Proceedings of Symposia in Applied Mathematics
Volume 44, 1991

Constructing random-like graphs

Fan R. K. Chung
Bellcore
Morristown, NJ 07960

1. Introduction

Many problems in combinatorics, theoretical computer science and communication theory can be solved by the following probabilistic approach: To prove the existence of some desired object, first an appropriate (probability) measure is defined on the class of subjects; second, the subclass of desired objects are shown to have positive measure. This implies that the desired objects must exist. This technique, while extremely powerful, suffers from a serious drawback. Namely, it gives no information about how one might actually go about explicitly constructing the desired objects. Thus, while we might even be able to conclude that almost all of our objects have the desired property (that is, all except for a set of measure zero), we may be unable to exhibit a single one. A simple example of this phenomenon from number theory is that of a normal number. A real number x is said to be normal if for each integer $b \geq 2$, each of the digits $0, 1, \cdots, b-1$ occurs asymptotically equally often in the base b expansion of x. It is known that almost all (in Lebesgue measure) real numbers are normal, but no one has yet succeeded in proving that any particular number (such as π, e or $\sqrt{2}$) is normal.

One of the earliest examples of the above probabilistic method is Erdös' classical result in the 50's on the existence of graphs on n nodes which have maximum cliques and independent sets of size $2 \log n$. Since then, probabilistic methods have been successfully used

1991 *Mathematics Subject Classification.* Primary 05C; Secondary 68.

0160-7634/91 $1.00 + $.25 per page

in a wide range of areas in extremal graph theory, computational complexity and communication networks. However, in spite of the success of probabilistic methods, there is a clear need for explicit constructions, especially for applications in algorithmic design and building efficient communication networks.

In the past ten years, substantial progress has been made on explicit constructions of graphs which satisfy certain desired properties possessed by "random" graphs (i.e., properties possessed by almost all graphs, under the probabilistic models for graphs used in [13, 51, 85]). While it is logically impossible to construct a truly random graph, it is, however, often feasible to obtain constructions which simulate random graphs in the sense of sharing similar properties. We will discuss a number of useful properties which can be loosely partitioned into the following categories: the *Ramsey property*, the *discrepancy property*, the *expansion property*, the *eigenvalue property* and the *extremal properties*. The detailed definitions of these properties will be described in Section 2. Roughly speaking, the Ramsey property concerns the size of maximum cliques and independent sets; the discrepancy property asserts that each subset of nodes spans about the expected number of edges; the expansion property implies each subset of nodes has many neighbors; and the eigenvalue property deals with separation of the eigenvalues. The extremal properties involve the occurrence and frequency of specified subgraphs. Among these properties, the eigenvalue property is the easiest to achieve. We can now construct graphs with very good eigenvalue properties and these graphs also satisfy good expansion and discrepancy properties. On the other hand, relatively little progress has been made on the classical problems concerning the Ramsey property or certain extremal properties. Our plan here is to report the current progress on explicit constructions, identify the boundary of our knowledge and mention numerous related questions.

A major theme in extremal graphs is to study how one graph property affects another [66, 94, 100, 101]. Recently, the strong relationship between the various properties, all shared by random graphs, have been investigated in a series of papers for dense graphs and other combinatorial structures such as hypergraphs, sequences, etc. [31, 32, 33, 34, 35, 36, 37, 39]. It turns out that many of the useful properties fall naturally into a number of equivalence classes, the so-called "quasi-random" classes, each of which captures certain aspects of randomness. Although the study of "quasi-random" graphs is closely related to this paper, we will not discuss them here. Rather, we will focus on the constructive aspects for sparse, medium and dense graphs. By a construction, we mean an explicit scheme for constructing an infinite family of graphs.

This paper is organized as follows: In Section 2 we describe various graph properties that random graphs satisfy. Section 3 focuses on the eigenvalues property and its relation with other properties. In Section 4, explicit constructions are demonstrated for various ranges of edge densities. In Section 5, we illustrate the motivating application of using expander graphs to build communication networks. In Section 6, we discuss various other extermal properties such as diameter, girth and Turán type problems.

2. Random-like graph properties

2.1. The Ramsey property

A fundamental result of Ramsey [92] guarantees the existence of a number $R(k, \ell)$ so that any graph on $n \geq R(k, \ell)$ nodes contains either a clique of size k or an independent set of size ℓ. The problem of determining $R(k, \ell)$ is well known to be notoriously difficult. The first non-trivial lower bound for $R(k, k)$, due to Erdös [43] in 1947, states

$$R(k,k) > (1+o(1))\frac{1}{e\sqrt{2}}\, k \cdot 2^{k/2} \tag{1}$$

In other words, there exist graphs on n nodes which contain no cliques or independent sets of size $2\log n$ when n is sufficiently large. The proof for (1) is simple and elegant. By observing the probability of having a clique or independent set of size k is at most $\binom{n}{k} \cdot 2^{1-\binom{k}{2}}$ then, if this quantity is less than one, there must exist a graph without any clique or independent set of size k.

This basic result plays an essential role laying the foundations for both Ramsey theory and probabilistic methods, two of the major thriving areas in combinatorics. In the 40 years since its proof, the bound in (1) has only been improved by a factor of 2, also by probabilistic arguments [98].

Attempts have been made over the years to construct good graphs (i.e., with small cliques and independent sets) without much success [38, 63]. H.L Abbott [1] gives a recursive construction with cliques and independence sets of size $cn^{\log 2/\log 5}$. Nagy [84] gives a construction reducing the size to $cn^{1/3}$. A breakthrough finally occurred several years ago with the result of Frankl [54] who gave the first Ramsey construction with cliques and independent sets of size smaller than $n^{1/k}$ for any k. This was further improved to $e^{c(\log n)^{3/4}(\log\log n)^{1/4}}$ in [24]. Here we will outline a construction of Frankl and Wilson [56] for Ramsey graphs with cliques and independent sets of size at most $e^{c(\log n \log\log n)^{1/2}}$.

Construction 2.1. Let q be a prime power. The graph G has node set $N = \{F \subseteq \{1, \cdots, m\} : | F | = q^2 - 1\}$ and edge set $E = \{(F, F') : | F \cap F' | \not\equiv -1 (\mathrm{mod}\ q)\}$. A result in [56] implies G contains no clique or independent set of size $\binom{m}{q-1}$. By choosing $m = q^3$, we obtain a graph on $n = \binom{m}{q^2-1}$ nodes containing no clique or independent set of size $e^{c(\log n \log \log n)^{1/2}}$.

A graph which has often been suggested as a natural candidate for a Ramsey graph is the Paley graph (see more discussion in Section 4). Very little is known about its maximum size of cliques and independent sets. On the lower bound, a recent result of S. Graham and C. Ringrose [64] shows that for infinitely many Paley graphs on p nodes contain a clique of size $c \log p \log\log\log p$. (This contrasts with the trivial upper bound of $c\sqrt{p}$.) Earlier results of Montgomery [83] show that assuming the Generalized Riemann Hypothesis, we would have a lower bound $c \log p \log\log p$ infinitely often. If we take the Ramsey property as a measure of "randomness", the above results show Paley graphs deviate from random graphs. There is no question that the most "wanted" problem in constructive methods is the following problem, posed long ago by Erdös:

Problem 2.1. Construct graphs on n nodes containing no clique and no independent set of size $c \log n$.

Instead of focusing on the occurrence of cliques and independence sets, similar problems can be considered on the occurrence or the frequency of other specified subgraphs [15, 65, 93, 107]. It is not difficult to show that almost all graphs contain every graph with up to 2 log n nodes as an induced subgraph. The best current constructions containing every graph with up to $c\sqrt{\log n}$ nodes as induced subgraphs can be found in [34, 55].

2.2. The discrepancy property

Let $G = (N, E)$ be a graph having node set N with n nodes and edge set E with e edges. The edge density ρ is defined to be $e/\binom{n}{2}$. For each $S \subset N$, we define the set of edges *induced* by S to be $E(S) = \{\{u, v\} \in E : u, v \in S\}$ and $e(S) =\mid E(S) \mid$. The *discrepancy* of S, denoted by $disc_G(S)$, is defined to be $\mid e(S) - \rho \binom{\mid S \mid}{2} \mid / \mid S \mid$. The α-*discrepancy* of G is the maximum discrepancy of $S \subseteq N$ over all S with $\mid S \mid = \alpha n$. The discrepancy of G is the maximum discrepancy of S over all $S \subseteq N$.

In a certain sense, the discrepancy is the "continuous" version of the Ramsey property which asserts that when α is very small $\left(\sim \frac{c \log n}{n}\right)$, the α-discrepancy is as large as it can possibly be. In general, the problem of determining the α-discrepancy is a very difficult problem. However, very good bounds can be derived, for example, for $\alpha > \frac{1}{\sqrt{n}}$, by using eigenvalue arguments which will be discussed in detail in Section 3. Constructions of graphs with good discrepancy properties will be illustrated in Section 4.

In the remaining part of this subsection, we concentrate on the discrepancy of a random graph. Let G denote a random graph with fixed edge density ρ. We define a function f which assigns the value $(1 - \rho)$ to edges of G and the value $-\rho$ to non-edges of G. It is easy to see that $\mid \sum_{u,v \in S} f(u, v) \mid = disc_G(S) \mid S \mid$. We will examine the easier case of $\rho = \frac{1}{2}$ (the general case can be dealt with in a similar manner.) Using the Chernoff bound [51], the probability that a fixed S, with $s =\mid S \mid$, having discrepancy more than x is $exp\left(-2x^2 s^2 / \binom{s}{2}\right)$. Therefore the total probability of having some set having discrepancy x is at most $\binom{n}{s} exp\left(-2x^2s^2/\binom{s}{2}\right)$. When the above quantity is smaller than 1, there must exist a graph with discrepancy no more than x. Suppose we choose x to be $c\,n^{1/2}$. We can then conclude the discrepancy of a random graph is at most $c'\,n^{1/2}$.

2.3. The expansion property

The expansion property is crucial in many applications [10, 72, 73, 88, 89, 86, 103, 104] and has become the driving force for recent progress in constructive methods. The success is due, in large part, to a combination of tools from graph theory, network theory, theoretical computer science and various mathematical disciplines such as number theory, representation theory, and harmonic analysis. Perhaps, because of the large number of different applications in disparate settings, the definitions of expansion-like properties vary from one situation to another often with cumbersome names such as expander, magnifier, enlarger, generalizer, concentrator, and superconcentrator, just to name a few. To make matters worse, most of these definitions involve a large number of parameters. One typical example for the definition of a concentrators is as follows: An $(n, \theta, k, \alpha, \beta)$-concentrator is a bipartite graph with n inputs, θn outputs and $k\,n$ edges, such that every input subset A with $\mid A \mid \geq \alpha\,n$ has at least $\beta\,n$ neighbors. It is conceivable that such tedious definitions hindered the early progress in this area.

The expansion property basically means each subset X of nodes must have "many" neighbors. That is, the neighborhood set $\Gamma(X) = \{y : y \text{ is adjacent to some } x \in X\}$ is "large" in comparison with X. The difficulty lies in finding a good way to define the quantity in place of "many" or "large". There is an obvious condition that when the subset S is almost the entire node set, the strict neighborhood $\Gamma(S) - S$ is very small. The typical definition for expander graphs is as follows: A regular graph G is a (n, k, c)-expander if G has n nodes with degree k so that every subset S of $N(G)$ satisfies

$$|\Gamma(S) - S| \geq c(1 - \frac{|S|}{n}) \mid S \mid.$$

This definition is still somewhat unsatisfactory since the expander factor c and the degree k are intimately related. For example, a random regular graph of degree k has an expander factor about k when the subset is small. The expander factor c should be judged in comparison with a function of k. This leads to the following definition. A graph G is said to have *expansion* c for $c > 1/k$, denoted by *expan* (G), if c is the largest value so that every $S \subset N(G)$ with $\mid S \mid /n = \alpha$ satisfies

$$|\Gamma(S)| \geq \frac{ck}{ck\alpha + 1 - \alpha} \mid S \mid$$

where k is the average degree. Although this definition is not as succinct as we may have wished, it gives a lower bound for $|\Gamma(S)|$ of about $ck \mid S \mid$ if $\mid S \mid$ is small and about $\mid S \mid$ if $\mid S \mid$ is close to n. This definition turns out to be useful for our later discussions of eigenvalues.

The expansion of G is closely related with the discrepancy of G in the following sense: The discrepancy property implies every subset S contains about the expected number of edges; therefore there are "many" edges leaving S. Another related invariant is the isoperimetric number [20, 82], denoted by $i(G)$ and defined by

$$i(G) = Min_{S \subset N, |S| < \frac{n}{2}} \frac{\mid \{\{u, v\} \in E(G) : u \in S, v \notin S\} \mid}{\mid S \mid}$$

Analogous to Cheeger constant of a Riemannian manifold, $i(G)$ is sometimes called the Cheeger constant of a graph G. The so-called *conductance* is $1/k$ times $i(G)$ for a k-regular graph G [95]. Clearly, for a k-regular graph, we have also $i(G) \geq k/2 - 2\, disc(G)$.

Discrepancy and conductance are useful for producing edge-disjoint paths while the expansion properties are useful for forming node-disjoint paths joining given pairs of nodes.

2.4. The eigenvalue property

Let $M = (M_{ij})$ denote the adjacency matrix of a graph G. Thus M_{ij} equals 1 if $\{i, j\}$ is an edge, and 0 otherwise. Let $\lambda_1, \lambda_2, \cdots, \lambda_n$ denote the eigenvalues of M, labelled so that $\mid \lambda_1 \mid \geq \mid \lambda_2 \mid \geq \cdots \geq \mid \lambda_n \mid$. A result of Perron-Frobenius [59, 62, 87] guarantees that λ_1 is positive and, in particular, an eigenvector v_1 corresponding to λ_1 has all coordinates positive. If G is regular graph of degree k, then $\lambda_1 = k$ and v_1 is the all 1's vector. Since M is symmetric, the λ's are all real.

Although the problem of determining the eigenvalues of a matrix is in genernal not so simple, some matrices have very special eigenvalues. Here we state some examples which will be useful later (also see [27, 40]).

Example 2.4.1. Suppose M is a circulant matrix. In other words, there are $a_1, \cdots, a_n$ so that $M_{ij} = a_{i-j}$ (index addition is performed modulo p). Then, M has eigenvalues $\sum_{i=1}^{n} a_i$ where θ ranges over all nth roots of 1. The corresponding eigenvectors are $(1, \theta, \cdots, \theta^{n-1})$.

Example 2.4.2. Suppose M is skew-circulant. That is $M_{ij} = a_{i+j}$ for all i, j. Then M has eigenvalues $\sum_{i=1}^{n} a_i, \pm \mid \sum_{i=1}^{n} a_i \theta^i \mid$ where θ ranges over all nth roots of 1. The corresponding eigenvectors are $(1, \theta, \cdots, \theta^{n-1}) \pm (\sum_{i=1}^{n} a_i \theta^i) / \mid \sum_{i=1}^{n} a_i \theta^i \mid \cdot (1, \theta^{-1}, \cdots, \theta^{-n+1})$ if $\theta \neq 1$ and for $\theta = 1$, the eigenvector is the all 1's vector.

For the above examples, the eigenvalues are basically character sums. Therefore, well-known character sum inequalities [19, 106] can be used to bound the eigenvalues (more will be discussed in Section 4).

What are the eigenvalues of a random graph? It was shown by Juhasz [70] that the random graph has $\lambda_1 = (1 + o(1))n/2$ and $\lambda_2 = o(n^{1/2+\epsilon})$ for any fixed $\epsilon > 0$. Füredi and Komlos [60] sharpened the bound to $\lambda_2 = O(n^{1/2})$. A k-regular random graph has second largest eigenvalue $O(\sqrt{k})$ while the largest eigenvalue is k. When k is a fixed constant, Friedman [57] showed the second largest eigenvalue is $2\sqrt{k-1} + O(\log\ k)$. The separation of the first and second largest eigenvalues turns out to be essential in deriving expanding and discrepancy properties. Such relationships will be further discussed in Section 3.

For a graph G we can easily obtain a lower bound for the absolute value of the second largest eigenvalue $\lambda = \mid \lambda_2 \mid$ by the following argument.

$$\begin{aligned} \lambda_1^2 + (n-1)\lambda^2 &\geq \sum_{i=1}^{n} \lambda_i^2 \\ &= TrM^2 \\ &= 2e(G) \end{aligned}$$

When G is a k-regular graph, we then have

$$\lambda \geq \sqrt{k - \frac{(k^2-k)}{n-1}}$$

This bound is quite good when k is large, say, more than $\sqrt{n}$. In fact, it is almost tight for Paley graphs. When k is a fixed small constant, by considering the trace of higher powers of M (see [57]), one can obtain

$$\lambda \geq 2\sqrt{k-1} - \log\ k + O(1)$$

Recent results on constructing expander graphs all involve constructions of which the second largest eigenvalues can be successfully upper bounded. The techniques of bounding eigenvalues are drawn from a variety of areas using character sums, linear algebra, group representations and harmonic analysis.

The relation of eigenvalues with other random-like properties will be discussed in the next section and techniques for bounding eigenvalues will be selectively mentioned throughout Section 4 in which various constructions are illustrated.

3. The relation of eigenvalues with other properties

We will give simple proofs showing that the separation of eigenvalues implies the expansion property and discrepancy property (see [2, 99]). The reverse direction will also be proved by using additional arguments [22, 95]. Although the problem of checking whether a graph is an (n, k, c)-expander is *co-NP-complete* [11],the following relationship provides an efficient method to estimate the expansion and discrepancy of a graph.

Theorem 3.1. A k-regular graph G has expansion at least k/λ^2 where λ is the absolute value of the second largest eigenvalue, i.e. $expan(G) \geq k/\lambda^2$.

Proof: For a subset S of node set N of G, we consider a characteristic vector ψ_S, defined by

$$\psi_S(u) = \begin{cases} 1 & \text{if } u \in S, \\ 0 & \text{otherwise} \end{cases}$$

Suppose that the eigenvalues of the adjacency matrix M of G are $\lambda_1, \lambda_2, \cdots, \lambda_n$ so that $\mid \lambda_1 \mid \geq \mid \lambda_2 \mid \geq \cdots \geq \mid \lambda_n \mid$ where the corresponding orthonormal eigenvectors are $v_1, \cdots, v_n$. Suppose $\psi_S = \sum a_i v_i$ and therefore $\sum a_i^2 = \| \psi_S \|^2 = \mid S \mid = s$. We consider the inner product:

$$\begin{aligned} < \psi_S M, M\psi_S > &= \sum a_i^2 \lambda_i^2 \\ &\leq (k^2 - \lambda^2) a_1^2 + (\sum a_i^2)\lambda^2 \\ &= (k^2 - \lambda^2)\frac{s^2}{n} + s\lambda^2 \end{aligned} \tag{2}$$

On the other hand,

$$\begin{aligned} < \psi_S M, M\psi_S > &= \sum_{u \in S}\sum_{v \in S} \mid \{w : \{v,w\} \in E \text{ and } \{u,w\} \in E\} \mid \\ &= \sum_{w \in N} \mid \Gamma(w) \cap S \mid^2 \end{aligned}$$

where, as mentioned before, for $T \subseteq N$, $\Gamma(T) = \{u : \{u,v\} \in E \text{ for some } v \in T\}$ and $\Gamma(w) = \Gamma(\{w\})$. Applying the Cauchy-Schwarz inequality, we have:

$$\begin{aligned} \sum_{w \in N} \mid \Gamma(w) \cap S \mid^2 &\geq \frac{(\sum_{w \in N} \mid \Gamma(w) \cap S \mid)^2}{\mid \Gamma(S) \mid} \\ &= \frac{k^2 s^2}{\mid \Gamma(S) \mid} \end{aligned}$$

Combining with (2), we obtain

$$| \Gamma(S) | \geq \frac{k^2 s}{(k^2 - \lambda^2)\frac{s}{n} + \lambda^2}$$

We conclude G has expansion at least $\frac{k}{\lambda^2}$, that is, $expan(G) \geq \frac{k}{\lambda^2}$.

Although Theorem 3.1 is quite useful for deriving expansion properties from eigenvalues, still this lower bound is usually a constant factor off from the "true" value. For example, a k-regular random graph has $\lambda \leq 2\sqrt{k-1}$ for small fixed k. Theorem 3.1 gives expansion about $\frac{1}{4}$ while direct calculation shows that a random k-regular graph has expansion about 1. In most applications, constant factors are not crucial. However some applications in parallel architecture require the construction of graphs with expansion $> \frac{1}{2}$. It seems that new ideas will be needed in order to achieve this goal.

Theorem 3.2 A k-regular graph G has discrepancy at most λ. In other words,

$$disc\,(G) \leq \lambda\,/2$$

Proof: Using the same notation as in the proof of Theorem 1, we consider

$$\begin{aligned} < \psi_S, M\psi_S > &= \sum_{u\in S}\sum_{v\in S} M_{uv} \\ &= 2e(S) \end{aligned}$$

where $e(S)$ is the number of edges in S.

On the other hand,

$$\begin{aligned} |< \psi_S, M\psi_S > -\lambda_1 a_1^2 \,| &\leq |\sum_{i\neq 1} \lambda_i a_i^2 \,| \\ &\leq \lambda(s - \frac{s^2}{n}) \end{aligned}$$

Since $\lambda_1 = k$ and $a_1 = s/\sqrt{n}$, we have

$$| \, 2e(S) - k\frac{s^2}{n} \, | \leq \lambda(s - \frac{s^2}{n})$$

Therefore, we have $disc(G) \leq \lambda/2$.

As an immediate consequence, we have

Corollary 3.1. The isoperimetric number of a k-regular graph G is at least $k/2 - 2\lambda$.

The following proof of bounding positive eigenvalues in terms of the isoperimetric number can be viewed as the discrete analogue of Cheeger's inequality [22].

Theorem 3.3. A k-regular graph G has eigenvalues $\lambda_1 = k, \lambda_2, \cdots, \lambda_n$. For $i \neq 1$, we have

$$\lambda_i \leq k - \frac{i(G)^2}{2k}$$

In fact, the following sharper inequality holds:

$$\lambda_i \leq k - \frac{i(G)^2}{k + \lambda_i}$$

Before proceeding to the proof of Theorem 3.3, we remark that if we replace λ_i by $\lambda = max_{i \neq 1} \lambda_i$ in the statements of Theorem 3.3, the inequalities no longer hold (by considering the examples of bipartite graphs).

Proof: Let f be an eigenvector of the adjacency matrix M of G, where f is orthogonal to the all 1's vector. That is, $\sum_{v \in N} f(v) = 0$. Let $N_+ = \{v \in N : f(v) > 0\}$ and $N_- = N - N_+$. Without loss of generality, we can assume that $0 <| N_+ |\leq n/2$ since otherwise we can consider $-f$ instead. We also define a positive vector g so that $g(v) = f(v)$ if v is in N_+ and 0 otherwise. By the definition of λ_i, $Mf(v) = \lambda_i f(v)$ for all v in N. We may assume $\lambda_i > 0$ since the theorem holds for $\lambda_i \leq 0$. Then,

$$k - \lambda_i = \frac{\sum_{v \in N_+} (kf^2(v) - (Mf)(v) \cdot f(v))}{\sum_{v \in N_+} f^2(v)}$$

Since

$$\sum_{v \in N_+} (kf^2(v) - (Mf)(v) \cdot f(v))$$

$$= \sum_{u,v \in N_+} (f(u) - f(v))^2 + \sum_{u \in N_+} \sum_{v \in N_-} f(u)(f(u) - f(v))$$

$$\geq \sum_{\{u,v\} \in E} (g(u) - g(v))^2,$$

we have the following:

$$k - \lambda_i \geq w = \frac{\sum_{\{u,v\} \in E}(g(u) - g(v))^2}{\sum_{v \in N} g^2(v)} \tag{3}$$

Now we use the max-flow min-cut theorem [53] as follows. Consider the network with node set $\{s, t\} \cup N$ where s is the source, t is the sink. The directed edges and their capacities are given by:

- For every u in N_+, the directed edge (s, u) has capacity $\alpha = i(G)$.
- For every $\{u, v\} \in E$, there are two directed edges (u, v) and (v, u), each with capacity 1.
- For every $v \in N_-$, the directed edge (v, t) has capacity ∞ (or choose a large number such as kn.)

It is easy to check that this network has min-cut of size $\alpha \mid N_+ \mid$ by the definition of the isoperimetric number. By the max-flow min-cut theorem, there exists a flow function $h(u, v)$ for all directed edges in the network so that $h(u, v)$ is bounded above by the capacity of (u, v) and for each fixed v in N, we have

$$\sum_u h(u, v) = \sum_u h(v, u).$$

Furthermore, it is easy to modify h so that at most one of $h(u, v)$ and $h(v, u)$ is nonzero. Suppose α is an integer. It can be viewed that h specifies exactly $\alpha \mid N_+ \mid$ directed paths in G so that there are exactly α paths starting from a fixed node in N_+ and end at some node in N_-. In general, h specifies a set of paths $\mathcal{P}$, each of which associates with a weight $w(P)$ for $P \in \mathcal{P}$, and the total weight of paths starting from one specified node in N_+ is α. Back to (3), we have

$$\begin{aligned} w &= \frac{\sum_{\{u,v\} \in E}(g(u) - g(v))^2}{\sum_{v \in N_+} g^2(v)} \\ &= \frac{\sum_{\{u,v\} \in E}(g(u) - g(v))^2 \sum_{\{u,v\} \in E} h^2(u, v)(g(u) + g(v))^2}{\sum_{v \in N_+} g^2(v) \sum_{\{u,v\} \in E} h^2(u, v)(g(u) + g(v))^2} \end{aligned}$$

$$\geq \frac{(\sum_{\{u,v\}\in E} \mid h(u,v)(g^2(u)-g^2(v)) \mid)^2}{\sum_{v\in N_+} g^2(v)(\sum_{\{u,v\}\in E}(2g^2(u)+2g^2(v)-(g(u)-g(v))^2)}$$

$$\geq \frac{(\sum_{P\in\mathcal{P}} w(P)\sum_{(u,v)\in P} \mid g^2(u)-g^2(v) \mid)^2}{\sum_{v\in N_+} g^2(v)(2k\sum_{v\in N_+} g^2(v) - w\sum_{v\in N_+} g^2(v))}$$

$$\geq \frac{(\sum_{v\in N_+} \alpha g^2(v))^2}{(2k-w)(\sum_{v\in N_+} g^2(v))^2}$$

$$= \frac{\alpha^2}{2k-w} \geq \frac{\alpha^2}{2k}$$

This gives

$$\lambda_i \leq k - \frac{(i(G))^2}{k+\lambda_i} \leq k - \frac{(i(G))^2}{2k}$$

The proof of Theorem 3.3 in [95] does not use max-flow min-cut theorem and is probably simpler than the above proof. However, this proof follows from the natural correspondence of the isoperimetric number and the min-cuts and seems to be interesting on its own right. It is also similar to the proof of Alon in [2] which leads to the following upper bound of the second largest eigenvalue in terms of expansion. This bound is quite useful although it is often rather weak.

Theorem 3.4. A k-regular graph with expansion c has eignevalues λ_i satisfying

$$\lambda_i \leq k - \frac{(ck-1)^2}{6c^2k^2+4ck+6}$$

if $\lambda_i > 0$ and $\lambda_i \neq k$.

The proof of Theorem 3.4 follows from the fact that $|\Gamma(S)| \geq \frac{ck-1}{ck+1} \mid S \mid$ for all $\mid S \mid \leq \frac{n}{2}$ and the above inequality is an immediate consequence of results in [2].

We conclude this section by mentioning the following problems.

Conjecture 3.1 Suppose a k-regular graph G satisfies the property that $|e(S)-\rho\binom{|S|}{2} \mid < \alpha|S|$ for every subset S of nodes in G where ρ is the edge density. Then the second largest eigenvalue of G is upper bounded by αc for some absolute constant c. In other words, is it true that $\lambda \leq c \, disc \, G$?

Using Theorem 3.3, we have $\lambda \leq k - \frac{(\frac{k}{2} - 2 \, disc \, G)^2}{2k}$, which is about $\frac{7}{8}k + disc \, G$ for some graph G with small discrepancy. In a certain sense, Conjecture 3.1, if true, would be stronger and more natural than Theorem 3.3, the discrete version of Cheeger's inequality.

A slight variation of Conjecture 3.1 is the following:

Conjecture 3.2. Suppose a k-regular graph G satisfies the property that $|e(X,Y) - \rho|X||Y|| < \alpha\sqrt{|X||Y|}$ for every subset X and Y of $N(G)$ where $e(X,Y)$ denote the number of ordered pairs (x,y), $x \in X$, $y \in Y$ and $\{x,y\}$ is an edge. Then $\lambda \leq c \cdot \alpha$ for some constant c.

4. Explicit Constructions

We will give explicit constructions for dense and sparse graphs. For each construction, a bound for the second largest eigenvalue will be proved or discussed. Using theorems in Section 3, these constructions can therefore be shown to have good expansion and discrepancy properties. We will begin with graphs with edge density about $\frac{1}{2}$ and then proceed to graphs with lower edge density, say $\frac{k}{n}$ for fixed k.

Construction 4.1. The Paley graph Q_p.

Let p be a prime number congruent to 1 modulo 4. The Paley graph consists of p nodes, $0, 1, 2, \cdots, p-1$. Two nodes i and j are adjacent if and only if $i - j$ is a quadratic residue modulo p. Using 2.4.1, the eigenvalues of Q_p are exactly,

$$\sum_{x \in Z_p} e^{\frac{2\pi i j x^2}{p}}$$

for each $j = 0, \cdots, p-1$. This is closely related to Gauss sums modulo p (see [69]). In particular, it is known that for any $j \not\equiv 0 \pmod{p}$, the above sum is either $(\sqrt{p}-1)/2$ or $(-\sqrt{p}-1)/2$ and of course, the largest eigenvalue is $(p-1)/2$. Therefore, using results in Section 3, we conclude that the expansion of Q_p is $2 + O(\frac{1}{\sqrt{p}})$

and the discrepancy of Q_p is $O(\sqrt{p})$. It can also be shown that Q_p contains all subgraphs on $c\sqrt{\log\, p}$ nodes [15, 65].

Construction 4.2. The Paley sum graphs $\tilde{Q}_p$.

Let p be any prime number. $\tilde{Q}_p$ has node set $0, \cdots, p-1$, and two nodes i and j are adjacent if and only if $i+j$ is a quadratic residue modulo p. By 2.4.1, the eigenvalues of Q_p^* are $\frac{p-1}{2}$, and $(\pm\sqrt{p}-1)/2$.

The Paley graphs and Paley sum graphs both have edge density about $\frac{1}{2}$. This can be generalized to graphs with edge density $\frac{t}{r}$ for any fixed constants t and r with $t < r$. Paley sum graphs are actually a special case of the following:

Construction 4.3. The generalized Paley sum graphs $Q_{p,r,T}$.

For a fixed integer $r > 0$, let $p = mr + 1$ be a prime congruent to 1 mod 4 and let $T \subset \mathcal{Z}_p^*$ consist of t non-zero residues so that for any distinct $a, b \in T, ab^{-1}$ is not an rth power in $\mathcal{Z}_p^*$. The generalized Paley graph has node set $\{0, 1, \cdots, p-1\}$. Two nodes i and j are adjacent if and only if $i + j = aq$ for $a \in T$ and q is a rth power. The eigenvalues are $\sum_{x\in S} \zeta^{jx}$, where $\zeta = e^{2\pi i/p}$ and $S = \{aq : a \in T, q \text{ is a } r\text{th power}\}$.

For $j \neq 0$, we have

$$\begin{aligned} |\sum_{x\in S} \zeta^{jx}| &= \frac{1}{r} |\sum_{x\in Z_p} \sum_{a\in T} \zeta^{jax^r}| \\ &\leq \frac{1}{r} \sum_{a\in T} |\sum_{x\in Z_p} \zeta^{jax^r}| \\ &\leq \frac{1}{r} \sum_{a\in T} (r-1)\sqrt{p} \\ &= \frac{t(r-1)}{r}\sqrt{p} \end{aligned}$$

Therefore the generalized Paley sum graph $Q_{p,r,T}$ has expansion at least $\frac{r}{t(r-1)^2} + o(1)$ and discrepancy $\frac{t(r-1)}{r}\sqrt{p}$.

In the other direction, the Paley graph can be generalized to the following coset graphs on n nodes with edge density $n^{-1+\frac{1}{t}}$ for any positive integer t (see [27]).

Construction 4.4. The coset graphs $C_{p,t}$.

We consider the finite field $GF(p^t)$ and a coset $x + GF(p)$ for $x \in GF(p^t) \simeq GF(p)(x)$. There is a natural correspondence between elements of the multiplicative group $GF^*(p^t)$ and $1, \cdots, p^t - 1$. For example, choosing a generator g, each element y in $GF^*(p^t)$ corresponds to an integer k where $y = g^k$. Now we consider the coset graph $C_{p,t}$ with nodes $1, \cdots, p^t - 1 = n$, and edges $\{a, b\}$ if $a + b$ is in the subset X of integers corresponding to the coset $x + GF(p)$. The eigenvalues of the coset graph $C_{p,t}$ are $\sum_{a \in X} \theta^a$ for θ ranging over all nth roots of 1.

Bounding the eigenvalues of the coset graphs leads a natural generalization of Weil's character sum inequality. The following inequality was conjectured by the author [27] and proved by Katz [71] and others [74, 76]. Suppose θ is the $(p^t - 1)$-th root of 1 and $\theta \neq 1$, we have

$$| \sum_{a \in X} \theta^a | \leq (t-1)\sqrt{p}$$

The coset graph has edge density $n^{1-\frac{1}{t}}$, expansion at least $\frac{1}{(t-1)^2}$ and discrepancy at most $(t-1)\sqrt{p}$.

Construction 4.5. The Margulis graphs M_n.

In the early 70's, Margulis [78] ignited the whole area of constructive methods by relating Kazhdan's property T to expanders. This approach was later on successfully continued by Gabber and Galil [61] who obtained explicit values for estimating the expander constant. Here we construct 6-regular graphs, which we call Margulis graphs, similar to the constructions in [4, 61, 78]. Set $n = m^2$ and $V = Z_m \times Z_m$. Consider the following six transformations from V to itself.

$$\begin{aligned}
\sigma_1(x,y) &= (x, y+2x) \\
\sigma_2(x,y) &= (x, y+2x+1) \\
\sigma_3(x,y) &= (x, y+2x+2) \\
\sigma_4(x,y) &= (x+2y, y) \\
\sigma_5(x,y) &= (x+2y+1, y) \\
\sigma_6(x,y) &= (x+2y+2, y)
\end{aligned}$$

(all addition here is modulo m)

Let $G = M_n = (V, E)$ be a graph on V with edges $\{u, v\}$ if $u = \sigma_i(v)$ for some i. (Thus, e.g., $(0, 0)$ is joined to itself by 2 loops - note that here we consider as usual that a loop adds 2 to the degree of a node). Obviously, G is 12-regular. Furthermore, the second largest eigenvalue is at most $4+\sqrt{48} < 11$.

Claim 4.5.1.

$$\lambda < 4+\sqrt{48}$$

Proof: It suffices to show that for $f: V \to R, \sum f = 0$ and $f \not\equiv 0$, we have

$$(Af, f) \leq (12 - (8-\sqrt{48})) \cdot (f, f).$$

where A is the adjacency matrix of M_n.

Let T be the $(0,1)\times(0,1)$ torus, and define two measure-preserving automorphisms ψ_1, ψ_2 on T by $\psi_1(x,y) = (x, y+2x), \psi_2(x,y) = (x+2y, y)$, where the addition is modulo 1.

By Lemma 4 of [61] if ϕ is measurable on T and $\int_T \phi = 0$, then

$$\int_T |\, \phi \cdot \psi_1^{-1} - \phi \,|^2 + \int_T |\, \phi \cdot \psi_2^{-1} - \phi \,|^2 \geq c \int_T \phi^2, \qquad (4)$$

where $c = 4 - \sqrt{12}$.

Now suppose that $f: V \to R$ satisfies $\sum_{j,k=1}^{m} f(j,k) = 0$. Define a measurable function $\phi: T \to R$ as follows: If $(j,k) \in Z_m \times Z_m$ then for

$$\frac{j}{m} \leq x < \frac{j+1}{m}, \frac{k}{m} \leq y < \frac{k+1}{m}, \phi(x,y) = f(j,k).$$

Clearly $\int_T \phi = 0$.

It is easy to check that

$$\int_T |\, \phi \cdot \psi_1^{-1} - \phi \,|^2 + \int_T |\, \phi \cdot \psi_2^{-1} - \phi \,|^2$$

$$= \frac{1}{m^2}\Big[\frac{1}{2} \sum_{v\in V} \sum_{i=2,5} (f)(\sigma_i(v)) - f(v))^2 + \frac{1}{4} \sum_{v \in V} \sum_{i=1,3,4,6} (f(\sigma_i(v) - f(v))^2\Big]$$

$$\leq \frac{1}{2m^2} \sum_{(v,u)\in E} (f(v) - f(u))^2.$$

Also $\int_T \phi^2 = \frac{1}{m^2}\sum_{v\in V} f^2(v)$. Therefore, by (4) we have

$$\frac{1}{2m^2}\sum_{(v,u)\in E}(f(v)-f(u))^2 \geq \frac{c}{m^2}\sum_{v\in V} f^2(v),$$

Therefore

$$\sum f = 0 \text{ implies } \qquad \sum_{(v,u)\in E}(f(v)-f(u))^2 \geq 2c(f,f)$$

Since $(Af,f) = -\sum_{(v,u)\in E}(f(v)-f(u))^2 + 12(f,f)$, the last inequality implies $\lambda \leq 4+\sqrt{48}$. The claim is proved.

We can construct graphs with larger degrees and bounded eigenvalues by taking products of M_n as follows. The graph M_n^k has node set V, and two nodes u and v are joined by s parallel edges where s is the number of walks of length k in M_n from v to u. Thus the adjacency matrix of M_n^k has eigenvalues λ_i^k where λ_i are eigenvalues of M_n. Although this construction does not give as good eigenvalues as the following Ramanujan graphs, the construction schemes are simple and the approach is interesting.

Construction 4.6. The Ramanunjan graphs $X^{p,q}$.

One of the major developments in constructive methods is the construction of Ramanujan graphs by Lubotzky, Phillips and Sarnak [77] and independently by Margulis [79, 80, 81]. Ramanujan Graphs are k-regular graphs with eigenvalues (other than $\pm k$) at most $2\sqrt{k-1}$. For large n and a fixed k, this eigenvalue bound is the best possible, as mentioned in 2.4.

The construction can be described as follows: Let p be a prime congruent to 1 modulo 4 and let $H(Z)$ denote the integral quaternious

$$H(Z) = \{\alpha = a_o + a_1 i + a_2 j + a_3 k : a_j \in Z\}$$

Let $\bar{\alpha} = a_0 = a_1 i - a_2 j - a_3 k$ and $N(\alpha) = \alpha\bar{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2$. It can be shown that there are precisely $\frac{p+1}{2}$ conjugate pairs $\{\alpha, \bar{\alpha}\}$ of elements of $H(Z)$ satisfying $N(\alpha) = p, \alpha \equiv 1 (\bmod\ 2)$ and $a_0 > 1$. Denote by S the set of all such elements. For each α in S, we associate the matrix $\tilde{\alpha}$

$$\tilde{\alpha} = \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix}$$

Let q be another prime congruent to 1 modulo 4. By taking the i in $\tilde{\alpha}$ to be $i^2 \equiv -1 \pmod{q}$, $\tilde{\alpha}$ can be viewed as an element in $PGL(2, Z/qZ)$, which is the group of all 2×2 matrices over Z/qZ. Now we form the Cayley graph of $PGL(2, Z/qZ)$ relative to the above $p+1$ elements. (The Cayley graph of a group G relative to a symmetric set of elements S is the graph with node set G and edges $\{x, y\}$ if $x = sy$ for some s in S). If the Legendre symbol $\left(\frac{p}{q}\right) = 1$, then this graph is not connected since the generators all lie in the index two subgroup $PSL(2, Z/qZ)$, each element of which has determinant a square. So there are two cases. The Ramanujan graph $X^{p,q}$ is defined to be the above Cayley graph if $\left(\frac{p}{q}\right) = -1$, and to be the Cayley graph of $PSL(2, Z/qZ)$ relative to S if $\left(\frac{p}{q}\right) = 1$. For $\left(\frac{p}{q}\right) = -1$, $X^{p,q}$ is bipartite with edges between $PSL(2, Z/qZ)$ and its complement. The Ramanujan graphs of interest here correspond to taking $\left(\frac{p}{q}\right) = 1$ and are $(p+1)$-regular graphs with $q(q^2-1)/2$ nodes.

In addition, the second largest eigenvalue can be shown to be $2\sqrt{p}$ by using the results of Eichler [41] on the Ramanujan conjecture [77, 91]. Therefore the Ramanujan graphs have expansion about $\frac{1}{4}$ and discrepancy $2\sqrt{p}$.

5. Applications in communication networks

Among various applications of expander graphs, their applications in communication networks have the longest history and provide the motivation and formulation of the problem [23, 78, 88, 89]. One of the networks of interest is a non-blocking network which can be viewed as a directed graph with two specified disjoint subsets of nodes, one of which consists of input nodes and the other consists of output nodes. Now suppose that a number of calls take place in the network, i.e., there are node-disjoint paths joining some inputs to outputs in the graph. Suppose one additional call comes in and it is desired to establish a new path joining the given input to the given output without disturbing the existing calls, i.e., the new path is node-disjoint from the existing paths. The problem is to minimize

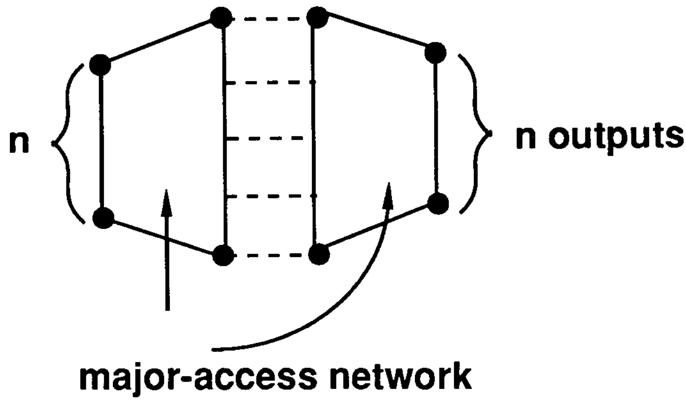

Figure 1: a nonblocking network

the number of edges in such a non-blocking network. To build a non-blocking network, we need several types of building blocks, one of which is called a k-access graph which has the property that, for any given set S of node-disjoint paths connecting inputs to outputs, a new input can be connected to k different outputs by paths not containing any node in S. If k is greater than or equal to half of the total number of outputs, the k-access graph is so-called a *major access* network. A non-blocking network can then be built by combining a major access network and its mirror image as shown in Fig. 1.

We construct here a major-access network $M(n)$ with n inputs and $24n$ outputs by combining 2 copies of $M(n/2)$ and 2 copies of bipartite Ramanujan $R(12n, 5)$ graphs with $12n$ inputs and with degree $p + 1 = 6$, as illustrated in Fig. 2.

To verify the above construction is a major-access network, we consider an inputs v which must have access to $6n$ of the middle nodes. After deleting the possible n nodes in S, the remaining set has at least $5n$ inputs of $M(n)$. In each of the Ramanujan graph with $k = 6$ and $\lambda = 2\sqrt{5}$, we have

$$\frac{k^2 5n}{(k^2 - \lambda^2)\frac{5}{12} + \lambda^2} = \frac{27n}{4}$$

Among the $\frac{27}{2}n$ such outputs, there are at least $\frac{25}{2}n$ of them not in S which is more than half of the outputs of $M(n)$. Therefore the above construction yields $M(n)$ satisfying

$$| M(n) | = 2 \mid M(\frac{n}{2}) \mid + 6 \cdot 12 \cdot 2n$$

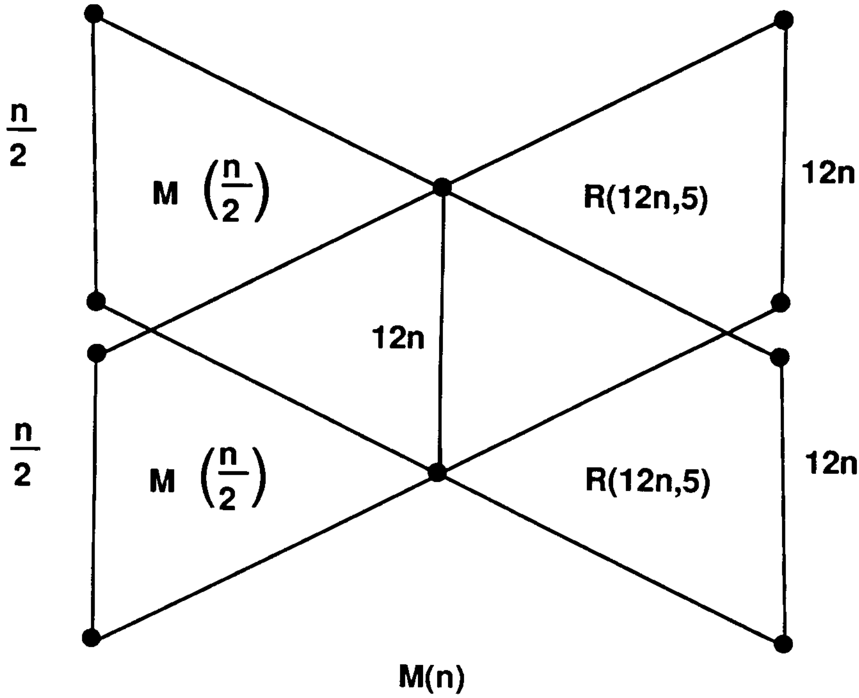

Figure 2: a major access network

It can then be easily checked that the above major-access network has at most $144n\ \log\ n$ edges and therefore the nonblocking network has at most $288n\ \log\ n$ edges.

Another useful network is the so called *superconcentrator.* Despite this impressive name, it actually has very simple property. Namely, it is a graph with n inputs and n outputs, having the property that, for any set of inputs and any set of outputs, a set of node-disjoint paths exists that join the inputs in a one-to-one fashion to the outputs (although it does not matter here who is connected to whom!) The question of interest is to determine how few edges a superconcentrator can have. In fact, this has been taken as a measure to compare the effectiveness of the expanders which are used to build superconcentrators. Here is a simple recursive construction [78] for a superconcentrator in Figure 3.

In the network in Figure 3, there is a matching between the n inputs and n outputs Furthermore, the graph B has n inputs and $5n/6$ outputs satisfying the property that for any given $n/2$ inputs there is a set of node-disjoint paths joining the inputs in a one-to-one fashion to different outputs. For example, as defined in Section 2.3,

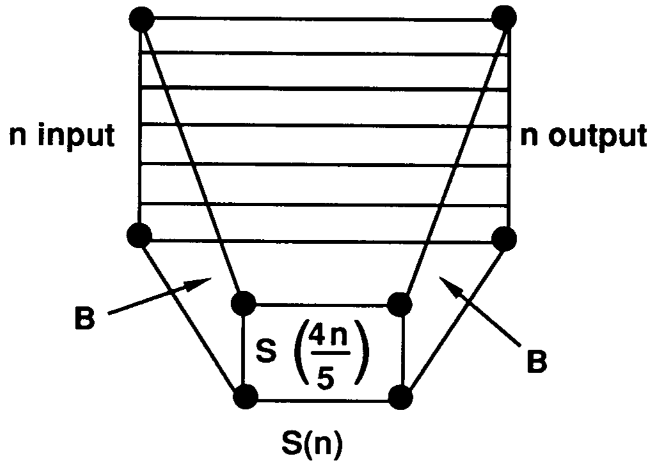

Figure 3: a superconcentrator

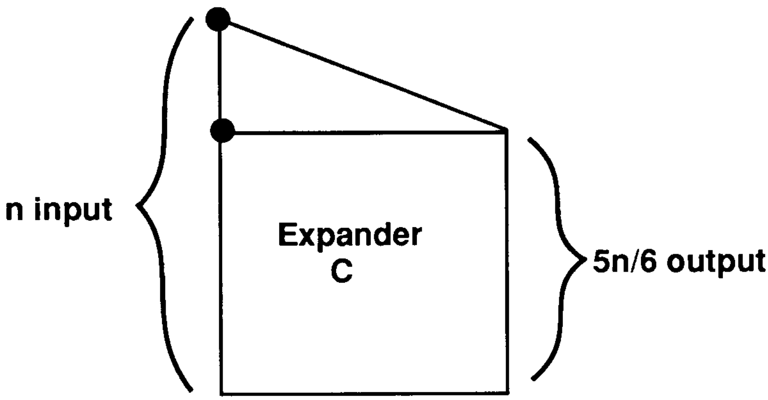

Figure 4: a concentrator

an $(n, 5/6, k, 1/2, 1/2)$-concentrator has the above property. So for any given set of m inputs and m outputs in $S(n)$ of Figure 3, we can use the matching to provide $m - n/2$ disjoint paths and let the rest be taken care of recursively by $S(\frac{5n}{6})$. Therefore the key part of the construction is made of an expander as in Figure 4.

In Figure 4, the first $n/6$ inputs, each having degree 5, are joined to $5n/6$ distinct outputs. The remaining $5n/6$ inputs are joining to the outputs by a Ramanujan graph with degree $6 = p + 1$. Now suppose we have a set of inputs X. It suffices to show that X has at least $\mid X \mid$ neighbors as outputs. Here we verify the situation for $\mid X \mid = n/2$, (where the other cases of $\mid X \mid < n/2$ are easier). If

X contains at least $\frac{n}{10}$ inputs among the first $\frac{n}{6}$ inputs, then we are done. We may assume X contains at least $\frac{2n}{5}$ inputs as an input set X' of the expander C. Since the expander graph has the second largest eigenvalue $2\sqrt{5}$, it is straightforward to check that

$$\Gamma(X') \geq \frac{k^2 \mid X' \mid}{(k^2 - \lambda^2)\frac{|X'|}{\frac{5}{6}n} + \lambda^2} \geq \frac{36 \cdot \frac{2}{5}n}{16 \cdot \frac{12}{25} + 20} > n/2$$

Now the total number of edges in the superconcentrator $S(n)$ satisfies

$$\begin{aligned} S(n) &= n + 2 \mid B \mid + S(5n/6) \\ &= n + 2 \cdot 5/6n \cdot 7 + S(5n/6) \end{aligned}$$

It is easy to verify that the above superconcentrator $S(n)$ has at most $76n$ edges. The number of edges in $S(n)$ can be reduced to $69.8n$ by replacing $S(\frac{5}{6}n)$ by $S((\frac{4}{5} + \epsilon)n)$ where $\epsilon = .0288776$ and in B each of the first $(\frac{1}{5} - \epsilon)n$ inputs of B has degree 4 or 5, and are joined to a total of $(\frac{4}{5} + \epsilon)n$ distinct outputs of B. This construction is based on standard methods as described in [61]. The widely quoted number $58n$ for the edge number of a superconcentrator with n inputs and n outputs does not seem to be obtainable by the above methods. It is a challenge to improve on the above bounds or even to construct a superconcentrator $S(n)$ of $58n$ edges.

It is worth mentioning that by using expanders guaranteed by probabilistic methods [5], one can have superconcentrators of $36n$ edges. The best current lower bound for superconcentrator of size n is $5n + O(logn)$, due to Lev and Valiant [75].

6. Other extremal properties

There are many related extremal properties that are satisfied by random graphs but are "weaker" than the properties mentioned in Section 2. One such example is the diameter, which is defined to be the maximum distance between pairs of nodes. There are graphs with small diameter but not having expansion, discrepancy or eigenvalue properties.

A random graph has small diameter. To be specific, Bollobas and de la Vega [16] proved that a random k-regular graph has diameter $\log_{k-1} n + \log_{k-1} \log\ n + c$ for some small constant $c < 10$. This is almost best possible in the sense that any k-regular graph has diameter at least $\log_{k-1} n$. An upper bound for the diameter in terms of eigenvalues was derived in [27]. Namely, a k-regular graph G on n nodes has diameter at most $\lceil \frac{\log(n-1)}{\log(k/\lambda)} \rceil$ where λ is the absolute second largest eigenvalue. Recently, further improvement was made in [29] by showing that a k-regular graph G on n nodes has diameter at most $\lceil \frac{arc\ cosh(n-1)}{arc\ cosh(k/\lambda)} \rceil$.

Using the above bound, the Ramanujan graph has diameter at most $\lceil \frac{\log\ n}{\log(k/\lambda)} \rceil$ which falls within a factor 2 of the optimum. This is closely related to the following extremal problem which often arises in interconnection networks [42].

Problem 6.1. Given k and D, construct a graph with as many nodes as possible with degree k and diameter D.

It is not difficult to see that such graphs can have at most $M(k, D) = 1 + k + \cdots + k(k-1)^{i-1} + \cdots + k(k-1)^{D-1}$ nodes, which is sometimes called the Moore bound. The Ramanujan graph achieves about a factor 2^{-D} times the Moore bound [67]. Quite a few other constructions such as de Bruijn graphs [18] and their variations also fall in the range of 2^{-D} of the Moore bound. It remains an open problem to determine the maximum number $n(k, D)$ of nodes in a graph with degree and diameter D. Relatively little is known about the upper bound for $n(k, D)$. The following somewhat trivial sounding question concerning the upper bound is still unresolved [44]:

Problem 6.2. Is it true that for every integer c, there exist k and D such that $n(k, D) < M(k, D) - c$?

Except for a small number of cases [44, 67], it is known that $n(k, D) < M(k, D)$; the reader is referred to [7, 8, 21, 25, 26] for a brief survey on this topic.

Another direction is to allow additional edges to minimize diameter:

Problem 6.3. How small can the diameter be by adding a matching to an n-cycle?

It was shown in [14] that by adding a random matching to an n-cycle the resulting graph has best possible diameter in the range of $\log_2 n$. In fact, a more general theorem can be proved so that by adding a random matching to k-regular graphs, say Ramanujan graphs, the resulting graphs have diameter about $\log_{k-1} n$. It would be of interest to answer Problem 6.3 and its generalization by explicit constructions [3, 6, 30, 58, 105].

Another related graph invariant is the girth of the graph which is the size of the smallest cycle in the graph [9, 68, 108]. The girth of a random k-regular graph was shown to be $\log_{k-1} n$ [48]. In [77], it was shown that the Ramanujan graphs have girth $\frac{4}{3}\log_{k-1} n$; which is better than that of a random graph in the sense of avoiding small cycles. This is closely related to the following old extremal problem which is still open [17, 96]:

Problem 6.4. For a given integer t, how many edges can a graph on n nodes have without containing any cycle of length $2t$?

Erdös conjectures that the maximum number $f(n,t)$ of edges in a graph on n nodes avoiding C_{2t} is $O(n^{1+\frac{1}{t}})$. It is not hard to see $f(n,t) < n^{1+\frac{1}{t}}$. The Ramanujan graphs yield $f(n,t) > n^{1+\frac{2}{3t}}$ which is a substantial improvement upon previous lower bounds of $n^{1+\frac{1}{2t-1}}$ in [17].

The above Problem 6.4 is a special case of a whole class of Túran-type extremal problems. For any fixed graph H, the Túran number is the maximum number of edges in a graph on n nodes avoiding H. There is a great deal of literature on these problems (see [12, 45, 47, 49]) but this topic is somewhat outside the scope of this paper. Conceivably, for each extremal property, say independence number, chromatic number, connectivity and so on, a similar question can be posed by comparing the best explicit construction with the probabilistic ones. Numerous problems remain to be explored.

Acknowledgement:

The author wishes to thank Bill Kantor (for discussions on Ramanujan graphs), Hendrik Lenstra (for discussions on character sums), Noga Alon (for discussions on expanders,Milena Mihail (for a careful reading) and Ron Graham for inspiring comments.

References

[1] H.L. Abbott, Lower bounds for some Ramsey numbers, *Discrete Math.* **2** (1972) 289-293.

[2] N. Alon, Eigenvalues and expanders, *Combinatorica* **6** (1986) 83-86.

[3] N. Alon and F.R.K. Chung, Explicit constructions of linear-sized tolerant networks, *Discrete Math.* **72** (1988) 15-20.

[4] N. Alon, Z. Galil and V.D. Milman, Better expanders and superconcentrators, *J. Algorithms* **8** (1987) 337-347.

[5] L.A. Bassalygo, Asymptotically optimal switching circuits, *Problems Inform. Transmission* **17** (1981) 206-211.

[6] J. Beck, On size Ramsey number of paths, trees and circuits I., *J. Graph Theory* **7** (1983) 115-129.

[7] J.C. Bermond and B. Bollobás, The diameter of graphs – a survey, *Proc. in Congressus Numerantium* **32** (1981) 3-27.

[8] J.C. Bermond, C. Delorme and G. Farhi, Large graphs with given degree and diameter III, *In Proc. Coll. Cambridge* (1981). *Ann. Discr. Math.* **13**, North Holland (1982) 23-32.

[9] N.L. Biggs and M.H. Hoare, The sexlet construction for cubic graphs, *Combinatorica* **3** (1983) 153-165.

[10] F. Bien, Constructions of telephone networks by group representations, *Notices Amer. Math. Soc.* **36** (1989) 5-22.

[11] M. Blum, R. M. Karp, O. Vornberger, C. H. Papadimitriou, and M. Yannakakis, The complexity of testing whether a graph is a superconcentrator, *Inf. Proc. Letters* **13** (1981) 164-167

[12] B. Bollobás, Extremal Graph Theory, Academic Press, London (1978).

[13] B. Bollobás, Random Graphs, *Academic Press,* New York (1987).

[14] B. Bollobás and F.R.K. Chung, The diameter of a cycle plus a random matching,*SIAM J. on Discrete Mathematics* **1** (1988) 328-333

[15] B. Bollobás, and A. Thomason, Graphs which contain all small graphs, *European J. of Combinatorics* **2** (1981) 13-15.

[16] B. Bollobás and W.F. de la Vega, The diameter of random graphs, *Combinatorica* **2** (1982) 125-134.

[17] J.A. Bondy and M. Simonovits, Cycles of even length in graphs, *J. Combin. Theory Ser. B* **16** (1974) 97-105.

[18] N.G. de Bruijn, A combinatorial problem, *Nederl. Akad. Wetensch. Proc.* **49** (1946) 758-764.

[19] D.A. Burgess, On character sums and primitive roots, *Proc. London Math. Soc.* **12** (1962) 179-192.

[20] P. Buser, Cubic graphs and the first eigenvalue of a Riemann surface, *Math. Z.* **162** 1978) 87-99

[21] L. Caccetta, On extremal graphs with given diameter and connectivity, *Ann. New York Acad. Sci.* **328** (1979) 76-94.

[22] J. Cheeger, A lower bound for the smallest eigenvalue of the Laplacian, Problems in Analysis, edited by R.C. Gunning, Princeton Univ. Press (1970) 195-199.

[23] F.R.K. Chung, On concentrators, superconcentrators, generalizers and nonblocking networks, *Bell Systems Tech. J.* **58** (1978) 1765-1777.

[24] F.R.K. Chung, A note on constructive methods for Ramsey numbers, *J. Graph Th.* 5 (1981) 109-113.

[25] F.R.K. Chung, Diameters of communications networks, *Mathematics of Information Processing*, AMS Short Course Lecture Notes (1984) 1-18.

[26] F.R.K. Chung, Diameters of graphs: Old problems and new results, *Congressus Numerantium* **60** (1987) 295-317.

[27] F.R.K. Chung, Diameters and eigenvalues, *J. of AMS* **2** (1989) 187-196.

[28] F.R.K. Chung, Quasi-random classes of hypergraphs, Random Structures and Algorithms, 1 (1990) 363-382

[29] F.R.K. Chung, V. Faber and T. Manteuffel, An upper bound on the diameter of a graph from eigenvalues of its Laplacian, preprint.

[30] F.R.K. Chung and M.R. Garey, Diameter bounds for altered graphs, *J. of Graph Theory*, **8** (1984) 511-534.

[31] F.R.K. Chung and R.L. Graham, Quasi-random hypergraphs, *Random Structures and Algorithms* **1** (1990) 105-124.

[32] F.R.K. Chung and R.L. Graham, Quasi-random tournaments (to appear in *J. of Graph Theory).*

[33] F.R.K. Chung and R.L. Graham, Maximum cuts and quasi-random graphs (to appear).

[34] F.R.K. Chung and R.L. Graham, On graphs with prescribed induced subgraphs (to appear).

[35] F.R.K. Chung and R.L. Graham, Quasi-random set systems (to appear).

[36] F.R.K. Chung and R.L. Graham, Quasi-random subsets of Z_n (to appear in *J. Combin. Th. (A)*).

[37] F.R.K. Chung, R.L. Graham and R.M. Wilson, Quasi-random graphs, *Combinatorica* **9** (1989) 345-362.

[38] F.R.K. Chung and C.M. Grinstead, A survey of bounds for classical Ramsey numbers, *J. of Graph Theory* **7** (1983) 25-38.

[39] F.R.K. Chung and P. Tetali, Communication complexity and quasi-randomness preprint.

[40] P.J. Davis, Circulant Matrices, John Wiley and Sons, New York (1979).

[41] M. Eichler, Quaternary quadratic forms and the Riemann hypothesis for congruence zeta functions, *Arch. Math.* **5** (1954) 355-366.

[42] B. Elspas, Topological constraints on interconnection limited logic, *Switching Circuit Theory and Logical Design* **5** (1964) 133-147.

[43] P. Erdös, Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.* **53** (1947) 292-294.

[44] P. Erdös, S. Fajtlowicz and A.J. Hoffman, Maximum degree in graphs of diameter 2, *Networks* **10** (1980) 87-90.

[45] P. Erdös and A. Hajnal, On spanned subgraphs of graphs, *Betrage zur Graphentheorie und deren Anwendungen*, Kolloq. Oberhof (DDR), (1977) 80-96.

[46] P. Erdös and A. Rényi, On a problem in the theory of graphs, *Publ. Math. Inst. Hungar. Acad. Sci.* **7** (1962) 623-641.

[47] P. Erdös, A. Rényi and V.T. Sós, On a problem of graph theory, *Studia Sci. Math. Hungar.* **1** (1966) 215-235.

[48] P. Erdös and H. Sachs, Reguläre Graphen gegenebener Teillenweite mit Minimaler Knotenzahl, Wiss. Z. Univ. Halle – Wittenberg, *Math. Nat. R.* **12** (1963), 251-258.

[49] P. Erdös and V.T. Sös, On Ramsey-Turán type theorems for hypergraphs, *Combinatorica* **2** (1982) 289-295.

[50] P. Erdös and J. Spencer, Imbalances in k-colorations, *Networks* **1** (1972) 379-386.

[51] P. Erdös and J. Spencer, Probabilistic Methods in Combinatorics, Academic Press, New York (1974).

[52] R.J. Faudree and M. Simonovits, On a class of degenerate extremal graph problems, *Combinatorica* **3** (1983) 97-107.

[53] L.R. Ford and D.R. Fulkerson, Flows in Networks, Princeton Univ. Press (1962).

[54] P. Frankl, A constructive lower bound for some Ramsey numbers, *Ars Combinatoria* 3 (1977) 297-302.

[55] P. Frankl, V. Rödl and R.M. Wilson, The number of submatrices of given type in a Hadamard matrix and related results, *J. Combinatorical Th. (B)* **44** (1988) 317-328.

[56] P. Frankl and R.M. Wilson, Intersection theorems with geometric consequences, *Combinatorica* **1** (1981) 357-368.

[57] Joel Friedman, On the second eigenvalue and random walks in random d-regular graphs, preprint.

[58] J. Friedman and N. Pippenger, Expanding graphs contain all small trees, *Combinatorica* **7** (1987) 71-76.

[59] G. Frobenius, Über Matrizen aus nicht negative Elementen, Sitzber. Akad. Wiss. Berlin (1912) 456-477.

[60] Z. Füredi and J. Komlós, The eigenvalues of random symmetric matrices, *Combinatorica* **1** (1981) 233-241.

[61] O. Gabber and Z. Galil, Explicit construction of linear sized superconcentrators, *J. Comput. System Sci.* **22** (1981) 407-420.

[62] F.R. Gantmacher, The Theory of Matrices, Vol. 1, Chelsea Pub. Co., New York (1977).

[63] R.L. Graham and V. Rödl, Numbers in Ramsey theory, Surveys in Combinatorics (1987), (C. Whitehead, ed.) London Math. Soc. Lecture Notes Series 123, 111-153.

[64] S.W. Graham and C. Ringrose, Lower bounds for least quadratic non-residues (to appear).

[65] R.L. Graham and J.H. Spencer, A constructive solution to a tournament problem, *Canad. Math. Bull.* **14** (1971) 45-48.

[66] J. Haviland and A. Thomason, Pseudo-random hypergraphs, *Discrete Math.* **75** (1989) 255-278.

[67] A.J. Hoffman and R.R. Singleton, On Moore graphs with diameter 2 and 3, *IBM J. of Res. Development* **4** (1960) 497-504.

[68] W. Imrich, Expicit construction of regular graphs without small cycles, *Combinatorica* **4** (1984) 53-59.

[69] K. Ireland and M. Rosen, A classical introduction to modern number theory, Springer-Verlag, New York 1982.

[70] F. Juhász, On the spectrum of a random graph, *Colloq. Math. Soc. Jánoos Bolyai* **25**, *Algebraic Methods in Graphs Theory*, Szeged (1978) 313-316.

[71] N.M. Katz, An estimate for character sums, *J. Amer. Math. Soc.* **2** (1989) 197-200.

[72] M. Klawe, Non-existence of one-dimensional expanding graphs, *22nd Symposium on Foundations of Computer Science*, (1981) 109-113.

[73] T. Lengauer and R.E. Tarjan, Asymptotically tight bounds on time space tradeoffs in a pebble game, *J. Assoc. Comput. Mach.* **29** (1982) 1087-1130.

[74] H. Lenstra, personal communication.

[75] G. Lev, Size bounds and parallel algorithms for networks, Thesis, Department of Computer Science, University of Edinburg.

[76] W. Li, Character sums and abelian Ramanujan graphs, preprint.

[77] A. Lubotsky, R. Phillips and P. Sarnak, Ramanujan graphs, *Combinatorica* **8** (1988) 261-278.

[78] G.A. Margulis, Explicit constructions of concentrators, *Problemy Peredaci Informacii* **9** (1973) 71-80 (English transl. in *Problems Inform. Transmission* **9** (1975) 325-332.

[79] G.A. Margulis, Arithmetic groups and graphs without short cycles, *6th Internat. Symp. on Information Theory, Tashkent* (1984) *Abstracts* **1** 123-125, (in Russian).

[80] G.A. Margulis, Some new constructions of low-density parity-check codes, *3rd Internat. Seminar on Information Theory, convolution codes and multi-user communication, Sochi* (1987) 275-279 (in Russian).

[81] G.A. Margulis, Explicit group theoretic constructions of combinatorial schemes and their applications for the construction of expanders and concentrators, *Journal of Problems of Information Transmission* (1988) (in Russian).

[82] B. Mohar, Isoperimetric number of graphs,*J. of Comb. Theory (B)* **47** (1989), 274-291.

[83] H.L. Montgomery, Topics in multiplicative number theory, *Lecture Notes in Math.* **227**, Springer-Verlag, New York (1971).

[84] Zs. Nagy, A constructive estimation of the Ramsey numbers, *Mat. Lapok* **23** (1975) 301-302.

[85] E.M. Palmer, Graphical Evolution, Wiley, New York (1985).

[86] W.J. Paul, R.E. Tarjan and J.R. Celoni, Space bounds for a game on graphs, *Math. Soc. Theory* **10** (1977) 239-251.

[87] O. Perron, Zur Theorie der Matrizen, *Math. Ann.* **64** (1907) 248-263.

[88] M. Pinsker, On the complexity of a concentrator, 7th Internat. Teletraffic Conf., Stockholm, June 1973, 318/1-318/4.

[89] N. Pippenger, Superconcentrators, *SIAM J. Comput.* **6** (1977) 298-304.

[90] N. Pippenger, Advances in pebbling, *Internat. Collow. On Automation Languages and Programming*, Vol. 9 (1982) 407-417.

[91] S. Ramanujan, On certain arithmetical functions, *Trans. Cambridge Philos. Soc.* 22 (9) (1916) 159-184.

[92] F.P. Ramsey, On a problem of formal logic, *Proc. London Math. Soc.* **30** (1930), 264-286.

[93] V. Rödl, On the universality of graphs with uniformly distributed edges, *Discrete Math.* **59** (1986) 125-134.

[94] M. Simonovits and V.T. Sós, Szemerédi partitions and quasi-randomness (to appear in *Random Structures and Algorithms)*.

[95] A.J. Sinclair and M.R. Jerrum, Approximate counting, uniform generation, and rapidly mixing markov chains (to appear in *Information and Computation*).

[96] R. Singleton, On minimal graphs of maximum even girth, *J. Combin. Theory* **1** (1966) 306-332.

[97] J. Spencer, Optimal ranking of tournaments, *Networks* **1** (1971) 135-138.

[98] J. Spencer, Ramsey's theorem – A new lower bound, *J. Combinatorial Theory* **18** (1975) 108-115.

[99] R.M. Tanner, Explicit construction of concentrators from generalized N-gons, *SIAM J. Algebraic Discrete Methods* **5** (1984) 287-294.

[100] A. Thomason, Random graphs, strongly regular graphs and pseudo-random graphs, in Survey in Combinatorics (1987) (C. Whitehead, ed.) LMS.

[101] A. Thomason, Pseudo-random graphs, Proc. Random Graphs, Poznán (1985) (M. Karónski, ed.), *Annals of Discrete Math.* **33** (1987) 307-331.

[102] A. Thomason, Dense expanders and pseudo-random bipartite graphs, *Discrete Math.* **75** (1989) 381-386.

[103] M. Tompa, Time space tradeons for computing using connectivity properties of the circuits, *J. Comput. System Sci.* **10** (1980) 118-132.

[104] L.G. Valiant, Graph theoretic properties in computational complexity, *J. Comput. System Sci.* **13** (1976) 278-285.

[105] K. Vijayan and U.S.R. Murty, *Sankhya Ser. A.* **26** (1964) 299-302.

[106] A. Weil, Sur les courbes algébrique et les variétés qui s'en déduisent, *Actualités Sci. Ind.* No. 1041 (1948).

[107] R. M.. Wilson, Constructions and uses of pairwise balanced designs, in Combinatorics (M. Hall, Jr., and J.H. van Lint, eds.) Math Centre Tracts 55, Amsterdam (1974) 18-41.

[108] A. Weiss, Girths of bipartite sextet graphs, *Combinatorica* **4** (1984) 241-245.