

DIAMETERS AND EIGENVALUES

F. R. K. CHUNG

1. INTRODUCTION

In a graph (or directed graph) G , the distance $d(u, v)$ of two vertices is defined to be the length of the shortest path (or directed path) joining u to v . The diameter $D(G)$ is then the maximum distance among all $\binom{n}{2}$ pairs of vertices. The underlying graphs of various communications networks are often required to have small diameters so that information can be transmitted efficiently in the network.

Let M denote the adjacency matrix of G with eigenvalues $\lambda_1, \lambda_2, \dots$ where $|\lambda_1| \geq |\lambda_2| \geq \dots$. Suppose G is k -regular so that all row sums and column sums of M are equal to k . A well-known theorem of Frobenius states that $\lambda_1 = k$. Let λ denote $|\lambda_2|$. We will show that the diameter is small if λ is small compared to k . In particular, we will derive the following upper bound:

$$(1) \quad D(G) \leq \lceil \log(n-1) / \log(k/\lambda) \rceil.$$

This improves a previous bound given by Alon and Milman [2] who showed that $D(G) < 2\sqrt{2k/(k-\mu)} \log_2 n$ (by considering the expanding properties of G) where μ^2 is the second largest eigenvalue of $M^T M$. If G is a directed graph, (1) still holds provided that the eigenvectors of M satisfy certain properties. We note that for undirected graphs, M is symmetric and $\lambda = \mu$. However, for directed graphs, M is not symmetric, in general, and only the inequality $\mu \geq \lambda$ holds. As we shall see in the next section, a graph has nice expanding properties if μ is small. When μ is large and λ is small, the graph is not necessarily an expander. Still, it can often be shown to have a small diameter.

In the first half of the paper, we will give the proof of the diameter bounds using eigenvalues. In the second half, we will consider families of graphs whose eigenvalues can be precisely identified. These graphs have rather simple structures. Namely, a k -sum graph on n vertices can be specified by a set of k integers between 1 and n . A pair $\{i, j\}$ is an edge if and only if $i + j \pmod{n}$ is one of the k integers. We also define directed graphs, the so-called k -difference graphs, where $i \rightarrow j$ is an edge if $i - j$ is one of the specified integers. We will

Received by the editors February 10, 1988.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 05Cxx.

©1989 American Mathematical Society
0894-0347/89 \$1.00 + \$.25 per page

demonstrate that certain choices for the k integers result in small values of λ by using the following inequality on character sums, which was recently proved by N. M. Katz [25]. Although this inequality was motivated by the construction of sum graphs, it is of potential use in many other problems.

Let Ψ denote a nontrivial complex-valued multiplicative character defined on an extension field E over a finite field K with dimension t . Then for any $x \in E$ such that $E = K(x)$ we have $|\sum_{a \in K} \Psi(x + a)| \leq (t - 1)\sqrt{|K|}$.

These k -sum graphs and k -difference graphs can be shown to be good expanders with small diameters. The diameter bound is closely related to the following theorem.

For a prime p in $GF(p^t) \simeq GF(p)[x]/(F(x))$, every element in $GF(p^t)$ can be represented as a product of $x + i$, $i \in GF(p)$, such that the number of the $x + i$'s needed is no more than $2t + 4t \log t / (\log p - 2 \log(t - 1))$.

The paper is organized as follows. In §2, we give the proof of the diameter bound (1). In §3, we first briefly discuss constructive methods and the expanders. Then we construct the sum graphs and difference graphs. In §4 we consider the eigenvalues of sum graphs and difference graphs. These eigenvalues can be bounded from above by considering character sums. We then show these graphs are expanders with small diameters. In §5, we discuss some other extremal properties and applications of these graphs.

2. DIAMETER BOUNDS

Theorem 1. *For a k -regular graph G with second largest eigenvalue λ (in absolute value), we have $D(G) \leq \lceil \log(n - 1) / \log(k/\lambda) \rceil$.*

Proof. Let M denote the adjacency matrix of a k -regular graph G on n vertices. We want to determine D , which is the minimum value of m such that M^m has all entries nonzero. Let v^* denote the n -tuple with all entries 1. Let u_1, u_2, \dots, u_n denote orthonormal eigenvectors with eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_n$ where $u_1 = v^* / \sqrt{n}$, $\lambda_1 = k$, and $|\lambda_i| \leq \lambda$ for $i \neq 1$.

Then clearly we have $M = \sum_i \lambda_i u_i u_i^*$ where u_i is an n by 1 matrix and u_i^* denotes the transpose of u_i .

$$\begin{aligned} (M^m)_{r,s} &= \sum_i \lambda_i^m (u_i u_i^*)_{r,s} \\ &\geq k^m/n - \left| \sum_{i>1} \lambda_i^m (u_i)_r (u_i)_s \right| \\ &\geq k^m/n - |\lambda|^m \left\{ \sum_{i>1} |(u_i)_r| |(u_i)_s| \right\} \\ &\geq k^m/n - |\lambda|^m \left\{ \sum_{i>1} |(u_i)_r|^2 \right\}^2 \left\{ \sum_{i>1} |(u_i)_s|^2 \right\}^2 \\ &= k^m/n - |\lambda|^m \{1 - (u_1)_r^2\}^2 \{1 - (u_1)_s^2\}^2 \end{aligned}$$

$$\begin{aligned}
 &= k^m/n - |\lambda|^m(1 - 1/n) \\
 &> 0
 \end{aligned}$$

if $(k/\lambda)^m > n - 1$.

This implies $D(G) \leq \lceil \log(n - 1)/\log(k/\lambda) \rceil$ and the proof for Theorem 1 is complete.

We remark that the diameter upperbound is tight for some graphs, such as the complete graphs.

Theorem 1 can be extended to nonregular graphs by slightly modifying the preceding proof.

Theorem 2. For a graph G with eigenvalues $\lambda_1, \lambda_2, \dots$ where $|\lambda_1| \geq |\lambda_2| \geq \dots$, and $w = \min_i |(u_1)_i|$, we have $D(G) \leq \lceil \log((1 - w^2)/w^2)/\log(|\lambda_1|/|\lambda_2|) \rceil$.

Before we proceed to the directed case, we first consider a generalized inner product for vectors in \mathbb{C}^n . The product of two vectors u and v is defined as the sum of the product of u_i and the conjugate of v_i . That is $\langle u, v \rangle = \sum_i u_i \cdot \bar{v}_i$. We say u and v are orthogonal if $\langle u, v \rangle = 0$.

Theorem 3. Suppose a directed graph G has outdegree k and eigenvectors of G form an orthogonal basis. Then we have $D(G) \leq \lceil \log(n - 1)/\log(k/\lambda) \rceil$, where λ is the second largest eigenvalue (in absolute value) of the adjacency matrix M of G .

Proof. The proof is quite similar to that of Theorem 1, except that X^* now denotes the conjugate transpose of a matrix X . That is $(X^*)_{r,s} = (\bar{X})_{s,r}$. The rest of the calculation is straightforward and will be omitted.

We remark that the condition that the eigenvectors form an orthogonal basis is essential. The directed graph with the following adjacency matrix A has eigenvalues 2, 0, -1, and -1.

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}.$$

However the diameter of A is ∞ , as pointed out by Herbert S. Wilf (personal communication).

3. SUM AND DIFFERENCE GRAPHS AS EXPANDER GRAPHS

Expander graphs first came up in connection with permutation networks in the early 1970s [30]. Since then the fundamental properties of expander graphs have led to many applications in a variety of areas ranging from extremal graph theory [7, 10] to parallel sorting [1], graph pebbling [27, 33, 32], connection networks [4, 30], and computational complexity [23, 33, 39]. An expander graph G is a graph with the property that any set X of vertices, with $|X|$ small in comparison with $|V(G)|$, has at least $\beta|X|$ neighbors, where β is

proportional to the average degree of G . It is not difficult to check that random regular graphs (in fact, almost all r -regular graphs) are expander graphs. Like many other combinatorial problems, “good” configurations are assured by probabilistic arguments (often by showing almost all are good), but constructing a “good” configuration often turns out to be a harder problem. (By an explicit construction, we mean a scheme to specify, for each n , or for infinitely many n , a “good” configuration.) There are many reasons why explicit constructions are preferable. While random graphs are easy to obtain and easy to analyze probabilistically, efficient testing algorithms are required (and typically, are not available) to ensure the graph is indeed good. In addition, it takes more memory, namely, n^2 entries, to write a random graph, whereas a systematic approach often has a much shorter description, e.g., such as the k -regular expander graphs we will discuss here which require only k numbers to specify the graphs. For finding paths among vertices in many sorting or routing problems, explicit constructions are particularly crucial.

It has long been a major thrust of so-called constructive methods (in contrast to the probabilistic approach) to study various methods that yield good constructions. In the past several years major progress has been made on constructing expander graphs (although many other problems remain unresolved, as we mention in §5). Margulis [29] constructed linear-sized expander graphs with certain undetermined factors of expansion. Gabber and Galil [21] gave a family of linear expander graphs with an effective estimate on the expansion coefficients. Other constructions appeared in Schmidt [36], Alon and Milman [2], Jimbo and Maruoka [24], and Buck [12]. The Jimbo-Maruoka method uses elementary but rather complicated linear algebraic tools. The analysis of the other constructions used techniques from harmonic analysis. One important step in analyzing expander graphs is to establish the relation between the expanding properties of a k -regular graph and μ^2 , the second largest eigenvalue of $M^T M$. Tanner first proved [38] that for any set X of vertices of G , the number of neighbors $N(X)$ satisfies

$$N(X) \geq \frac{k^2|X|}{(k^2 - \mu^2)|X|/n + \mu^2}.$$

Hence μ provides very good control of the expanding property (also see [2]). The smaller μ is the more “expanding” the graph is. How small can μ be as a function of k ? Alon and Boppana (see [28]) proved that the \liminf of μ is at least $2\sqrt{k-1}$ (as n approaches infinity). On the other hand, Lubotsky, Phillips, and Sarnak [28] recently applied some results of Eichler [16] on the Ramanujan conjectures [36] and constructed expander graphs, which they called Ramanujan graphs, with $\mu \leq 2\sqrt{k-1}$.

In this paper we will construct a new family of expander graphs. Recall that a k -sum graph on n vertices can be specified by some set of k integers between 1 and n . A pair $\{i, j\}$ is an edge if and only if $i + j \pmod{n}$ is one of the k integers. We can also define the difference graphs where $i \rightarrow j$ is an edge if $i - j$

is one of the specified integers. We will show that the appropriate choices for the set S of the k integers will ensure that λ and μ are small. Thereby, the corresponding sum or difference graphs determined by S are expanders with small diameter.

We will now describe the following selection of the k -set S .

Let p denote a prime number. Let us form the finite field $GF(p^t)$ by adjoining to Z_p a root w of an irreducible t th degree polynomial $F(x)$ in $Z_p[x]$. Now take an element g in $GF(p^t)$ that generates $GF^*(p^t)$ and consider the p elements $w, w+1, \dots, w+p-1$. Clearly, $w+i$ can be expressed as g^{d_i} for some d_i , and these d_i , $0 \leq i \leq p-1$, will form the set S . In other words, the d_i 's can be viewed as the discrete logarithms with base g of the $w+i$'s.

Suppose there are two distinct sets of t numbers in S , say $d_{i_1}, d_{i_2}, \dots, d_{i_t}$ and d_{j_1}, \dots, d_{j_t} , with equal sums. In other words,

$$d_{i_1} + d_{i_2} + \dots + d_{i_t} = d_{j_1} + d_{j_2} + \dots + d_{j_t} = x.$$

By considering g^x , we get

$$(w + i_1)(w + i_2) \cdots (w + i_t) = (w + j_1)(w + j_2) \cdots (w + j_t).$$

We now have a nonzero polynomial of degree $< t$ that is satisfied by w . This contradicts the fact that w satisfies an irreducible polynomial of degree t . This shows that all t -sums of S are distinct modulo $p^t - 1$. This fact was first observed by Bose and Chowla [10] and they proved the following theorem.

For a prime number p and a fixed integer t , there exists a set S of p integers d_1, \dots, d_p with $1 \leq d_i \leq p^t$ such that all t -sums (i.e., sums of t numbers in S , allowing repetition) are distinct.

We now consider a sum graph G on $n = p^t - 1$ vertices determined by the p -set $S = \{d_1, \dots, d_p\}$. We note that although the choices of the values of d_i 's depend on the choice of the primitive element g , it can be easily seen that the resulting graph is, in fact, independent of g since the sum graph G can be viewed as having vertex set $GF(p^t)^*$, with an edge from u to v if $uv = w + i$ for some $i \in \{0, 1, \dots, p-1\}$.

We will show in the next section that the second largest eigenvalue of G is small and thus G has good expanding properties. We can also generalize the construction of the difference graphs in the following way. For a group H together with a subset H' that is stable under conjugation, we define a graph with vertex set H and two elements u and v forming an edge if uv^{-1} is in H' . Let M denote the adjacency matrix whose eigenvalues and eigenvectors can then be determined (see [15]). Namely, M has eigenvalues λ_ρ for each irreducible representation ρ of G given by

$$\lambda_\rho = \frac{1}{d_\rho} \sum_{h \in H'} \Psi_\rho(h)$$

where $\Psi_\rho(h) = \text{Tr } \rho(h)$ and the λ_ρ occurs with multiplicity d_ρ^2 where d_ρ is the dimension of ρ . The sum graph with edges (i, j) for $ij \in H'$ has eigenvalues λ_ρ if λ_ρ is real or $\pm|\lambda_\rho|$ if λ_ρ is not real.

4. THE EIGENVALUES OF THE k -SUM AND k -DIFFERENCE GRAPHS

The eigenvalues of k -sum and k -difference graphs can be determined as follows. Let θ denote an n th root of unity in the complex field \mathbb{C} . The following can be easily verified by straightforward matrix manipulation.

Lemma 1. *The difference graph on n vertices determined by a set $S = \{a_1, a_2, \dots, a_k\}$ has eigenvalues $\sum_{i=1}^k \theta^{a_i}$ where θ ranges over all n th roots of 1.*

Proof. The eigenvectors are $(1, \theta, \theta^2, \dots, \theta^{n-1})$.

We remark that the eigenvectors of the difference graph form an orthogonal basis so that Theorem 3 can be applied.

Lemma 2. *The sum graph on n vertices determined by a set $S = \{a_1, a_2, \dots, a_k\}$ has eigenvalue: $k \pm |\sum_{i=1}^k \theta^{a_i}|$ where θ ranges over all n th roots of 1 with $\theta \neq \pm 1$ and $\sum_{i=1}^k (-1)^{a_i}$ if n is even.*

Proof. The eigenvectors are $(1, \theta, \theta^2, \dots, \theta^{n-1}) \pm (\sum_{i=1}^k \theta^{a_i}) / |\sum_{i=1}^k \theta^{a_i}| \cdot (1, \theta^{-1}, \dots, \theta^{-(n-1)})$ if $\theta \neq \pm 1$.

It remains to be shown that $|\sum_{i=1}^n \theta^{d_i}|$ is small for $\theta \neq 1$ where the d_i 's are as specified in the preceding section.

Theorem 4. $|\sum_{i=1}^p \theta^{d_i}| \leq (t - 1)\sqrt{p}$.

Theorem 4 is an immediate consequence of the following theorem of N. M. Katz [25].

Theorem 5. *Let Ψ denote a nontrivial complex-valued multiplicative character defined on an extension field E over a finite field K with dimension t . Then for any $x \in E$ such that $E = K(x)$ we have*

$$\left| \sum_{a \in K} \Psi(x + a) \right| \leq (t - 1)\sqrt{|K|}.$$

A more general form of Theorem 5 on character sums for a finite étale algebra is proved in [25]. In the sum graphs we have $\lambda \leq (t - 1)\sqrt{p}$. Therefore by Theorem 1 we get the following.

Theorem 6. *Sum graphs on $n = p^t - 1$ vertices have degree p and diameter at most $2t + 4t \log t / (\log p - 2 \log(t - 1))$ if $\sqrt{p} > t - 1$.*

As an immediate consequence of Theorem 6, the sum graph is connected if $\sqrt{p} > t - 1$. This implies that the multiplicative group $GF(p^t)^*$ is generated by $\{w, w + 1; \dots, w + p - 1\}$ for a root w of an irreducible t th degree polynomial $F(x)$ in $\mathbb{Z}_p[x]$.

Another consequence of Theorem 6 is the following result.

Theorem 7. For a prime p , an element in $GF(p^t) \simeq GF(p)[x]/(F(x))$ can be written as

$$\frac{(x + a_1) \cdots (x + a_{\lceil m/2 \rceil})}{(x + b_1) \cdots (x + b_{\lfloor m/2 \rfloor})}$$

where a_i and b_i are in $GF(p)$ and

$$m \leq 2t + 4t \log t / (\log p - 2 \log(t - 1))$$

provided $\sqrt{p} > t - 1$.

We remark that the estimates for the diameter of the sum graph in Theorems 6 and 7 are quite close to best possible if $p \neq 2$. In fact, the sum graph has diameter at least $2t - 1$, if $p \neq 2$. Suppose we choose a in $GF(p) - \{1\} \neq \emptyset$, for $p \neq 2$, and try to go from 1 to a in the sum graph. If there is a path joining 1 and a of length $2r$, then

$$a = \prod_{i=1}^r (x + \alpha_i) / \prod_{i=1}^r (x + \beta_i)$$

where α_i and β_i are in $GF(p)$.

If there is a path joining 1 to a of length $2r - 1$, we then have

$$a = \prod_{i=1}^r (x + \alpha_i) / \prod_{i=1}^{r-1} (x + \beta_i)$$

for α_i and β_i in $GF(p)$. Now if $r < t$, cross-multiplying gives an identity in $GF[x]$ of degree r that is impossible. So the upper bound $2t + 1$ for p sufficiently large is quite sharp.

Similarly, by considering the diameter of the difference graphs, we have the following.

Theorem 8. For a prime number p , any element

$$\alpha \in GF(p^t) \simeq GF(p)[x]/(F(x))$$

can be written as $\alpha = (x + a_1) \cdots (x + a_m)$ for some $a_i \in GF(p)$ if $m \geq 2t + 4t \log t / (\log p - 2 \log(t - 1))$ and $\sqrt{p} > t - 1$.

An interesting problem is to find the exact number r such that any element can be written as a product of no more than r linear terms. It is easy to see that at least $t + t \log t / \log p$ terms are required since the total number of elements that can be written as a product of m linear terms is at most $\binom{p+m-1}{m} \geq p^t - 1$. From Theorem 6 we know that such t is between $2t + 4t \log t / (\log p - 2 \log(t - 1))$ and $t + t \log t / \log p$. A recent result of Katz [26] gives an upper bound of $t + 2$ provided p is large enough. Therefore the difference graph has diameter of at most $t + 2$.

5. CONCLUDING REMARKS

One immediate application of difference graphs is the problem of multi-loop networks. Multi-loop networks, which arise in connection with the design of

local computer networks, can be described by a directed graph as follows. The vertices of the graphs are $0, 1, \dots, n-1 \pmod{n}$ and directed edges from i to $i + a_j$ for some fixed set of a_j 's. The problem of interest is to minimize the diameter of such graphs. For the case of $|S| = 2$, so-called double loop networks, several papers [13, 34] obtained close bounds for the diameter, and recently Cheng [13] obtained the complete solution. By using difference graphs, we can construct multi-loop networks of size $n = p^t - 1$ by taking S to be d_i 's as mentioned in §3. Such graphs will have diameter of at most $t + 2$ and at least $t + t \log t / \log p$ if p is sufficiently large.

One of the outstanding open problems in extremal graph theory is to find a graph on n vertices with maximum number $f(n, 2t)$ of edges that does not contain a cycle on $2t$ vertices. It is known [9, 18] that $cn^{1-1/(2t-1)} < f(n, 2t) < c'n^{1+1/t}$. For small values of t , $t = 2, 3, 5$, finite geometries were used to construct extremal graphs with $cn^{1+1/t}$ edges [8, 11, 17, 37]. The sum graphs as described in §3 have $cn^{1+1/t}$ edges with the property that for almost all pairs of vertices there are at most a bounded number of paths of length t . This provides some evidence in support of the conjecture of P. Erdős (see [17]) that $f(n, 2t)$ behaves as $cn^{1+1/t}$ for n sufficiently large.

Although substantial progress has been made for constructions of relatively sparse random-like graphs, the constructions for dense graphs remain very poor. The following problem in Ramsey theory is still unresolved.

Construct a graph on n vertices with the property that the largest complete subgraphs have at most $c \log n$ vertices and the largest independent sets have at most $c \log n$ vertices.

The best construction [19] known so far guarantees only complete subgraphs and independence sets of size smaller than $e^{c\sqrt{\log n}}$. This remains one of the major open problems in combinatorics.

Another interesting problem is to find the actual "realization" of the linear products. Namely, for a prime p and integer m , we would like to find an efficient method which can generate, for a given element α in $GF(p^t)$, a representation of α as the linear product of no more than m terms.

ACKNOWLEDGMENT

The author wishes to thank Barry Mazur and Andrew Odlyzko for very helpful discussions. Many thanks are due to H. Wilf for simplifying the proofs of Theorems 1 and 2.

REFERENCES

1. M. Ajtai, J. Komlós, and E. Szemerédi, *Sorting in $c \log n$ parallel steps*, *Combinatorica* **3** (1983), 1–19.
2. N. Alon and V. D. Milman, λ_1 , *isoperimetric inequalities for graphs and superconcentrators*, *J. Combin. Theory Ser. B* **38** (1985), 73–88.
3. N. Alon, *Eigenvalues and expanders*, *Combinatorica* **6** (1983), 83–96.

4. N. Alon, Z. Galil, and V. D. Milman, *Better expanders and superconcentrators*, J. Algorithms **8** (1987), 337–347.
5. W. N. Anderson, Jr. and T. D. Morley, *Eigenvalues of the Laplacian of a graph*, Univ. Maryland Technical Report TR-71-45, 1971.
6. L. A. Bassalygo, *Asymptotically optimal switching circuits*, Problems Inform. Transmission **17** (1981), 206–211.
7. J. Beck, *On size Ramsey number of paths, trees and circuits*. I, J. Graph Theory **7** (1983), 115–129.
8. C. T. Benson, *Minimal regular graphs of girths eight and twelve*, Canad. J. Math. **8** (1966), 1091–1094.
9. J. A. Bondy and M. Simonovits, *Cycles of even length in graphs*, J. Combin. Theory Ser. B **16** (1974), 97–105.
10. R. C. Bose and S. Chowla, *Theorems in the additive theory of numbers*, Comment. Math. Helv. **37** (1962), 141–147.
11. W. G. Brown, *On graphs that do not contain a Thomsen graph*, Canad. Math. Bull. **9** (1966), 281–285.
12. M. W. Buck, *Expanders and diffusers*, SIAM J. Algebraic Discrete Methods **7** (1986), 282–304.
13. Ying Cheng, *Diameters of double loop local computer networks*, 1988, preprint.
14. F. R. K. Chung, *On concentrators, superconcentrators, generalizers and nonblocking networks*, Bell Systems Tech. J. **58** (1978), 1765–1777.
15. P. Diaconis, *Group representation in probability and statistics*, 1988, preprint.
16. M. Eichler, *Quaternary quadratic forms and the Riemann hypothesis for congruence zeta functions*, Arch. Math. **5** (1954), 355–366.
17. P. Erdős, A. Rényi, and V. T. Sós, *On a problem of graph theory*, Studia Sci. Math. Hungar. **1** (1966), 215–235.
18. R. J. Faudree and M. Simonovits, *On a class of degenerate extremal graph problem*, Combinatorica **3** (1983), 97–107.
19. P. Frankl and R. M. Wilson, *Intersection theorems with geometric consequences*, Combinatorica **1** (1981), 357–368.
20. J. Friedman and N. Pippenger, *Expanding graphs contain all small trees*, Combinatorica **7** (1987), 71–76.
21. O. Gabber and Z. Galil, *Explicit construction of linear sized superconcentrators*, J. Comput. System Sci. **22** (1981), 407–420.
22. Y. Ihara, *Discrete subgroups of $PL(2, k_p)$* , Proc. Sympos. Pure Math., Vol. 9, Amer. Math. Soc., Providence, R. I., 1968, pp. 272–278.
23. J. JáJa, *Time space tradeoffs for some algebraic problems*, Proc. 12th Annual ACM Sympos. on Theory of Computing, 1980, AMC, NY, 1980, pp. 339–350.
24. S. Jimbo and A. Maruoka, *Expanders obtained from affine transformations* (extended abstract), 1984, preprint.
25. N. M. Katz, *An estimate for character sums*, J. Amer. Math. Soc. **2** (1989), 197–200.
26. —, *Factoring polynomials in finite fields: an application of Lang-Weil to a problem in graph theory*, 1988, preprint.
27. 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.
28. A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), 261–278.
29. G. A. Margulis, *Explicit constructions of concentrators*, Problemy Peredači Informacii **9** (1973), 71–80 (English transl. in Problems Inform. Transmission **9** (1975), 325–332).
30. M. Pinsker, *On the complexity of a concentrator*, 7th Internat. Teletraffic Conf., Stockholm, June 1973, 318/1-318/4.

31. N. Pippenger, *Superconcentrators*, SIAM J. Comput. **6** (1977), 298–304.
32. —, *Advances in pebbling*, Internat. Colloq. on Automation Languages and Programming, Vol. 9, 1982, pp. 407–417.
33. W. J. Paul, R. E. Tarjan, and J. R. Celoni, *Space bounds for a game on graphs*, Math. Soc. Theory **10** (1977), 239–251.
34. C. S. Raghavendra and J. A. Silvester, *A survey of multi-connected loop topologies for local computer networks*, Computer Networks and ISDN Systems **2** (1986), 29–42.
35. S. Ramanujan, *On certain arithmetical functions*, Trans. Cambridge Philos. Soc. **22** (9) (1916), 159–184.
36. W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Math., Vol. 536, Springer-Verlag, Berlin and New York, 1976.
37. R. R. Singleton, *On minimal graphs of maximum even girth*, J. Combin. Theory **1** (1966), 306–332.
38. R. M. Tanner, *Explicit construction of concentrators from generalized N -gons*, SIAM J. Algebraic Discrete Methods **5** (1984), 287–294.
39. M. Tompa, *Time space tradeoffs for computing using connectivity properties of the circuits*, J. Comput. System Sci. **20** (1980), 118–132.
40. L. G. Valiant, *Graph theoretic properties in computational complexity*, J. Comput. System Sci. **13** (1976), 278–285.

ABSTRACT. We derive a new upper bound for the diameter of a k -regular graph G as a function of the eigenvalues of the adjacency matrix. Namely, suppose the adjacency matrix of G has eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_n$ with $|\lambda_1| \geq |\lambda_2| \geq \dots \geq |\lambda_n|$ where $\lambda_1 = k$, $\lambda = |\lambda_2|$. Then the diameter $D(G)$ must satisfy

$$D(G) \leq \lceil \log(n-1) / \log(k/\lambda) \rceil.$$

We will consider families of graphs whose eigenvalues can be explicitly determined. These graphs are determined by sums or differences of vertex labels. Namely, the pair $\{i, j\}$ being an edge depends only on the value $i+j$ (or $i-j$ for directed graphs). We will show that these graphs are expander graphs with small diameters by using an inequality on character sums, which was recently proved by N. M. Katz.

BELL COMMUNICATIONS RESEARCH, 445 SOUTH STREET, MORRISTOWN, NEW JERSEY 07960