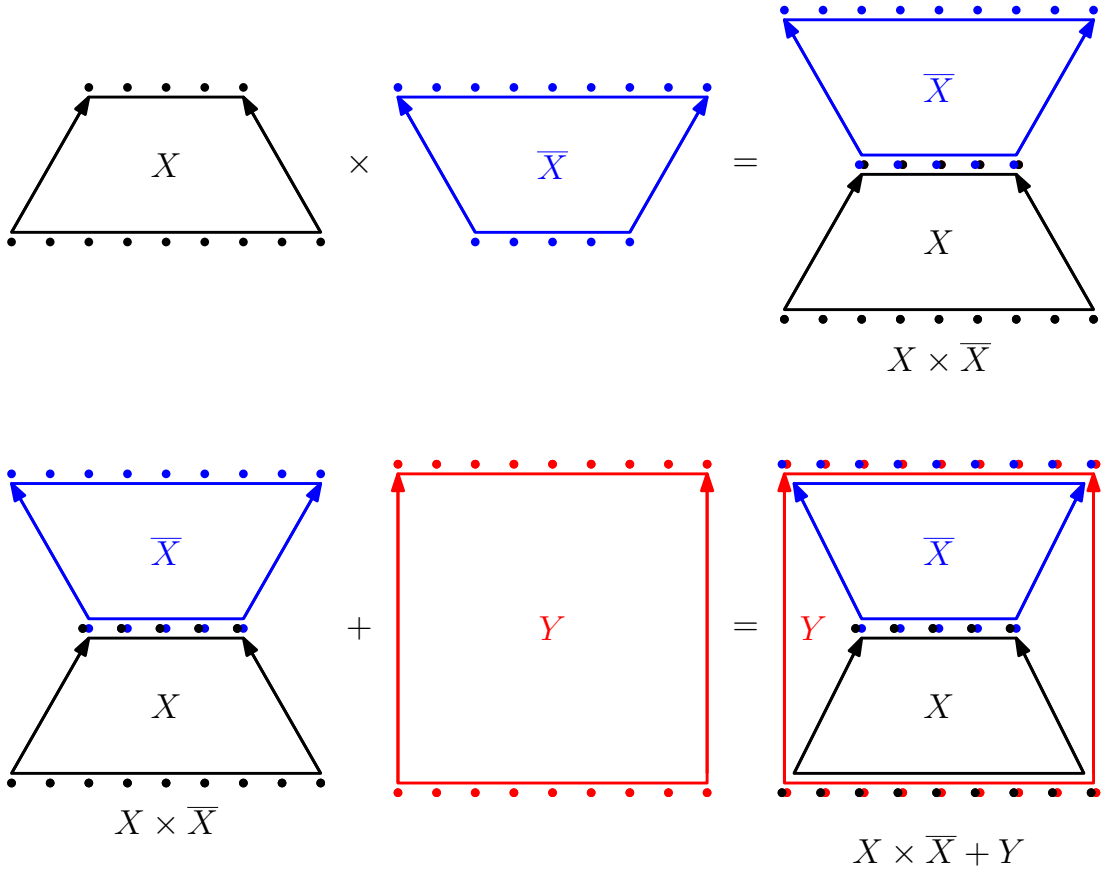


Figure 3.1: Operations on networks

obtained by identifying the outputs of $X$ with the inputs of $Y$ and taking a disjoint union of all the remaining vertices and edges.

**Addition**

Let $X$ and $Y$ be both $(n : m)$-networks of depths $h_x$, $h_y$ and sizes $s_x$ $s_y$ (again with no common vertex). Then $Z \stackrel{\text{def}}{=} X + Y$ is the network of depth $\max(h_x, h_y)$ and size $s_x + s_y$ obtained by identifying inputs of $X$ with inputs of $Y$, outputs of $X$ with outputs of $Y$ and taking disjoint union of all the remaining vertices and edges.

**Definition 14** (Superconcentrator)**.** *An $(n : n)$-network is a* superconcentrator *if, for every set of $k$ inputs $X$ and every set of $k$ outputs $Y$, the number of directed vertex-disjoint paths from $X$ to $Y$ is at least $k$.*

We will shorten "Superconcentrator(s)" to "SC(s)" for the rest of the thesis.

As the title suggests, we are mostly interested in SCs of limited depth and the smallest possible size. We will often think of the superconcentrator property as "handling requests" – we have $k$ requests on both sides of the SC, and we handle them by connecting them through vertex-disjoint paths. We denote $\mathsf{SC}_h(n)$ a SC with $n$ inputs and depth $h$. The smallest possible size of the SC is then $|\mathsf{SC}_h(n)|$.

A weakening of SCs, that we need for the constructions are *partial superconcentrators*. We shortly refer to them as partial SC(s).

**Definition 15** (Partial superconcentrator)**.** *An $(n : n)$-network is a partial $(p, q)$-superconcentrator if for every $k \leq p$ and every set of $k$ inputs $X$ and every set of $k$ outputs $Y$, the number of directed vertex-disjoint paths from $X$ to $Y$ is at least $k - q$.*

We denote partial $(p, q)$-superconcentrator of depth $h$ and with $n$ inputs as $\mathsf{SC}_h(n, p, q)$. It means, that $\mathsf{SC}_h(n) = \mathsf{SC}_h(n, n, 0)$. We denote $|\mathsf{SC}_h(n, p, q)|$ the smallest possible size of the partial SC.

Note that for $k \leq q$, the condition is always met. That means that we are only interested in the behavior of the network for $p \geq k > q$.

**Definition 16** (Concentrator)**.** *An depth-$h$ $(n : m)$-network for $n \geq m$ is $k$-concentrator, denoted by $\mathsf{C}_h(n : m, k)$, if for every set $|S| \leq k$ of inputs there are $|S|$ vertex-disjoint paths from $S$ to some $|S|$ outputs.*

All concentrators in this thesis have depth 1, so we omit this fact later and just denote them "concentrators" instead of "depth-1 concentrators". In the depth-1 case, the vertex-disjoint paths correspond to edges, so the definition says we have a matching of $S$ inputs to some outputs. As the SCs are symmetric and the concentrators are not, we usually need also the inverse $\overline{\mathsf{C}_1(n : m, k)}$ for the constructions. Again, we denote $|\mathsf{C}_1(n : m, k)|$ the smallest possible size of a concentrator.

### 3.1.2 Slowly growing functions

To determine the sizes of bounded-depth SCs, we need to define a family of functions with low enough growth rate. The same definition was used by Pudlák [1994] (who proved the optimal lower bounds) and by Dolev et al. [1983], who constructed the upper bounds.

For a function $f$, and integer $i \geq 0$ let's denote $f^{(i)}(x)$ an $i$-th iteration of $f$, so that $f^{(0)}(x) = x$, and $f^{(i+1)}(x) = f(f^{(i)}(x))$. Further, for function $g$, let $g^*(x) = \min_{i \geq 0}\{i : g^{(i)}(x) \leq 1\}$.

**Definition 17** (Inverse Ackermann function)**.** *Let $\lambda_i(j)$ be a family of functions defined for all non-negative integers as follows: $\lambda_0(j) = \left\lceil \frac{j}{2} \right\rceil$, and otherwise $\lambda_i(j) = \lambda^*_{i-1}(j)$.*

It's easy to see that $\lambda_0 \approx \frac{x}{2}$, $\lambda_1 \approx \log_2 x$, $\lambda_2 \approx \log^*_2 x$, and so on.

To determine the depth of a linear-size SC, we need a function $\beta$, which grows even more slowly.

**Definition 18.** *For all integers $i \geq 1$, $x \geq 1$:*

$$\beta(x) = \min_{i \geq 0}\{i : \lambda_i(x) \leq i\}$$

For the proofs, we also need the Ackermann function. There exist several definitions; this one is originally by Tarjan [1975] and was used by Dolev et al. [1983] (from whom we use the constructions of optimal SCs for all $h \geq 4$).

**Definition 19** (Ackermann function)**.** *Let $\mathsf{A}_i(j)$ be a family of functions defined for all non-negative integers $i$, $j$ as follows: $\mathsf{A}_0(j) = 2j$, and otherwise $\mathsf{A}_i(j) = \mathsf{A}^{(j)}_{i-1}(1)$.*

In the proofs, we also use a few properties of these functions:

$$\lambda_2(x) \approx \log_2^* x;\ \mathsf{A}_2(x) = 2^x \tag{3.1}$$

$$\lambda_i(\mathsf{A}_i(x)) = x;\ \mathsf{A}_i(\lambda_i(x)) \geq x \tag{3.2}$$

The Property 3.1 is immediate from the definitions. The Property 3.2 follows from the fact, that $\lambda_i$ is discrete inverse of $\mathsf{A}_i$. In other words, $\lambda_i(x) = \min_{j\geq 0}\{j : \mathsf{A}_i(j) \geq x\}$. This can be easily proved by induction – the base case $i = 0$ is true, and for the induction step:

$$\begin{aligned}\lambda_i(x) = \lambda^*_{i-1}(x) = \min\{j : \lambda^{(j)}_{i-1}(x) \leq 1\} &\overset{\text{ind}}{=} \\ &\overset{\text{ind}}{=} \min\{j : A^{(j)}_{i-1}(1) \geq x\} = \min\{j : A_i(j) \geq x\}\end{aligned}$$

Note that this also implies, that $\beta$ is so called "diagonal function" of $\mathsf{A}$: $\beta(x) = \min\{j : \mathsf{A}_j(j) \geq x\}$.

## 3.2 Lower bounds

We mention there the known lower bounds on sizes of SCs for every constant depth and also a lower bound on the depth of a SC of linear size. In Section 3.4, we will show constructions of all these SCs that match the lower bound up to constant factors. That's how we know that both the lower bounds and the constructions are asymptotically optimal. The optimal sizes are summarized in Table 3.1.

The SC of depth 1 is trivial as it is just a complete bipartite graph. Pudlák [1994] developed a nice general framework for proving lower bounds on different communication circuits, which yields asymptotically optimal lower bound for every SC of depth $h \geq 3$. Moreover, his bounds work also for partial SCs.

**Theorem 18** (Thm. 3 in Pudlák [1994])**.** *For every constant $h \geq 2$, for every two positive integers $n \geq r$,*

$$\begin{aligned}\left|\mathsf{SC}_3\left(n, n, \frac{n}{r}\right)\right| &\in \Omega(n \log\log r),\\ \left|\mathsf{SC}_{2h}\left(n, n, \frac{n}{r}\right)\right| &\in \Omega(n\, \lambda_h(r)),\\ \left|\mathsf{SC}_{2h+1}\left(n, n, \frac{n}{r}\right)\right| &\in \Omega(n\, \lambda_h(r)).\end{aligned}$$

Note that by substituting $r = n$, we get $\mathsf{SC}_i\,(n, n, 1)$, which can be easily modified to $\mathsf{SC}_i\,(n, n, 0) = \mathsf{SC}_i\,(n)$ by adding one special vertex $v$ and edge from every input to $v$ and from $v$ to every output. This doesn't change the asymptotic size, so we use this fact also further in construction and omit the last one request, as it can be easily handled without asymptotic change in size.

Also note that for $h = 2$ Pudlák [1994] got lower bound $n \log n$, and soon, he improved it to $n \log^{3/2} n$ by different technique (Alon and Pudlák [1994]).

The asymptotically optimal lower bound for $h = 2$ was found by Radhakrishnan and Ta-Shma [2000] using lower bounds on disperser graphs mentioned in Section 1.3, which in turn are a consequence of the upper bound on *the Zarankiewicz problem* by Kövari et al. [1954] known as Kővári-Sós-Turán theorem.

| Depth[a] | Size |
|---|---|
| 2 | $\Theta\left(n\frac{\log^2 n}{\log\log n}\right)$ |
| 3 | $\Theta\left(n\log\log n\right)$ |
| $2h$<br>$2h+1$ | $\Theta\left(n\,\lambda_h(n)\right)$ |
| $\Theta\left(\beta(n)\right)$ | $n$ |

[a]For all integers $h \geq 2$

Table 3.1: Optimal sizes of superconcentrators of different depths

**Theorem 19** (Thm. 1.1 in Radhakrishnan and Ta-Shma [2000])**.** *For every positive integer $n$,*

$$\left|\mathsf{SC}_2\left(n\right)\right| \in \Omega\left(n\frac{\log^2 n}{\log\log n}\right).$$

The lower bound for depth of a linear-size superconcentrator was found by Dolev et al. [1983] and it uses the even slower growing function $\beta$:

**Theorem 20** (Corollary 2.2 in Dolev et al. [1983])**.** *For every postitive integer $n$,*

$$\left|\mathsf{SC}_{h(n)}\left(n\right)\right| \in \mathcal{O}\left(n\right) \Rightarrow h(n) \in \Omega\left(\beta(n)\right).$$

## 3.3 Useful bipartite expanders

Now, let's recall a few important tools from previous chapters.

For any unbalanced vertex expander with $\gamma = 1$, we can direct the edges from left to right to obtain $\mathsf{C}_1\left(n:m,k\right)$. That's true, because according to Hall's marriage theorem, the matching of any $|S| \leq k$ inputs to some outputs (from definition of a concentrator) exists iff every subset $S' \subseteq S$ of size $i$ has at least $i$ neighbours in $m$. That is guaranteed by the vertex expander property. Using the upper bound on unbalanced vertex expanders, we get the following proposition:

**Proposition 21.**

$$\left|\mathsf{C}_1\left(n:m,k\right)\right| \in \mathcal{O}\left(n\frac{\log\left(\frac{n}{k}\right)}{\log\left(\frac{m}{k}\right)}\right)$$

A *balanced $k$-expanding graph* is a bipartite multigraph, in which every pair of subsets $|S| \geq k$ of left vertices and $|T| \geq k$ of right vertices is connected by an edge. There are balanced $k$-expanding graphs of size $\mathcal{O}\left(\frac{n^2}{k}\log\left(\frac{n}{k}\right)\right)$.

Let's realize that if we direct all the edges from left to right, $k$-expanding graphs correspond to $\mathsf{SC}_1\left(n,n,k\right)$. To prove it by contradiction, let there be a set $|S| = i > k$ of left vertices (inputs) with less than $i-k$ neighbours (distinct neighbours correspond to vertex-disjoint paths in depth-1 networks). Then, the subset $T$ of right vertices (outputs) with no neighbour in $S$ has size $|T| > n-(i-k) > k$,

which contradicts the $k$-expanding property. So, the graph is really $\mathsf{SC}_1(n, n, k)$ and so the following proposition holds.

**Proposition 22.**

$$|\mathsf{SC}_1(n, n, q)| \in \mathcal{O}\left(\frac{n^2}{q}\log\left(\frac{n}{q}\right)\right)$$

A *(k, ε)-Disperser graph* is a bipartite multigraph with left and right part sizes $n, m$, so that every set of left vertices of size at least $k$ has at least $(1-\varepsilon)m$ neighbours. For constant epsilon, there are disperser graphs of size $\mathcal{O}\left(\log\left(\frac{n}{k}\right) + \frac{m}{k}\right)$. For the purpose of the constructions, we direct the edges in disperser graph from left to right to form *disperser network* $\mathsf{D}_1(n : m, \varepsilon, k)$.

**Proposition 23.** *For ε constant,*

$$|\mathsf{D}_1(n : m, \varepsilon, k)| \in \mathcal{O}\left(n\left(\log\left(\frac{n}{k}\right) + \frac{m}{k}\right)\right).$$

## 3.4 The Constructions

### 3.4.1 General construction for all depths

We start with the general construction by Dolev et al. [1983], which yields asymptotically optimal results for all depths greater than three. In fact, for every $h \geq 2$, we construct the partial SCs from Theorem 18, which satisfies $\left|\mathsf{SC}_{2h}\left(n, n, \frac{n}{r}\right)\right| \in \mathcal{O}(n\,\lambda_h(r))$ (and we omit the last one request, as explained above).

For the construction, we need two types of concentrators. For the construction of depth-2 SC, we need a concentrator with $k = \frac{3}{4}m$ of size $\mathcal{O}(n \log r)$ and for the recursive construction of SCs of the remaining depths from the depth-2 SC, we need a linear concentrator with $m = \frac{n}{r}$ and $k = \frac{n}{r^2}$. The sizes are guaranteed by the Proposition 21.

Note that the constants in the concentrators are not important – in the first concentrator we can have any real from $\left(\frac{1}{2}, 1\right)$ instead of $\frac{3}{4}$ and its size could be $\mathcal{O}(n \log^\alpha r)$ for any positive constant $\alpha$. In the second concentrator, we can have any positive integer instead of 2 in the term $r^2$.

#### Overview of the construction

Let's summarize the construction before we go into the details.

To construct a depth-2 SC, we take a product of a concentrator and its inverse to form a depth-two $(n, n)$-network with small middle layer of size $m \leq n$ with $k = \frac{3}{4}m$. We use the concentrators to concentrate at most $k$ requests from both sides of the network to the small middle layer. If we pair all requests which meet each other in the middle layer, there can remain only at most $\frac{m}{2}$ unhandled requests on each side. So, for $k = \frac{3}{4}m$, we leave at most $\frac{2}{3}k$ of requests unhandled. Using this trick twice, we build $\mathsf{SC}_2\left(n, \frac{n}{r}, \frac{n}{2r}\right)$ of size $\mathcal{O}(n \log r)$.

Then, by taking sum of $\log_2 s$ instances of this SC for every $r = 2^i$, we build $\mathsf{SC}_2\left(n, n, \frac{n}{s}\right)$ of size $\mathcal{O}\left(n \log^2 s\right)$. This size is close enough to optimum

for the rest of the construction to work (any power of $\log_2 s$ would suffice, as mentioned earlier).

Then, from the almost-optimal depth-2 SC and the linear concentrator, we build linear $\mathsf{SC}_4\left(n, \frac{n}{t}, \frac{n}{2^t}\right)$. The trick for this construction is to first use the linear concentrator and its inverse to concentrate the requests from both sides to layers of size $\frac{n}{\sqrt{t}}$ and then use the one almost-optimal $\mathsf{SC}_2\left(\frac{n}{\sqrt{t}}, \frac{n}{\sqrt{t}}, \frac{n}{t^4}\right)$ of size $\mathcal{O}\left(\frac{n}{\sqrt{t}} \log^2\left(t^{7/2}\right)\right) \subseteq \mathcal{O}(n)$ in the middle. Again, we must use this trick twice and take the sum of the results to achieve the desired partial SC.

As in the depth-2 construction, we can now take sum of $\lambda_2(u) \approx \log_2^* u$ instances of such partial SC for every $t = 1, 2, 2^2, 2^{2^2}, 2^{2^{2^2}} \ldots$ to get $\mathsf{SC}_4\left(n, n, \frac{n}{u}\right)$ of size $\mathcal{O}(n\,\lambda_2(u))$, which is asymptotically optimal by Theorem 18.

Then, we take the depth-4 SC as a base case for induction and prove that we can repeat the procedure any number of times. By the induction, we get the general relation $\left|\mathsf{SC}_{2h}\left(n, n, \frac{n}{r}\right)\right| \in \mathcal{O}(n\,\lambda_h(r))$. From that, it is easy to see, that also $\left|\mathsf{SC}_{2h+1}\left(n, n, \frac{n}{r}\right)\right| \in \mathcal{O}(n\,\lambda_h(r))$.

### Depth of 2 (suboptimal)

First, we present a construction of depth-2 SC. It is not optimal; however, the recursive construction for greater depths based on this depth-2 SC still yields asymptotically optimal results. For the optimal construction of depth-2 SC, see Section 3.4.3.

**Lemma 24.** *For all positive integers $r \leq n$,*

$$\left|\mathsf{SC}_2\left(n, \frac{n}{r}, \frac{n}{2r}\right)\right| \in \mathcal{O}(n \log r).$$

**Corollary 25.** *For all positive integers $s \leq n$,*

$$\left|\mathsf{SC}_2\left(n, n, \frac{n}{s}\right)\right| \in \mathcal{O}\left(n \log^2 s\right).$$

*Proof of Lemma 24.* In the case $r = 1$, the construction is trivial even for depth 1; just take a matching between inputs and outputs. For the rest of the proof, let $r \geq 2$. We construct the SC from the lemma as a sum of two depth-2 partial SCs – let's call them $SC_a$ and $SC'_a$:

$$SC_a \stackrel{\text{def}}{=} \mathsf{SC}_2\left(n, \frac{n}{r}, \frac{2}{3}\frac{n}{r}\right); \quad SC'_a \stackrel{\text{def}}{=} \mathsf{SC}_2\left(n, \frac{2}{3}\frac{n}{r}, \frac{n}{2r}\right)$$

First, we construct $SC_a$ as a product of a concentrator and its inverse:

$$SC_a = \mathsf{C}_1\left(n : \frac{4}{3}\frac{n}{r}, \frac{n}{r}\right) \times \overline{\mathsf{C}_1\left(n : \frac{4}{3}\frac{n}{r}, \frac{n}{r}\right)}.$$

Why does the construction works? Let's denote the size of the middle layer of the network $m$, so that $m = \frac{4}{3}\frac{n}{r}$. The concentrators concentrate any at most $\frac{n}{r} = \frac{3}{4}m$ requests from inputs and outputs to the middle layer. If some pair of the requests from input and output matches the same vertex, we connect them by a path through that vertex. After we connect all such pairs, there can

remain at most $\frac{m}{2}$ unhandled requests on each side, as the number of unhandled request on the left and the right side is the same and every unhandled request corresponds to a middle vertex matched only from one side. So, on every side there remains at most $\frac{m}{2} = \frac{2}{3}\frac{n}{r}$ unhandled requests and therefore the network is really $\mathsf{SC}_2\left(n, \frac{n}{r}, \frac{2}{3}\frac{n}{r}\right)$.

We construct $SC'_a$ in a similar way:

$$SC'_a = \mathsf{C}_1\left(n : \frac{8}{9}\frac{n}{r}, \frac{2}{3}\frac{n}{r}\right) \times \overline{\mathsf{C}_1\left(n : \frac{8}{9}\frac{n}{r}, \frac{2}{3}\frac{n}{r}\right)}$$

Again we denote $m'$ the size of the middle layer, so $m' = \frac{8}{9}\frac{n}{r}$. By the same reasoning, from any at most $\frac{2}{3}\frac{n}{r} = \frac{3}{4}m'$ requests, at most $\frac{m'}{2}$ of them remains unahndled. As $\frac{m'}{2} = \frac{4}{9}\frac{n}{r} \leq \frac{1}{2}\frac{n}{r}$, the network is really $\mathsf{SC}_2\left(n, \frac{2}{3}\frac{n}{r}, \frac{n}{2r}\right)$.

We obtain the partial SC from the statement of the lemma by taking the sum $SC_a + SC'_a$:

$$\mathsf{SC}_2\left(n, \frac{n}{r}, \frac{n}{2r}\right) = \mathsf{SC}_2\left(n, \frac{n}{r}, \frac{2}{3}\frac{n}{r}\right) + \mathsf{SC}_2\left(n, \frac{2}{3}\frac{n}{r}, \frac{n}{2r}\right)$$

The $SC_a$ takes at most $\frac{n}{r}$ requests and lets at most $\frac{2}{3}\frac{n}{r}$ of requests unhandled and $SC'_a$ takes at most $\frac{2}{3}\frac{n}{r}$ requests and lets at most $\frac{1}{2}\frac{n}{r}$ requests unhandled. So, we first let operate $SC_a$ to reduce the number of requests to at most $\frac{2}{3}\frac{n}{r}$ and then use $SC'_a$ to to reduce the rest to at most $\frac{1}{2}\frac{n}{r}$, so the network really is the desired $\mathsf{SC}_2\left(n, \frac{n}{r}, \frac{n}{2r}\right)$ of size $\mathcal{O}(n \log r)$. The whole construction is shown in Figure 3.2.

By the Proposition 21, the concentrators used in the construction have size $\mathcal{O}(n \log r)$, so the lemma is proved.

□

*Proof of Corollary 25.* Let $s \in [n]$ and $i \in \{0, 1, \ldots \log_2(s) - 1\}$. For each $i$ we take an instance of $\mathsf{SC}_2\left(n, \frac{n}{r}, \frac{n}{2r}\right)$ with $r = 2^i$ which we have from the Lemma 24 and we build a network as a sum of all of these $\log_2(s)$ instances. In this new network, for any at most $\frac{n}{s}$ requests, we first use the $\mathsf{SC}_2\left(n, \frac{n}{1}, \frac{n}{2}\right)$ to handle a half of them, then the $\mathsf{SC}_2\left(n, \frac{n}{2}, \frac{n}{4}\right)$ to handle a half of the remaining and generally, we use $\mathsf{SC}_2\left(n, \frac{n}{2^i}, \frac{n}{2^{i+1}}\right)$ to push the number of unhandled requests under $\frac{n}{2^{i+1}}$, so at the end, we have at most $\frac{n}{2^{\log_2(s)}} = \frac{n}{s}$ requests left.

As for all the used partial SCs, we have $r \leq s$, every one of the SCs has size $\mathcal{O}(n \log s)$, so the size of the whole network is $\mathcal{O}\left(n \log^2 s\right)$.

□

### Depth of 4

Now, we use the depth-2 SC from Corollary 25 to construct optimal depth-4 SC. Then, we prove by induction that the same procedure can be iterated to achieve optimal SCs for all greater depths.

**Lemma 26.** *For all positive integers $t \leq n$,*

$$\left|\mathsf{SC}_4\left(n, \frac{n}{t}, \frac{n}{2^t}\right)\right| \in \mathcal{O}(n).$$

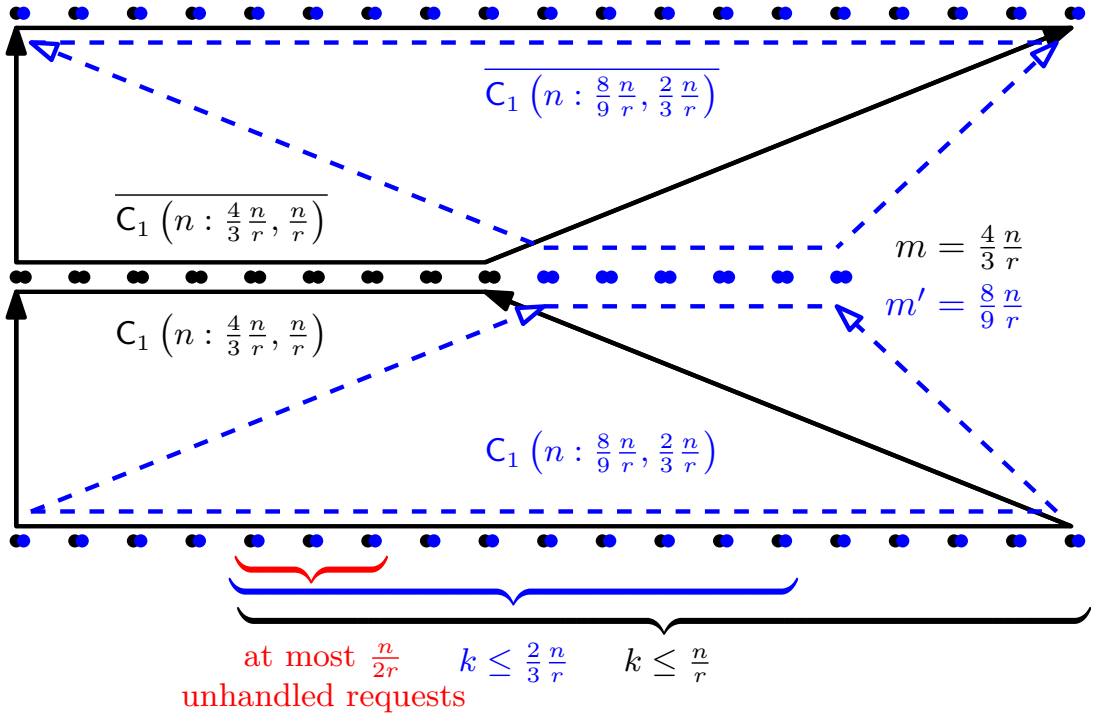


Figure 3.2: $\mathsf{SC}_2\left(n, \frac{n}{r}, \frac{n}{2r}\right)$ as a sum of $SC_a$ and $SC'_a$.

**Corollary 27.** *For all positive integers $u \leq n$,*

$$\left|\mathsf{SC}_4\left(n, n, \frac{n}{u}\right)\right| \in \mathcal{O}\left(n\,\lambda_2(u)\right).$$

*Proof of Lemma 26.* The construction is somewhat similar to the one for depth 2 – we again construct the desired SC as a sum of two depth-4 partial SCs, let's call them $SC_b$ and $SC'_b$:

$$SC_b \stackrel{\text{def}}{=} \mathsf{SC}_4\left(n, \frac{n}{t}, \frac{n}{t^4}\right); \quad SC'_b \stackrel{\text{def}}{=} \mathsf{SC}_4\left(n, \frac{n}{t^4}, \frac{n}{2^t}\right)$$

We start with the construction of $SC_b$. For the construction, we use two concentrators to concentrate the requests from inputs and outputs, and in the center, we use one depth-2 partial SC to route the concentrated requests:

$$SC_b = \mathsf{C}_1\left(n : \frac{n}{\sqrt{t}}, \frac{n}{t}\right) \times \mathsf{SC}_2\left(\frac{n}{\sqrt{t}}, \frac{n}{\sqrt{t}}, \frac{n}{t^4}\right) \times \overline{\mathsf{C}_1\left(n : \frac{n}{\sqrt{t}}, \frac{n}{t}\right)}$$

Any at most $\frac{n}{t}$ requests are moved by the concentrators to the SC and the SC can take all the concentrated requests and left only $\frac{n}{t^4}$ of them unhandled, so the network is really $\mathsf{SC}_4\left(n, \frac{n}{t}, \frac{n}{t^4}\right)$. The concentrators are linear by the Proposition 21 and by the Corollary 25, the partial SC in the middle has size $\mathcal{O}\left(\frac{n}{\sqrt{t}}\log^2\left(t^{7/2}\right)\right) \subseteq \mathcal{O}\left(n\right)$, so $SC_b$ has linear size.

Now, we construct $SC'_b$ in a similar way:

$$SC'_b = \mathsf{C}_1\left(n : \frac{n}{t^2}, \frac{n}{t^4}\right) \times \mathsf{SC}_2\left(\frac{n}{t^2}, \frac{n}{t^2}, \frac{n}{2^t}\right) \times \overline{\mathsf{C}_1\left(n : \frac{n}{t^2}, \frac{n}{t^4}\right)}$$

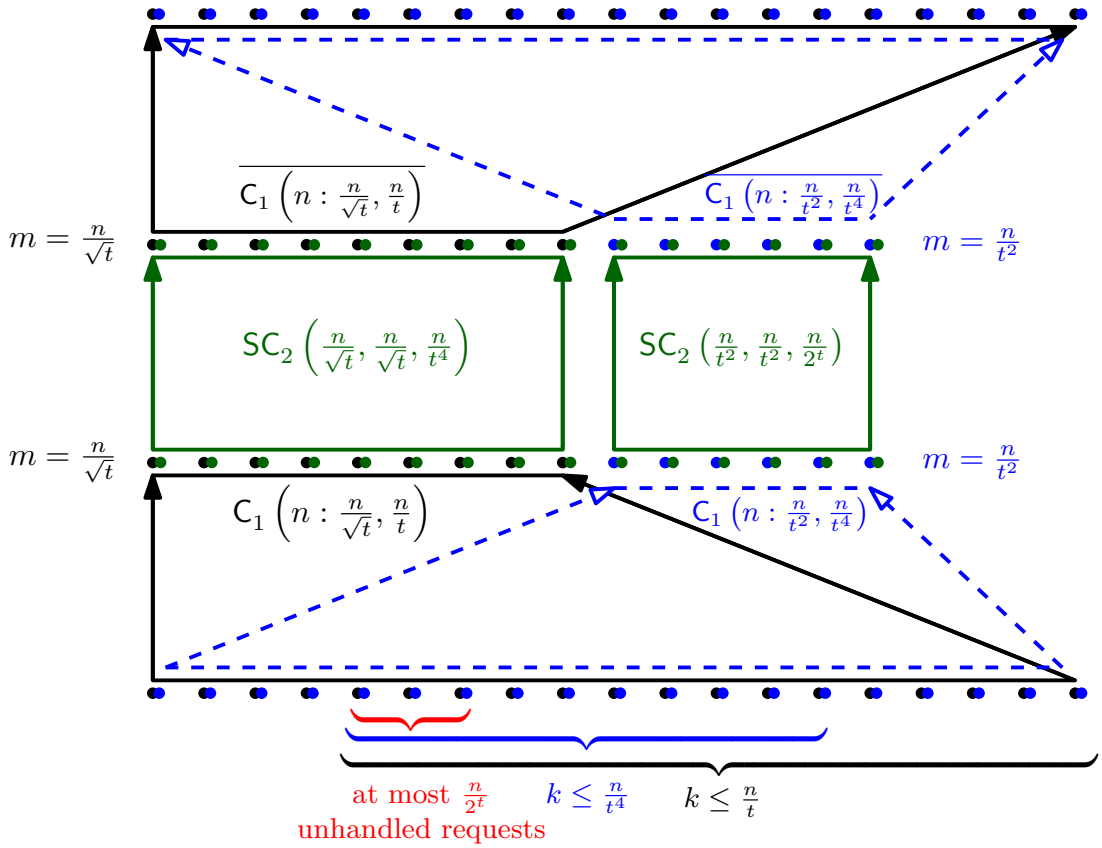


Figure 3.3: $\mathsf{SC}_4\left(n, \frac{n}{t}, \frac{n}{2^t}\right)$ as a sum of $SC_b$ and $SC'_b$.

The construction works for the same reason as for the $SC_b$, the concentrators are again linear by Proposition 21 and the partial SC in the middle has size $\mathcal{O}\left(\frac{n}{t^2}\log^2\left(\frac{2^t}{t^2}\right)\right) \subseteq \mathcal{O}(n)$ by the Corollary 25, so $SC'_b$ is also linear.

To get the SC from the statement of the lemma, we take the sum $SC_b + SC'_b$:

$$\mathsf{SC}_4\left(n, \frac{n}{t}, \frac{n}{2^t}\right) = \mathsf{SC}_4\left(n, \frac{n}{t}, \frac{n}{t^4}\right) + \mathsf{SC}_4\left(n, \frac{n}{t^4}, \frac{n}{2^t}\right)$$

The $SC_b$ takes care of all but $\frac{n}{t^4}$ requests and from the remaining requests $SC'_b$ handles all but $\frac{n}{2^t}$, so the network is $\mathsf{SC}_4\left(n, \frac{n}{t}, \frac{n}{2^t}\right)$ and as both $SC_b$ and $SC'_b$ are linear, the whole network is linear. You can see the whole construction in Figure 3.3.

□

*Proof of Corollary 27.* Let $u \in [n]$ and $i \in \{0, 1, \ldots, \lambda_2(u) - 1\}$. For each $i$, take an instance of $\mathsf{SC}_4\left(n, \frac{n}{t}, \frac{n}{2^t}\right)$ for $t = \mathsf{A}_1^{(i)}(1) = \mathsf{A}_2(i)$, which is linear the Lemma 26 and take sum of all these instances. The first partial SC takes care of all but $\frac{n}{2}$ requests, the second handles all the rest but $\frac{n}{2^2}$, the third the rest but $\frac{n}{2^{2^2}}$ and so on, to the last one, which lets $\frac{n}{\mathsf{A}_2(\lambda_2(u))} \leq \frac{n}{u}$ requests unhandled.

□

**Depth of $2h$**

Now, we prove by induction on $h$ that by the same procedure, we can achieve optimal SCs of all greater even depths. That solves also all odd depths greater than 3, as by Theorem 18, the lower bounds for depths $2h$ and $2h+1$ are the same for all $h \geq 2$.

**Theorem 28** (Proposition 1.3 in Dolev et al. [1983])**.** *For every constant $h \geq 2$, for all integers $n \geq 1$ and $v, w \in [n]$:*

$$\left|\mathsf{SC}_{2h}\left(n, \frac{n}{v}, \frac{n}{\mathsf{A}_{h-1}(v)}\right)\right| \in \mathcal{O}(n) \tag{3.3}$$

$$\left|\mathsf{SC}_{2h}\left(n, n, \frac{n}{w}\right)\right| \in \mathcal{O}(n\,\lambda_h(w)) \tag{3.4}$$

*Proof.* In the Lemma 26 and in the Corollary 27, we have already proven ( 3.3) and ( 3.4) for the case $h = 2$. That means, that the base case is true and it remains to prove the induction step. So, let's first construct ( 3.3) using the induction hypothesis $\left|\mathsf{SC}_{2(h-1)}\left(n_p, n_p, \frac{n_p}{r}\right)\right| \in \mathcal{O}(n_p\,\lambda_{h-1}(r))$. The construction is analogous to the one for depth-4 case above, so it is a sum of two linear SCs $SC_c + SC'_c$:

$$SC_c = \mathsf{SC}_{2h}\left(n, \frac{n}{v}, \frac{n}{v^2}\right); \quad SC'_c = \mathsf{SC}_{2h}\left(n, \frac{n}{v^2}, \frac{n}{\mathsf{A}_{h-1}(v)}\right)$$

First, we construct $SC_c$:

$$SC_c = \mathsf{C}_1\left(n : \frac{n}{\sqrt{v}}, \frac{n}{v}\right) \times \mathsf{SC}_{2(h-1)}\left(\frac{n}{\sqrt{v}}, \frac{n}{\sqrt{v}}, \frac{n}{v^2}\right) \times \overline{\mathsf{C}_1\left(n : \frac{n}{\sqrt{v}}, \frac{n}{v}\right)}$$

The concentrators are linear by the Proposition 21 and by the induction hypothesis, the partial SC has size $\mathcal{O}\left(\frac{n}{\sqrt{v}}\,\lambda_{h-1}(v^{3/2})\right) \subseteq \mathcal{O}\left(\frac{n}{\sqrt{v}}\log\left(v^{3/2}\right)\right) \subseteq \mathcal{O}(n)$, so the whole $SC_c$ is linear.

In the same manner, we construct $SC'_c$:

$$SC'_c = \mathsf{C}_1\left(n : \frac{n}{v}, \frac{n}{v^2}\right) \times \mathsf{SC}_{2(h-1)}\left(\frac{n}{v}, \frac{n}{v}, \frac{n}{\mathsf{A}_{h-1}(v)}\right) \times \overline{\mathsf{C}_1\left(n : \frac{n}{v}, \frac{n}{v^2}\right)}$$

Once again, the concentrators are linear by Proposition 21 and by the induction hypothesis, the partial SC has size $\mathcal{O}\left(\frac{n}{v}\,\lambda_{h-1}(\mathsf{A}_{h-1}(v))\right) = \mathcal{O}(n)$, as $\lambda_i(\mathsf{A}_i(x)) = x$, so $SC'_c$ is linear.

Taking the sum $SC_c + SC'_c$, we obtain $\left|\mathsf{SC}_{2h}\left(n, \frac{n}{v}, \frac{n}{\mathsf{A}_{h-1}(v)}\right)\right| \in \mathcal{O}(n)$, so ( 3.3) is proven.

The second part ( 3.4) follows from ( 3.3). Let $i \in \{0, 1, \ldots, \lambda_h(w) - 1\}$ and for each $i$, take instance of $\mathsf{SC}_{2h}\left(n, \frac{n}{v}, \frac{n}{\mathsf{A}_{h-1}(v)}\right)$ for $v = \mathsf{A}^{(i)}_{h-1}(1) = \mathsf{A}_h(i)$ and build the final network by taking sum of all the instances. The final network leaves only $\frac{n}{\mathsf{A}_h(\lambda_h(w))} \leq \frac{n}{w}$ requests unhandled, so it is $\left|\mathsf{SC}_{2h}\left(n, n, \frac{n}{w}\right)\right| \in \mathcal{O}(n\,\lambda_h(w))$.

□

### 3.4.2 Depth of 3

Below, we present asymptotically optimal depth-3 SC construction by Alon and Pudlák [1994]. As the general depth above, this construction also works for partial SCs, so we construct $\left|\mathsf{SC}_3\left(n, n, \frac{n}{u}\right)\right| \in \mathcal{O}\left(n \log\log(u)\right)$ (which matches the lower bound from Theorem 18).

The principle is the same as in the construction for depth 4. For constants $r$, $q$, we construct linear $\mathsf{SC}_3\left(n, \frac{n}{r^{q^i}}, \frac{n}{r^{q^{i+1}}}\right)$ using two concentrators to concentrate the inputs and outputs, and then one partial SC in the middle to route the requests to the next side. We just use depth-1 partial SC instead of the depth-2 one to save one level. Then, we use a sum of $\mathcal{O}\left(\log\log u\right)$ instances of this linear partial SC to get the final partial SC.

Note that we could use this depth-3 partial SC instead of the depth-2 one in the general construction to get all the partial SCs of the same sizes only with the depth larger by one.

**Theorem 29.** *For all positive integers $u \leq n$,*

$$\left|\mathsf{SC}_4\left(n, n, \frac{n}{u}\right)\right| \in \mathcal{O}\left(n \log\log u\right).$$

**Lemma 30.** *There is a real constant $\alpha > 1$ and an integer constant $r \geq 1$, so that for all integers $i \geq 0$ and $n \geq 1$,*

$$\left|\mathsf{SC}_3\left(n, \frac{n}{r^{\alpha^i}}, \frac{n}{r^{\alpha^{i+1}}}\right)\right| \in \mathcal{O}\left(n\right).$$

*Proof of Lemma 30.* In addition to the constants from the statement of the lemma, let there be also a real constant $0 < \beta < 1$ (we determine the exact values later). We build the desired linear partial SC from two concentrators and one partial SC:

$$\begin{aligned}&\mathsf{SC}_3\left(n, \frac{n}{r^{\alpha^i}}, \frac{n}{r^{\alpha^{i+1}}}\right) = \\ &= \mathsf{C}_1\left(n : \frac{n}{r^{\beta\alpha^i}}, \frac{n}{r^{\alpha^i}}\right) \times \mathsf{SC}_1\left(\frac{n}{r^{\beta\alpha^i}}, \frac{n}{r^{\beta\alpha^i}}, \frac{n}{r^{\alpha^{i+1}}}\right) \times \overline{\mathsf{C}_1\left(n : \frac{n}{r^{\beta\alpha^i}}, \frac{n}{r^{\alpha^i}}\right)}\end{aligned}$$

The concentrators concentrate any at most $\frac{n}{r^{\alpha^i}}$ requests and the partial SC lets at most $\frac{n}{r^{\alpha^{i+1}}}$ of them unhandled, so the construction works (see the Figure 3.4).

By the Proposition 21, the concentrators have size $\mathcal{O}\left(n\frac{\log(n/k)}{\log(m/k)}\right)$ which for $k = \frac{n}{r^{\alpha^i}}$ and $m = \frac{n}{r^{\beta\alpha^i}}$ equals $\mathcal{O}\left(n\frac{1}{1-\beta}\right) = \mathcal{O}\left(n\right)$.

According to Proposition 22, the partial SC has size $\mathcal{O}\left(\frac{n_0^2}{k}\log\left(\frac{n_0}{k}\right)\right)$ which for $n_0 = \frac{n}{r^{\beta\alpha^i}}$ and $k = \frac{n}{r^{\alpha^{i+1}}}$ equals $\mathcal{O}\left(nr^{\alpha^i(\alpha-2\beta)}\alpha^{i(\alpha-\beta)}\log(r)\right)$. We need to set the values of the constant so that the size is linear. Such setting exists, for example $\alpha = \frac{7}{6}$, $\beta = \frac{2}{3}$ and $r = 4$. So we have linear $\mathsf{SC}_3\left(n, \frac{n}{r^{\alpha^i}}, \frac{n}{r^{\alpha^{i+1}}}\right)$ for all $i$.

□

*Proof of Theorem 29.* Let $u \in [n]$ and $i \in \{0, 1, \ldots, \log_\alpha \log_r u - 1\}$. For each $i$, take an instance of the SC from Lemma 30 and take sum of all the instances. Resulting network is clearly $\mathsf{SC}_3\left(n, \frac{n}{r}, \frac{n}{u}\right)$. If we add an $\left|\mathsf{SC}_1\left(n, n, \frac{n}{r}\right)\right| \in \mathcal{O}\left(n\right)$ to

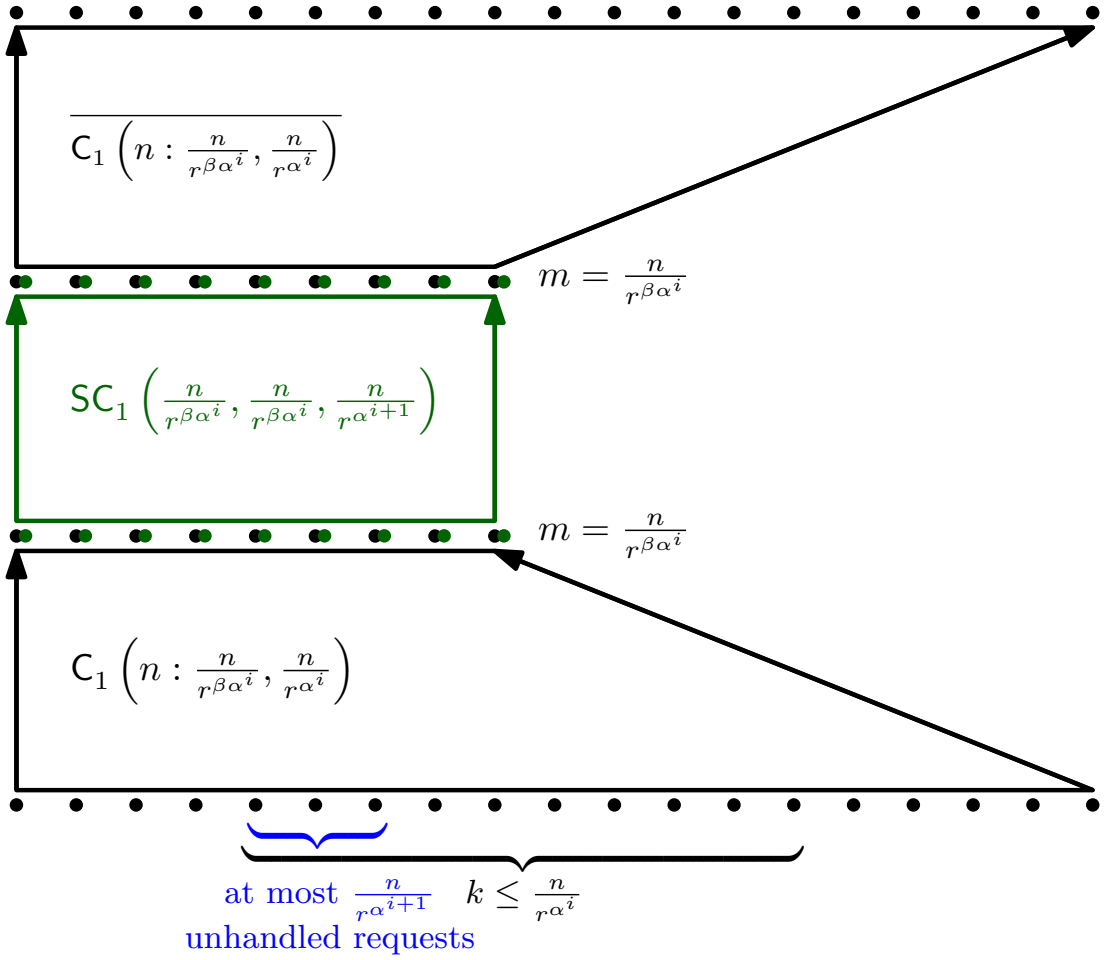


Figure 3.4: Construction of $\mathsf{SC}_3\left(n, \frac{n}{r^{\alpha^i}}, \frac{n}{r^{\alpha^{i+1}}}\right)$

the network, we get the desired $\mathsf{SC}_3\left(n, n, \frac{n}{u}\right)$, and as $\log_\alpha \log_r u \in \mathcal{O}(\log \log u)$, it has size $\mathcal{O}(n \log \log u)$.

□

### 3.4.3 Depth of 2

The construction which we present here is analogous to the one from Section 3.4.1; however, it is based on disperser networks instead of concentrators. It was first used by Wigderson and Zuckerman [1993], but they focused on the explicit construction and so didn't achieve the optimal size (they also used it to construct concentrators, see Section 2.4). Later, Radhakrishnan and Ta-Shma [2000] used the same construction with optimal disperser graphs and got the asymptotically optimal depth-2 SC of size $\mathcal{O}\left(n\frac{\log^2 n}{\log \log n}\right)$.

Before the construction, we need to prove the following lemma. It was originally stated by Meshulam [1984] for SCs, but we state it for partial SCs:

**Lemma 31** (Thm. 1 in Meshulam [1984])**.** *Let $G$ be a depth-2 $(n : n)$-network with no edge between inputs and outputs. Then, $G$ is $\mathsf{SC}_2(n, p, q)$ iff for every $i \leq p$ and for every sets $S$ of $i$ inputs and set $T$ of $i$ outputs, the number of common neighbours of $S$ and $T$ is at least $i - q$.*

*Proof.* It is clear that the condition is necessary, as every one of the $i - q$ vertex-disjoint paths from the definition of partial SC must contain a middle vertex. To prove the sufficiency, we use the Mengers's theorem, which states that the size of a minimum vertex cut separating vertices $u$, $v$ equals the maximum number of internally vertex-disjoint paths from $u$ to $v$.

We add vertices $u$, $v$ to the network and then add edges from $u$ to every vertex of $S$ and from every vertex of $T$ to $v$. The theorem holds for undirected graphs; however, the undirected internally vertex-disjoint $u$ – $v$ paths correspond to the directed vertex-disjoint paths from $S$ to $T$ (and the eventual multiple edges also doesn't matter). So it suffices to prove that if the condition from the lemma holds, the minimum cut $C$ separating $u$ and $v$ has a size of at least $i - q$.

Let's denote $M$ the middle vertices of the network. It is clear, that $(M \cap C) \supseteq (\mathsf{N}(S \setminus C) \cap \mathsf{N}(T \setminus C))$, otherwise, there would be a path from $S \setminus C$ through $M \setminus C$ to $T \setminus C$ so $C$ wouldn't be a cut. By the condition from the lemma, $|\mathsf{N}(S \setminus C) \cap \mathsf{N}(T \setminus C)| \geq \min(|S \setminus C|, |T \setminus C|) - q$. That means, that

$$|M \cap C| \geq |\mathsf{N}(S \setminus C) \cap \mathsf{N}(T \setminus C)| \geq \min(|S \setminus C|, |T \setminus C|) - q$$

And now, we can bound $C$ from below and conclude the proof:

$$\begin{aligned} |C| &\geq |S \cap C| + |T \cap C| + |M \cap C| \\ &\geq |S \cap C| + |T \cap C| + \min(|S \setminus C|, |T \setminus C|) - q \geq i - q \end{aligned}$$

□

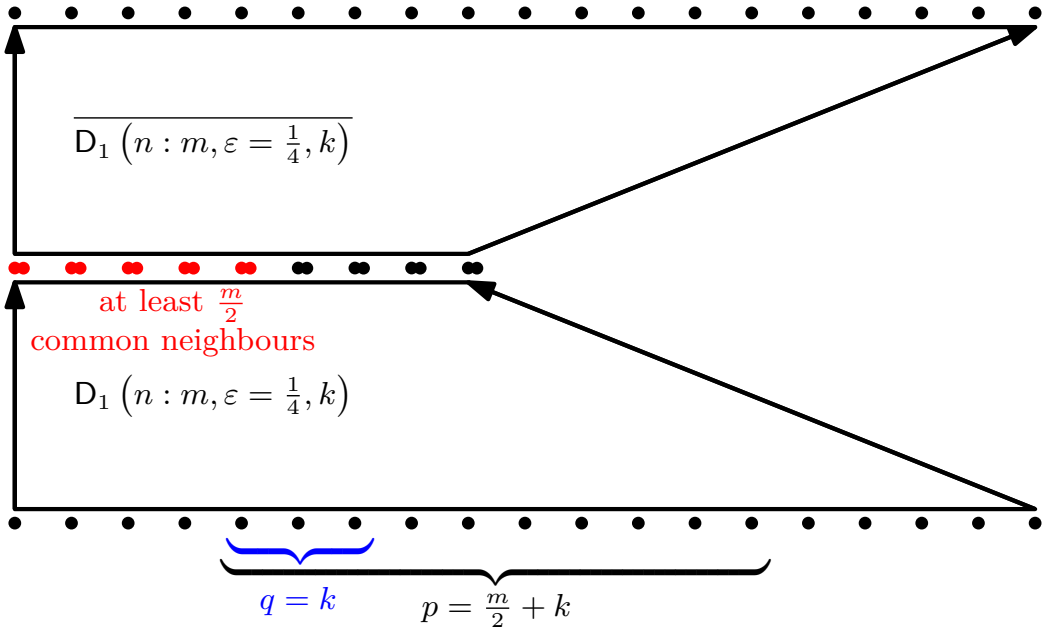


Figure 3.5: Construction of $\mathsf{SC}_2\left(n, \frac{m}{2} + k, k\right)$ from two disperser networks

### The construction

As in the previous sections, we state the theorem for the partial SCs. The non-partial case follows by substituting $r = n$.

**Theorem 32.** *For all positive integers $n \geq r$,*

$$|\mathsf{SC}_2(n, r, 1)| \in \mathcal{O}\left(n \frac{\log n \cdot \log r}{\log \log r}\right).$$

The idea of the construction is similar to the suboptimal one, and it is characterized by the following lemma.

**Lemma 33.** $\mathsf{D}_1\left(n : m, \varepsilon = \frac{1}{4}, k\right) \times \overline{\mathsf{D}_1\left(n : m, \varepsilon = \frac{1}{4}, k\right)} = \mathsf{SC}_2\left(n, \frac{m}{2} + k, k\right)$

*Proof.* In this network, every set of inputs $|S| = i \geq k$ has at least $\frac{3}{4}m$ neighbours and every set $|T| = i$ of outputs also has $\frac{3}{4}m$ neighbours, so it follows, that $S$ and $T$ have at least $\frac{m}{2}$ common neighbours.

Now, we need to use the Lemma 31 to show, that the network is $\mathsf{SC}_2(n, p, k)$. For which $p$ is this true? For any $i \leq p$ we need the number of the common neighbours to be at least $i - k$. For $i \leq k$ this is trivially true and for $i > k$ we have always at least $\frac{m}{2}$ common neighbours by the disperser property. It means, that we only need $\frac{m}{2} \geq p - k \geq i - k$ for the network to be $\mathsf{SC}_2(n, p, k)$. That gives us sufficient condition $p \leq \frac{m}{2} + k$. The construction is shown in Figure 3.5.

□

By the Proposition 23, we have $\left|\mathsf{D}_1\left(n : m, \frac{1}{4}, k\right)\right| \in \mathcal{O}\left(n\left(\log\left(\frac{n}{k}\right) + \frac{m}{k}\right)\right)$. If we now substitute for $p$, $q$ to this bound, we get following corollary of the lemma. The weaker bound on the right is sufficient for the construction.

**Corollary 34.** $|\mathsf{SC}_2(n,p,q)| \in \mathcal{O}\left(n\left(\log\left(\frac{n}{q}\right)+\frac{p-q}{q}\right)\right) \subseteq \mathcal{O}\left(n\left(\log\left(\frac{n}{q}\right)+\frac{p}{q}\right)\right)$

Note, that by the corollary, we can obtain $\mathsf{SC}_2\left(n,\frac{n}{r},\frac{n}{2r}\right)$ of size $\mathcal{O}(n\log r)$ from one pair of disperser networks. So, this method is a bit simpler, as it requires only one pair of disperser networks, compared to two pairs of concentrators in Section 3.4.1.

Let's now use the corollary to prove the theorem.

*Proof of Theorem 32.* Let $r \in [n]$ and $i \in \{0,1,\ldots\frac{\log r}{\log\log r}-1\}$. For every $i$, we construct $\mathsf{SC}_2\left(n,\log^i(r),\log^{i+1}(r)\right)$, which is $\mathcal{O}(n\log n)$ by the Corollary 34. Taking sum of all these partial SCs yields $\mathsf{SC}_2(n,r,1)$ of size $\mathcal{O}\left(n\frac{\log n\cdot\log r}{\log\log r}\right)$. □

### 3.4.4 Superconcentrator of linear size

When we have constructed (asymptotically) optimal-size SC for every constant depth, there comes a natural question – how large depth would we need to achieve linear size? Again, we show a construction matching the lower bound. It consists of recursive construction, which was first introduced by Bassalygo [1981] and then used by Dolev et al. [1983] by combining it with the asymptotically optimal bounds on bounded depth SC to achieve the asymptotically optimal depth. However, we took the recursive construction from Pippenger [1996] (instead of Bassalygo), as the Pippenger's construction can be easily made explicit, so we need it anyway in Chapter 5, where we discuss explicit SCs.[1]

#### Linear superconcentrator of logarithmic depth

First, let's introduce Pippenger's recursive construction[2], which can be expressed by this theorem:

**Theorem 35** (Thm. 1 in Pippenger [1996])**.** *For all integers $j > \ell > 1$ and $h \geq 0$:*

$$\mathsf{SC}_{h+2}(n) = \mathsf{SC}_1\left(n,n,\frac{n}{j}\right) + \mathsf{C}_1\left(n:\frac{n}{\ell},\frac{n}{j}\right) \times \mathsf{SC}_h\left(\frac{n}{\ell}\right) \times \overline{\mathsf{C}_1\left(n:\frac{n}{\ell},\frac{n}{j}\right)}$$

We believe that the principle of the construction is quite clear. First, we use one depth-1 SC to handle all but $\frac{n}{j}$ requests. Then, we concentrate all the remaining requests from both sides to space of size $\frac{n}{\ell}$ and then use $\mathsf{SC}_h\left(\frac{n}{\ell}\right)$ to handle all the concentrated requests (see Figure 3.6).

For constants $j > \ell > 1$ (let's choose $\ell = 2$, $j = 4$), both the concentrator and the depth-1 SC easily achieve linear size – see the bounds in Section 3.3. So, if we start with trivial $\mathsf{SC}_0(1)$ (one vertex) as a base of the recursive construction,

[1] And also because Bassalygo's article is in Russian. Its translation was published in "Problems of Information transmission", but the article is not in the online archive.

[2] The original version is more complicated, as Pippenger [1996] permitted sending a constant number of requests over every edge and vertex and also required for the paths to be distributively calculated by finite automatons placed in the vertices.

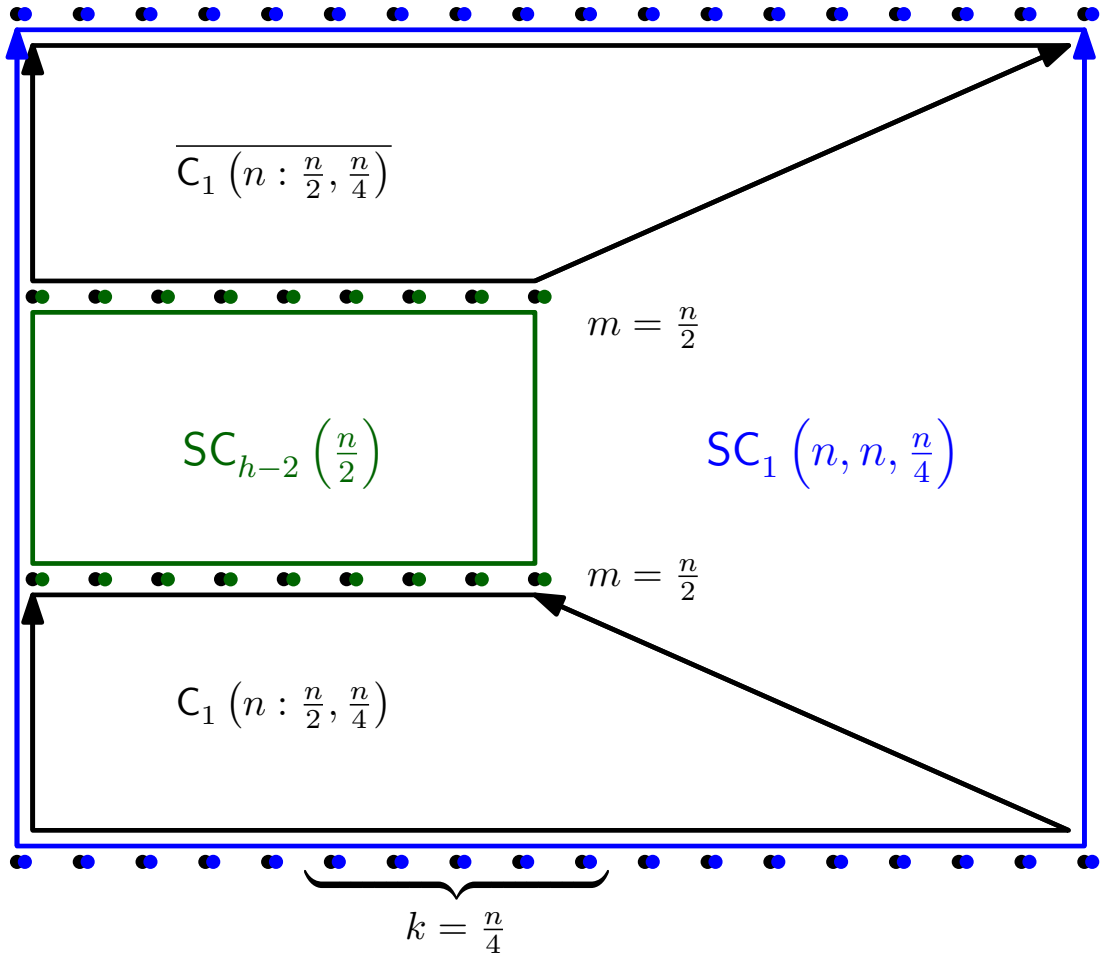


Figure 3.6: Pippenger's recursive construction for $\ell = 2$ and $j = 4$.

we get SC of depth $h = \lceil 2 \log_2 n \rceil$ for any $n$. The concentrator and depth-1 SC used in the last step has size $\mathcal{O}(n)$, the ones from previous step two times less and so on, so the overall size is $\mathcal{O}\left(n + \frac{n}{2} + \frac{n}{4} \ldots 1\right) = \mathcal{O}(n)$.

### Linear superconcentrator of asymptotically optimal depth

We can improve the logarithmic construction by using some good depth-$z$ SC as a base of the construction instead of the trivial depth-0 one. Informally, if we have depth-$z$ SC of size $an$, we can use the construction $\log_2 a$ times to push the input size under $\frac{n}{a}$ and then use the depth-$z$ SC of size $a\frac{n}{a} = n$. The resulting linear SC has depth $z + 2 \log_2 a$. This idea was used implicitly by Dolev et al. [1983] and was briefly mentioned by Wigderson and Zuckerman [1993].

**Theorem 36.** *There is a function $h(n)$ defined for all $n \geq 1$, so that $h(n) \in \mathcal{O}(\beta(n))$ and*

$$\left|\mathsf{SC}_{h(n)}(n)\right| \in \mathcal{O}(n).$$

The theorem is a consequence of this lemma.

**Lemma 37** (Lemma 4.7 in Wigderson and Zuckerman [1993])**.** *Let there be a positive integer $z$, a non-decreasing function $f_z$, $f_z(n) \geq 1$, and let $|\mathsf{SC}_z(n)| \in \mathcal{O}(n f_z(n))$. Then, there is a linear superconcentrator of depth*

$$h = z + \lceil 2 \log_2(f_z(n)) \rceil \in \mathcal{O}(z + f_z(n)).$$

That is true, as after $\lceil 2 \log_2(f_z(n)) \rceil$ recursion steps, the number of inputs and outputs is at most $\frac{n}{f_z(n)}$, so the size of the depth-$z$ SC we used as a base of the construction is $\mathcal{O}\left(\frac{n}{f_z(n)} f_z\left(\frac{n}{f_z(n)}\right)\right)$ which is linear for non-decreasing $f_z(n) \geq 1$.

*Proof of Theorem 36.* We use the lemma for the asymptotically optimal depth-$z$ SCs that we have by Theorem 28. So we get linear SC of depth $\mathcal{O}(z + \lambda_z(n))$ for any $z \geq 2$. We would like to minimize this expression. That means, that for every $n$, we would like to choose the lowest $z$ so that $z \geq \lambda_z(n)$. That is exactly the definition of $\beta(n) = \min\{z : \lambda_z(n) \leq z\}$. So, the theorem follows from the lemma by substituting $z = \beta(n)$.

□

# 4. Explicit expander constructions

In the previous chapter, we determined the asymptotic size of SCs of every depth. However, the upper bounds on expanders we used were mostly obtained by probabilistic construction, so the bounds didn't come with some algorithm for constructing these expanders. Of course, we could just construct all graphs of appropriate size and test, which one is the wanted expander, but this algorithm is exponential in $n$. This motivates us to define *explicit construction*[1].

**Definition 20** (Explicit construction)**.** *Let there be an infinite family $F$ of multigraphs. An explicit construction of $F$ is an poly$(n)$ time algorithm, which for any $n$ outputs a representation of $G \in F$ on $n$ vertices, if such $G$ exists. If we have such an algorithm, we say that $F$ is explicit.*

In this chapter, we try to find the best explicit expanders. We will see that there is a large gap between the upper bounds from Chapter 1 and the explicit expanders – we achieve the size from Chapter 1 only for the spectral expanders. Also, the explicit constructions are much more complex and are beyond the scope of this thesis, so we don't present there any of them.

We also utilize the relationships between expanders from Chapter 2 to convert some explicit expanders (mostly the optimal spectral expanders) to expanders of another type. We summarize the achieved sizes in Table 4.1. Sizes obtained by conversion from another type of expander are in grey; the conversions are denoted by arrows.

## 4.1 Spectral expanders

We start with spectral expanders, as they were the only source of explicit expanders for a long time. We already mentioned in Chapter 1, that by Nilli [1991], in every $d$-regular multigraph, $\lambda \geq 2\frac{\sqrt{d-1}}{d} - o(1)$ (where the $o$ notation is with respect to $n$).

$d$-regular multigraphs, for which $\lambda \leq 2\frac{\sqrt{d-1}}{d}$ are called *Ramanujan graphs*. As explained in Section 2.1, the bipartite Ramanujan graphs are defined so that every bipartite Ramanujan graph with parameter $\lambda'$ is balanced spectral $\lambda$-expander for some $\lambda \leq \lambda'$, so all the upper bound on bipartite Ramanujan graphs are also valid for the balanced spectral expanders. After many years of development, the problem of constructing Ramanujan graphs is nearly solved – we don't cover the whole history there and mention only the best achieved results.

Morgenstern [1994] found explicit construction of Ramanujan graphs on $q+1$ vertices for any prime power $q$ (the title of the article in fact is "Existence and Explicit Constructions of $q+1$ Regular Ramanujan Graphs for Every Prime Power $q$"), Mohanty et al. [2019] showed explicit construction of *nearly Ramanujan*

[1]Some authors distinguish between *mild* and *full* explicitness. Our definition corresponds to the mild version; for the full one, one must be able to compute $i$-th neighbour of a vertex in poly(log $n$) time.

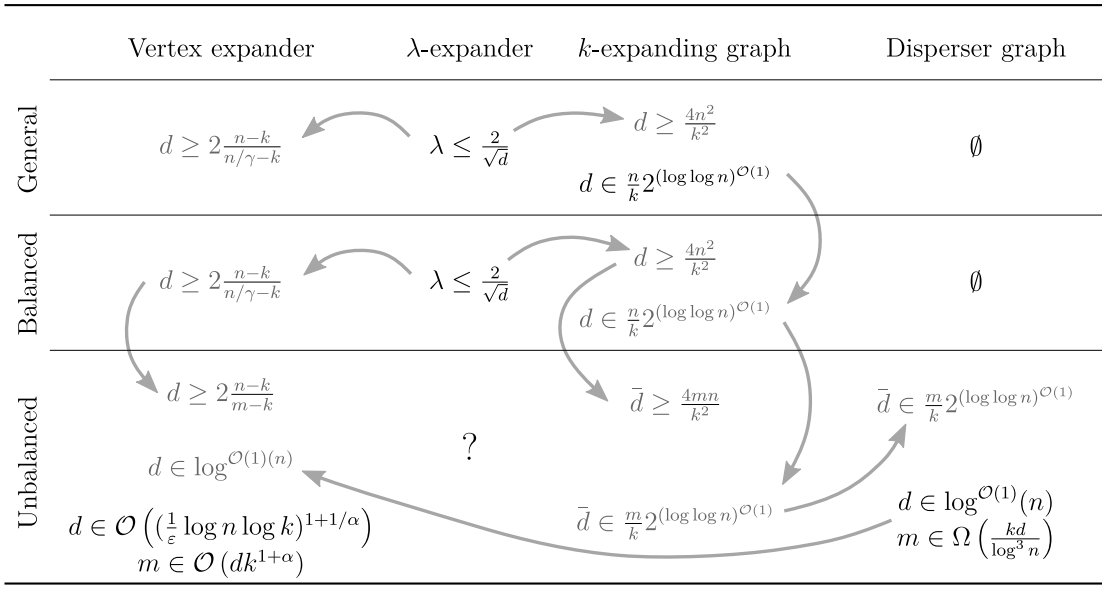


Table 4.1: Overview of explicit expanders

graphs for any $n$ and $d$. That means, that for every $d \geq 3$ and $\varepsilon \geq 0$, they give $poly(n)$ algorithm that outputs a graph on $\Theta(n)$ vertices with $\lambda \leq 2\frac{\sqrt{d-1}}{d} + \varepsilon$.

For the balanced bipartite version, the situation is even better – Marcus et al. [2015] proved the existence of bipartite Ramanujan graph for every $n$ and every degree $d$. Later, Cohen [2016] devised a polynomial algorithm to construct any of these graphs.

As we already mentioned in Chapter 1, we didn't find much information about unbalanced spectral expanders; especially, we didn't find the upper and lower bounds on the size, nor explicit constructions. It would be interesting to try to use the techniques from the articles mentioned above to construct the unbalanced versions; we were not able to do so in a limited time.

## 4.2 *k*-expanding graphs

First, we can use the Corollary 13 of a mixing lemma from Section 2.2 to get $k$-expanding graph from spectral expanders. We have already shown it in Section 2.2 – if we have $\lambda \geq \frac{2}{\sqrt{d}}$ (which we can achieve explicitly, as explained above), we get the condition $d \geq \frac{4n^2}{k^2}$ for both the general and balanced case. To obtain the unbalanced version, we can simply remove appropriate edges from the general case, as explained in Section 2.3. The bound on the right degree stays the same, so for the left average degree, we have $\bar{d} \geq \frac{m}{n}\frac{4n^2}{k^2} = \frac{4mn}{k^2}$.

Wigderson and Zuckerman [1993] gave explicit construction of $n^\delta$-expanding graph for any $d \geq n^{1-\delta}2^{(\log\log n)^{\mathcal{O}(1)}}$:

**Theorem 38** (Thm. 1.2 in Wigderson and Zuckerman [1993])**.** *There is a logspace algorithm that, on input $n$ (in unary) and $\delta$, where $0 < \delta = \delta(n) < 1$, constructs a $k$-expanding graph on $n$ nodes with $k = n^\delta$ and maximum degree*

$$d \geq \frac{n}{k}2^{(\log\log n)^{\mathcal{O}(1)}} = n^{1-\delta}2^{(\log\log n)^{\mathcal{O}(1)}}.$$

Note, that this is close to the probabilistic bound, as we only have $2^{(\log\log n)^{\mathcal{O}(1)}}$ instead of $\log\left(\frac{en}{k}\right)$ in the size. Again, by deleting edges, we get the unbalanced version with $\bar{d} \in \frac{m}{k}2^{(\log\log n)^{\mathcal{O}(1)}}$.

The construction is based on seeded randomness extractors, and as the article was published in 1993, it would be interesting to try to use the current best-known extractors to improve the construction. Again, we were not able to do it, and we leave it for future research.

## 4.3 Disperser graphs

As we explained in Section 2.4 unbalanced $k$-expanding graphs are equivalent to $\left(k,\ \frac{k}{m}\right)$-disperser graphs. So, from the construction of $k$-expanding graphs above follows, that for every $\delta$, there are explicit $\left(n^{\delta},\ \frac{n^{\delta}}{m}\right)$-disperser graphs for $\bar{d} \in \frac{m}{n^{\delta}}2^{(\log\log n)^{\mathcal{O}(1)}}$.

Ta-Shma et al. [2007] achieved polylogarithmic degree, for some $m \in \Omega\left(\frac{kd}{\log^3 n}\right)$.

**Theorem 39** (Thm. 1.4 in Ta-Shma et al. [2007])**.** *For every $n = 2^x$, $k = 2^y$ and constant $\varepsilon$, there is a degree $d \in \log^{\mathcal{O}(1)}(n)$ explicit $(k,\ \varepsilon)$-disperser graph with $m \in \Omega\left(\frac{kd}{\log^3 n}\right)$.*

This result is crucial, as it enables explicit construction of depth-2 SC of size $n\log^{\mathcal{O}(1)}(n)$.

## 4.4 Vertex expanders

We have already seen in Section 2.1 that with $\lambda = \frac{2}{\sqrt{d}}$ (which we have explicitly), the conversion from spectral to vertex expanders gives us general or balanced explicit vertex expander for every $d \geq 2\frac{n-k}{n/\gamma-k}$. However, we are mostly interested in the unbalanced case, which we can't achieve this way, as we do not have unbalanced spectral expanders.

One way out is to use Pippenger's construction from Section 2.6. If we use it on the explicit balanced vertex expander above, we get unbalanced vertex $(k,\ \gamma = 1)$-expander with $\frac{n}{m}$ integer for any $d \geq 2\frac{n-k}{m-k}$. However, we noted in Section 2.6, that even when used on the non-explicit balanced expanders, this construction is useless as $\frac{n}{m}$ goes close to $n$, so the same is of course still true now. (We chose $\gamma = 1$ as we need to use the expander as a concentrator.)

Another way is to use the construction from Section 2.5 (again with $\gamma = 1$). Let $i \in \{0, 1, \ldots, \log_2 k - 1\}$, $n = 2^x$ (for some integer $x$) and $\varepsilon$ constant. Then, by Theorem 39, we have for every $i$ explicit disperser with $k_i = 2^i$, $m_i = \frac{2^{i+1}}{1-\varepsilon}$ and degree $d_i \in \log^{\mathcal{O}(1)}(n)$. We now have for every $i$: $m_i(1-\varepsilon) \geq k_{i+1}$, so we can use the Proposition 16, which for every $n = 2^x$ and $2^y = k \leq n$ yields explicit unbalanced vertex $(k, \gamma = 1)$-expander with $m = \frac{k}{1-\varepsilon}$ and $d \in \log_2(k)\log^{\mathcal{O}(1)}(n) \subseteq \log^{\mathcal{O}(1)}(n)$.

And finally, there is a result by Guruswami et al. [2009], which yields vertex expanders with an even smaller degree and larger $\gamma$, but with larger $m$ with respect to $k$:

**Theorem 40** (Thm. 1.3 in Guruswami et al. [2009])**.** *For all constants $\alpha > 0$: for every $n \in \mathbb{N}$, $k \leq n$, and $\varepsilon > 0$, there is an explicit vertex $(k, (1-\varepsilon)d)$-expander with degree $d \in \mathcal{O}\left((\frac{1}{\varepsilon}\log n \log k)^{1+1/\alpha}\right)$ and $m \leq d^2 k^{1+\alpha}$.*

As we only need $\gamma = 1$, we can use the tradeoff between $\gamma$ and $m$ from Section 2.6 to achieve smaller $m$ with $\gamma = 1$. By using the Proposition 17 for $l = \lfloor (1-\varepsilon)d \rfloor$, we get $\gamma \geq 1$ and $m \leq \frac{d^2 k^{1+\alpha}}{\lfloor (1-\varepsilon)d \rfloor} \approx \frac{dk^{1+\alpha}}{1-\varepsilon} \in \mathcal{O}\left(dk^{1+\alpha}\right)$ for constant $\varepsilon$.

**Corollary 41.** *For all constants $\alpha > 0$: for every $n \in \mathbb{N}$, $k \leq n$, and constant $\varepsilon > 0$, there is an explicit unbalanced vertex $(k, \gamma = 1)$-expander with degree $d \in \mathcal{O}\left((\frac{1}{\varepsilon}\log n \log k)^{1+1/\alpha}\right)$ and $m \in \mathcal{O}\left(dk^{1+\alpha}\right)$.*

# 5. Explicit superconcentrator constructions

As we have seen in Chapter 4, our resources for explicit SC constructions are very limited. In this chapter, we state the so far best known explicit constructions – depth-2 SC of size $n \log^{\mathcal{O}(1)} n$ and linear SC of depth $\mathcal{O}(\log \log n)$. We also summarize some open problems and topics for further research, which arose during the creation of this thesis.

We denote the explicit networks by upper index e (for example $\mathsf{SC}_d^{\mathrm{e}}(n, m, k)$).

## 5.1 Depth-2 superconcentrator of polylogarithmic degree

The currently best known explicit construction of bounded-depth SC is the construction by Radhakrishnan and Ta-Shma [2000], which we explained in Section 3.4.3. When we use it with the best explicit disperser graphs by Ta-Shma et al. [2007], we achieve depth-2 SC of size $n \log^{\mathcal{O}(1)} n$ (Ta-Shma et al. noticed that and mentioned it in the article).

The construction is characterized by the following lemma:

**Lemma 42** (Lemma 33 restated)**.**

$$\mathsf{D}_1\left(n : m, \varepsilon = \frac{1}{4}, k\right) \times \overline{\mathsf{D}_1\left(n : m, \varepsilon = \frac{1}{4}, k\right)} = \mathsf{SC}_2\left(n, \frac{m}{2} + k, k\right)$$

Now, we use the explicit disperser from Section 4.3 which for constant $\varepsilon$, $n = 2^x$, $k = 2^y$ and some $m \in k \log^{\Omega(1)} n$ achieves size $n \log^{\mathcal{O}(1)} n$. So, we can choose $m = 2k$ and $k = 2^i$ to get the following corollary of the Lemma 42:

**Corollary 43.**

$$\left|\mathsf{SC}_2^{\mathrm{e}}\left(n, 2^{i+1}, 2^i\right)\right| \in n \log^{\mathcal{O}(1)} n \quad \forall i \in \{0, 1, \ldots \log(n) - 1\}$$

Now, as in the previous constructions, we just construct these partial SCs for every $i$ and take their sum to get the resulting theorem:

**Theorem 44.** *For all integers $n \geq 0$:*

$$|\mathsf{SC}_2^{\mathrm{e}}(n)| \in n \log^{\mathcal{O}(1)} n$$

## 5.2 Explicit linear superconcentrator

The linear SC construction by Pippenger [1996] which we presented in Section 3.4.4 can be made easily explicit by using only the spectral expanders – it was meant so by the author, as there were known explicit constructions of spectral expanders of appropriate size in 1996 (although with higher constants). The construction is characterized by Theorem 35:

**Theorem 45** (Theorem 35 restated)**.** *For all integers $j > \ell > 1$ and $h \geq 0$:*

$$\mathsf{SC}_{h+2}(n) = \mathsf{SC}_1\left(n, n, \frac{n}{j}\right) + \mathsf{C}_1\left(n : \frac{n}{\ell}, \frac{n}{j}\right) \times \mathsf{SC}_h\left(\frac{n}{\ell}\right) \times \overline{\mathsf{C}_1\left(n : \frac{n}{\ell}, \frac{n}{j}\right)}$$

In Section 3.4.4, we have chosen $\ell = 2$ and $j = 4$, so let's stick with the choice. That means that we need explicit networks $\mathsf{C}_1^{\mathrm{e}}\left(n : \frac{n}{2}, \frac{n}{4}\right)$ and $\mathsf{SC}_1^{\mathrm{e}}\left(n, n, \frac{n}{2}\right)$ of linear size. From Chapter 4, we know, that there is explicit unbalanced vertex expander with $\gamma = 1$ for any $d \geq 2\frac{n-k}{m-k}$ and $k$-expanding graph for any $d \geq \frac{2n^2}{a^2}$ (we got both from spectral expanders). It follows by simple substitution, that we have the needed explicit networks of linear size (particularly with $d = 6$ and $d = 8$).

Now, as mentioned in Section 3.4.4, we can start with trivial $\mathsf{SC}_0^{\mathrm{e}}(1)$ as a base of the recursive construction to get explicit linear SC of depth $h = \lceil 2\log_2 n \rceil$.

We have achieved the asymptotically optimal depth by starting with some good bounded-depth SC instead of the trivial $\mathsf{SC}_0^{\mathrm{e}}(1)$. The procedure was justified by Lemma 37:

**Lemma 46** (Lemma 37 restated for explicit SCs)**.** *Let there be a positive integer $z$, non-decreasing function $f_z$, $f_z(n) \geq 1$, and let $|\mathsf{SC}_z^{\mathrm{e}}(n)| \in \mathcal{O}(nf_z(n))$. Then, there is an explicit linear superconcentrator of depth*

$$h = z + \lceil 2\log_2(f_z(n)) \rceil \in \mathcal{O}(z + \log(f_z(n))).$$

We can do the same with the explicit depth-2 SC from this chapter – we use it as a base of the construction. In the terms of the lemma, we have $z = 2$ and $f_z = \log^{\mathcal{O}(1)} n$. Then, the lemma gives us an explicit linear SC of depth $d \in \mathcal{O}\left(2 + \log\left(\log^{\mathcal{O}(1)} n\right)\right) \subseteq \mathcal{O}(\log\log n)$.

**Theorem 47.** *There is a function $h(n)$ defined for all $n \geq 1$, so that $h(n) \in \mathcal{O}(\log\log n)$ and*

$$\left|\mathsf{SC}_{h(n)}^{\mathrm{e}}(n)\right| \in \mathcal{O}(n).$$

## 5.3 Open problems

### 5.3.1 Better explicit superconcentrators

We were not able to get any better explicit SCs with the available expanders. We have no proof for that, but we believe that we still need some better explicit expanders to move on. In any case, the major open problem is the construction of smaller explicit superconcentrators. We mention there a few particular ideas where to start.

#### Bipartite spectral expanders

It would be interesting to examine the situation around the construction of unbalanced vertex expanders – possibly by checking if some methods for constructing bipartite Ramanujan graphs can be modified to construct also the unbalanced case. Also, we are not sure if the lower bound on bipartite Ramanujan graphs also holds for the less strict definition of bipartite spectral expanders with one-sided expansion, which we used in the thesis (Definition 11).

#### Better $k$-expanding graphs from extractors

The construction of $k$-expanding graphs by Wigderson and Zuckerman [1993] is based on explicit extractors. It shouldn't be hard to plug in the currently best known explicit extractors and so possibly improve the construction. The probably best current explicit extractors were constructed by Ta-Shma and Umans [2012]. There is also a nice summary of the extractors known in 2004 by Shaltiel [2004].

#### Unbalanced vertex expander with smaller $\gamma$

The currently best known explicit construction of an unbalanced vertex expander by Guruswami et al. [2009] is also focused on maximizing $\gamma$. We showed a trivial method to lower simultaneously $\gamma$ and $m$; however, we wonder if it would be possible to achieve better parameters by analyzing their proof while focusing on the case $\gamma = 1$.

### 5.3.2 Another type of superconcentrators

Gal et al. [2013] gave following general definition of 3 types of superconcentrators:

**Definition 21** (Generalized Superconcentrators)**.** *Let $G$ be an $(n : m)$-network for $n \leq m$. Further, let $X$ be a subset of inputs, $Y$ a subset of outputs, $|X| = |Y| = k$, and denote $f(X, Y)$ the maximum number of directed vertex-disjoint paths from $X$ to $Y$. Then, for a fixed constant $0 < \delta \leq 1$, we give following hierarchy of superconcentrators ordered by strength:*

**Type 1:** *For each $X$, $Y$: $f(X, Y) \geq \delta k$*

**Type 2:** *For each $X$:* $\mathsf{E}_Y[f(X, Y)] \geq \delta k$

**Type 3:** $\mathsf{E}_{X,Y}[f(X, Y)] \geq \delta k$

The superconcentrators of the first type for $n = m$ and $\delta = 1$ are superconcentrators by the Definition 14, which we used in the thesis.

It would be interesting to investigate the SC constructions for the general definition, as we did with the "normal" superconcentrators. We originally planned to cover also the general version, but we didn't manage to do so in the time we had, so the problem remains.

# Conclusion

We studied a great amount of literature to find any information concerning bounded-depth superconcentrators and expanders relevant to their constructions. It was not easy to find the right articles, as there is no survey summarizing the achieved results. In the thesis, we tried to fill this gap.

We presented all the needed expanders in a systematic way together with proofs of their properties or pointers to appropriate articles. We restated the construction of optimal depth-$h$ superconcentrators by Dolev et al. [1983] in more detail (as it is originally just one page of a conference paper, and so it is very hard to read), and we added the later results for depth 2 and 3. We also provide pointers to relevant explicit expanders and current "world record" explicit superconcentrator constructions.

Despite a certain amount of effort, we did not succeed in designing brand new explicit constructions of superconcentrators, which is not surprising as this is a notoriously difficult problem.

We hope that our work will be useful to anybody interested in superconcentrators as a summary of the known techniques and results.

# Bibliography


Noga Alon and Pavel Pudlák. Superconcentrators of depths 2 and 3; odd levels help (rarely). *Journal of Computer and System Sciences*, 48(1):194–202, February 1994. ISSN 0022-0000. doi: 10.1016/S0022-0000(05)80027-3. URL https://doi.org/10.1016/S0022-0000(05)80027-3.

Leonid Alexandrovich Bassalygo. Asymptotically optimal switching circuits. *Problemy Peredachi Informatsii*, 17(3):81–88, 1981. URL http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=ppi&paperid=1410.

Michael B. Cohen. Ramanujan graphs in polynomial time. *CoRR*, abs/1604.03544, 2016. URL http://arxiv.org/abs/1604.03544.

Danny Dolev, Cynthia Dwork, Nicholas Pippenger, and Avi Wigderson. Superconcentrators, generalizers and generalized connectors with limited depth. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, STOC '83, page 42–51, New York, NY, USA, 1983. Association for Computing Machinery. ISBN 0897910990. doi: 10.1145/800061.808731. URL https://doi.org/10.1145/800061.808731.

Anna Gal, Kristoffer Arnsfelt Hansen, Michal Koucký, Pavel Pudlák, and Emanuele Viola. Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates. 59(10):6611–6627, October 2013. ISSN 0018-9448. doi: 10.1109/TIT.2013.2270275. URL https://doi.org/10.1109/TIT.2013.2270275.

Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from parvaresh–vardy codes. *J. ACM*, 56(4), July 2009. ISSN 0004-5411. doi: 10.1145/1538902.1538904. URL https://doi.org/10.1145/1538902.1538904.

T. Kövari, V. T. Sós, and P. Turán. On a problem of K. Zarankiewicz. *Colloq. Math.*, 3:50–57, 1954. ISSN 0010-1354. doi: 10.4064/cm-3-1-50-57. URL https://doi.org/10.4064/cm-3-1-50-57.

Adam W. Marcus, Daniel A. Spielman, and Nikhil Srivastava. Interlacing families iv: Bipartite ramanujan graphs of all sizes. In *Proceedings of the 2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS)*, FOCS '15, page 1358–1377, USA, 2015. IEEE Computer Society. ISBN 9781467381918. doi: 10.1109/FOCS.2015.87. URL https://doi.org/10.1109/FOCS.2015.87.

Roy Meshulam. A geometric construction of a superconcentrator of depth 2. *Theoretical Computer Science*, 32(1):215–219, 1984. ISSN 0304-3975. doi: 10.1016/0304-3975(84)90032-X. URL https://doi.org/10.1016/0304-3975(84)90032-X.

Sidhanth Mohanty, Ryan O'Donnell, and Pedro Paredes. Explicit near-ramanujan graphs of every degree. *CoRR*, abs/1909.06988, 2019. URL http://arxiv.org/abs/1909.06988.

M. Morgenstern. Existence and explicit constructions of q + 1 regular ramanujan graphs for every prime power q. *Journal of Combinatorial Theory, Series B*, 62(1):44–62, 1994. ISSN 0095-8956. doi: 10.1006/jctb.1994.1054. URL https://doi.org/10.1006/jctb.1994.1054.

A. Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91(2): 207–210, 1991. ISSN 0012-365X. doi: 10.1016/0012-365X(91)90112-F. URL https://doi.org/10.1016/0012-365X(91)90112-F.

Mark S. Pinsker. On the complexity of a concentrator. In *7th International Teletraffic Conference*, pages 318/1–318/4, 1973. URL https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.393.1430&rep=rep1&type=pdf.

Nicholas Pippenger. Self-routing superconcentrators. *Journal of Computer and System Sciences*, 52(1):53–60, feb 1996. doi: 10.1006/jcss.1996.0005. URL https://doi.org/10.1006/jcss.1996.0005.

Pavel Pudlák. Communication in bounded depth circuits. *Combinatorica*, 14(2): 203–216, 1994. doi: 10.1007/BF01215351. URL https://doi.org/10.1007/BF01215351.

Jaikumar Radhakrishnan and Amnon Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM J. Discret. Math.*, 13(1):2–24, January 2000. ISSN 0895-4801. doi: 10.1137/S0895480197329508. URL https://doi.org/10.1137/S0895480197329508.

Ronen Shaltiel. Recent developments in explicit constructions of extractors. In *Current Trends in Theoretical Computer Science: The Challenge of the New Century Vol 1: Algorithms and Complexity Vol 2: Formal Models and Semantics*, pages 189–228. World Scientific, 2004. URL https://www.cs.haifa.ac.il/~ronen/online_papers/survey.ps.

Amnon Ta-Shma and Christopher Umans. Better condensers and new extractors from parvaresh-vardy codes. In *2012 IEEE 27th Conference on Computational Complexity*, pages 309–315. IEEE, 2012. doi: 10.1109/CCC.2012.25. URL https://doi.org/10.1109/CCC.2012.25.

Amnon Ta-Shma, Christopher Umans, and David Zuckerman. Lossless condensers, unbalanced expanders, and extractors. *Combinatorica*, 27(2):213–240, 2007. doi: 10.1007/s00493-007-0053-2. URL https://doi.org/10.1007/s00493-007-0053-2.

R. Michael Tanner. Explicit concentrators from generalized n-gons. *SIAM Journal on Algebraic Discrete Methods*, 5(3):287–293, 1984. doi: 10.1137/0605030. URL https://doi.org/10.1137/0605030.

Robert Endre Tarjan. Efficiency of a good but not linear set union algorithm. *J. ACM*, 22(2):215–225, apr 1975. ISSN 0004-5411. doi: 10.1145/321879.321884. URL https://doi.org/10.1145/321879.321884.

Salil P. Vadhan. Pseudorandomness. *Foundations and Trends® in Theoretical Computer Science*, 7(1–3):1–336, 2012. ISSN 1551-305X. doi: 10.1561/0400000010. URL http://doi.org/10.1561/0400000010.

Leslie G. Valiant. On non-linear lower bounds in computational complexity. In *Proceedings of the Seventh Annual ACM Symposium on Theory of Computing*, STOC '75, page 45–53, New York, NY, USA, 1975. Association for Computing Machinery. ISBN 9781450374194. doi: 10.1145/800116.803752. URL https://doi.org/10.1145/800116.803752.

Avi Wigderson and David Zuckerman. Expanders that beat the eigenvalue bound: Explicit construction and applications. *Combinatorica*, 19:245–251, 1993. doi: 10.1007/s004930050049. URL https://doi.org/10.1007/s004930050049.