COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA **15** (1) (1995) 111–122

NATURAL BOUNDED CONCENTRATORS

MOSHE MORGENSTERN†

Received January 9, 1992
Revised May 20, 1994

We give the first known direct construction for linear families of bounded concentrators. The construction is explicit and the results are simple natural bounded concentrators.

Let $\mathbb{F}_q$ be the field with q elements, $g(x) \in \mathbb{F}_q[x]$ of degree greater than or equal to 2, $H = PGL_2(\mathbb{F}_q[x]/g(x)\mathbb{F}_q[x])$, $B = PGL_2(\mathbb{F}_q)$, and $A = \left\{ \begin{pmatrix} a & b+cx \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{F}_q^*; b, c \in \mathbb{F}_q \right\}$. Let $I_{\text{nputs}} = H/A$, $O_{\text{utputs}} = H/B$, and draw an edge between aA and bB iff $aA \cap bB \neq \phi$. We prove that for every $q \geq 5$ this graph is an $\left(|H/A|, \frac{q}{q+1}, q+1, \frac{q-4}{q-3}\right)$-bounded concentrator.

1. Introduction

An (n,d)-*superconcentrator* ((n,d)-*s.c.* for short) is a directed acyclic graph with n inputs, n outputs and not more than dn edges, such that for any $r \leq n$, given any two sets, S of r inputs and T of r outputs, there are r vertex disjoint paths from S to T. Superconcentrators are very useful in theoretical computer science for designing communication networks, proving lower bounds, sorting, etc. (see [1], [9]) and the references therein). One of the major difficulties in this theory is to give an economic construction for linear families of superconcentrators i.e., families of (n,d)-s.c. with $n \to \infty$ linearly, keeping the density d fixed and as small as possible. Such families were constructed from bounded concentrators [13, 6]. An (n,θ,k,α)-*bounded concentrator* is a bipartite graph with n inputs, θn outputs for $\theta < 1$, and not more than kn edges, but nevertheless any set S of not more than αn inputs ($\alpha \leq \theta$) has at least $|S|$ neighbors. By the P. Hall marriage lemma, there is a perfect matching between S and some subset of its neighbors. Bounded concentrators are important for switching networks, sorting and especially for constructing superconcentrators as follows [6]: To construct a superconcentrator of size n, put a direct edge between each of the n inputs and its twin in the outputs. Use these edges to connect as many vertices as possible of the two given sets $S \subseteq I$ and $T \subseteq O$. After it we may assume that $|S| = |T| \leq n/2$, this can be feed into two $(n,\theta,k,1/2)$-bounded concentrators, to reduce the problem to size θn.

Mathematics Subject Classification (1991): Primary: 05 C 35, Secondary: 05 C 25

† Part of this research was done while the author was at the department of Computer Science, The University of British Columbia, Vancouver, B.C., Canada.

Theorem A. [6] *If for every n an $(n,\theta,k,1/2)$ bounded concentrator is given, then for every n it is possible to construct an $\left(n,\frac{2k+1}{1-\theta}\right)$ superconcentrator.*

A bipartite k regular graph with n inputs and n outputs is an (n,k,c)-*expander*, if any set of s inputs has at least $[1+c(1-s/n)]s$ outputs as neighbors. Bounded concentrators were obtained from expanders as follows [6]: To construct a bounded concentrator with n inputs, let $p+1$ divide n and $r=n/(p+1)$. Let $G=(V=I\cup O,E)$ be a bipartite $(pr,k,2/(p-1))$ expander, divide O into r disjoint equal pieces $O_1,\ldots,O_r$ (each consist of p vertices), add r new vertices $i_1,\ldots,i_r$ to I, and for $1\leq j\leq r$ connect i_j to each vertex of O_j. The resulting graph is then an $\left(n,\frac{p}{p+1},\frac{(k+1)p}{p+1},\frac{1}{2}\right)$ bounded concentrator.

Theorem B. [6] *If for every n an $\left(n,k,\frac{2}{p-1}\right)$-expander is given, then for every n it is possible to construct an $(n,(2k+3)p+1)$-superconcentrator.*

This way using Margulis expanders, Gaber and Galil constructed linear families of superconcentrators with density $d=272$. This was improved in [1] to $d=123$, then Lubotzky et al. [11] using their Ramanujan graphs got $d=78$. But N. Pippenger draws to their attention that it is possible to have $d=64$, using expanders that are double covers of 8-regular Ramanujan graphs. Explicit constructions of such Ramanujan graphs can be found in [15].

Although for many reasons it is important to have these graphs homogeneous, i.e. distributing the inputs uniformly over the outputs, this is not the case in the above construction of bounded concentrators. The artificial way in which the new inputs are connected to the outputs, breaks the "close to random" structure of the expander. Here we give explicitly a direct construction of many infinite linear families of homogenous bounded concentrators, i.e. families in which $n\to\infty$ linearly, keeping k, θ and α fixed.

Our main result is: Let $\mathbb{F}_q$ be the field with q elements, $g(x)\in\mathbb{F}_q[x]$, $R=\mathbb{F}_q[x]/g(x)\mathbb{F}_q[x]$, $H=PGL_2(R)$, $H_0=PGL_2(\mathbb{F}_q)$,

$$H_1=\left\{\begin{pmatrix}a & b+cx\\ 0 & 1\end{pmatrix}\in G\,\middle|\, a\in\mathbb{F}_q{}^*, b,c\in\mathbb{F}_q\right\}.$$

H_0, $H_1\subseteq H$ and everything is finite. Let $I_{\text{nputs}}=H/H_1, O_{\text{utputs}}=H/H_0$, and an edge exist between aH_1 and bH_0 iff $aH_1\cap bH_0\neq\phi$. For every $q\geq 5$ and $g(x)$ of degree greater than or equal to 2, this graph is an $\left(|H/H_1|,\frac{q}{q+1},q,\frac{q-4}{q-3}\right)$ bounded concentrator. Superconcentrators made from these b.c. for $q=5$, come out to be of density 66.

In Section 2 we present the background about the discrete valuations of $\mathbb{F}_q(x)$, the local tree of PGL_2 and its quotients. Then we give an abstract presentation of the diagram that we work with, and prove that it is a Ramanujan diagram. In Section 3 we discover the explicit structure of this diagram. Then in Section 4 we prove that a subgraph of this diagram is a bounded concentrator, and discuss related issues.

2. The Ramanujan diagram D_g

We will recall a few fundamental definitions about diagrams (for more see [14]). A *diagram* is a triple $D=(V,E,w)$ where (V,E) is a bipartite graph, $w: V\cup E\to \{1/n \mid n=1,2,3,\ldots\}$ is the *weight function*, which satisfies:

1. $\sum_{v\in V} w(v)<\infty$.
2. For any $e=(u,v)\in E, w(e)^{-1}$ divides $w(u)^{-1}$ and $w(v)^{-1}$.

For an edge $e=(u,v)$ define $\theta(u,v)=w(e)/w(u)$ to be the *entering degree* of e to u, and call D *r-regular* if for every fixed $u\in V$, $\sum_{(u,v)\in E}\theta(u,v)=r$.

Let f,g be functions on V and set

$$\langle f,g\rangle = \sum_{v\in V} f(v)\overline{g(v)}w(v)$$

which defines $L_2(D)$. The *Laplacian* Δ on $L_2(D)$ which is defined by $\Delta f(u)=\sum_{(u,v)\in E}\theta(u,v)f(v)$ is hermitian, and well defined on

$$L_2^0(D)=\left\{ f\in L_2(D) \;\middle|\; \sum_{v\in I} f(v)w(v)=\sum_{v\in O} f(v)w(v)=0 \right\}.$$

Denote $\left\|\Delta|_{L_2^0(D)}\right\|$ by λ.

Let q be a prime power, and $\mathbb{F}_q$ the field with q elements, $\mathbb{F}_q[x]$ the polynomials over $\mathbb{F}_q$ and $k=\mathbb{F}_q(x)$ its quotient field. For every irreducible $f\in\mathbb{F}_q[x]$, the *discrete valuation* v_f on k is defined by $v_f(g/h)=\mathrm{ord}_f(g)-\mathrm{ord}_f(h)$, where $\mathrm{ord}_f(g)$ is the maximal power n such that f^n divides g. The valuation at $1/x$ (also called the valuation at infinity) is defined by $v_{1/x}(g/h)=\mathrm{degree}(h)-\mathrm{degree}(g)$. These are all discrete valuations of k, they are called the *places* of k. For a place p let k_p be the completion of k with respect to the metric $|a|=q^{-v_p(a)}$, and O_p its integers. $k_p=\mathbb{F}_q((p))$ is the field of Laurent series in p over $\mathbb{F}_q$, and $O_p=\mathbb{F}_q[[p]]$ is the ring of Taylor series in p over $\mathbb{F}_q$.

For a ring R let $PGL_2(R)$ be the group of 2×2 invertible matrices over R divided by its center. Let $PSL_2(R)=\{A\in PGL_2(R)\mid |A| \text{ is a square in } R\}$. Let us write G_R for $PGL_2(R)$ and G_R^1 for $PSL_2(R)$. In the special case when $R=k_p$ we'll also write G_p for G_{k_p} and G_p^1 for $G_{k_p}^1$.

Let H be G or G^1. The *Adele group* of H over k is defined by:

$$H_{\mathbb{A}}=\left\{ (\cdots,g_p,\cdots)\in\prod_p H_p \;\middle|\; g_p\in H_{O_p} \text{almost everywhere} \right\}$$

where by "almost everywhere" we mean: except for a finite number of places. Multiplication is componentwise, and a topology on $H_{\mathbb{A}}$ is defined by declaring the subring $\prod_p H_{O_p}$ with the usual Tychonoff product topology to be open. With this, $H_{\mathbb{A}}$ is a locally compact group. H_k is embedded naturally into $H_{\mathbb{A}}$ by $g\to(g,g,\cdots,g,\cdots)$ (see [7] for more details).

In [18, §II 1] the structure of the $q+1$ regular tree is defined on $G_{1/x}/G_{O_{1/x}}$. The tree $T = G_{1/x}/G_{O_{1/x}}$ is completely described by defining the neighbors of $gG_{O_{1/x}}$ to be the $q+1$ cosets $gs_iG_{O_{1/x}}$ $i=1,\ldots,q+1$, where

$$\{s_1,\ldots,s_{q+1}\} = \left\{\begin{pmatrix} 1/x & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbb{F}_q\right\} \bigcup \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1/x \end{pmatrix}\right\}. \tag{1}$$

From this point of view it is clear that $G_{1/x}$ acts on T (from the left) as a group of automorphisms.

$\Gamma = \Gamma(1) = PGL_2(\mathbb{F}_q[x])$ is a lattice in $G_{1/x}$ [18, §2.1.6] (i.e., Γ is discrete and $\Gamma\backslash G_{1/x}$ is of finite $G_{1/x}$-invariant measure). Hence, for every $g \in \mathbb{F}_q[x]$,

$$\Gamma(g) = \{A \in \Gamma(1) \mid \text{for some representative } a \text{ of } A, a \equiv I \bmod g\}$$

which is of finite index in $\Gamma(1)$, is also a lattice in $G_{1/x}$. Look at the action of $\Gamma(g)$ (from the left) on the tree $T = G_{1/x}/G_{O_{1/x}}$, and denote the quotient graph $\Gamma(g)\backslash G_{1/x}/G_{O_{1/x}}$ by X_g. If $\tilde{v}$ and $\tilde{v}'$ are two vertices of T which lie above $v \in X_g$, then the stabilizers of $\tilde{v}$ and $\tilde{v}'$ are conjugate subgroups of $\Gamma(g)$, so we may define the weights:

$$w(v) = |\{\gamma \in \Gamma(g) \mid \gamma\tilde{v} = \tilde{v}\}|^{-1} \quad w(e) = |\{\gamma \in \Gamma(g) \mid \gamma\tilde{e} = \tilde{e}\}|^{-1} \tag{2}$$

where $\tilde{v}$ and $\tilde{e}$ are any vertex and edge which lie above v and e respectively. As the quotient of the $q+1$ regular tree T, $D_g = (X_g, w)$ is a $q+1$ regular diagram (as we will later see in detail).

Theorem 2.1. *D_g is a Ramanujan diagram, i.e., $\left\|\Delta|_{L_2^0(D_g)}\right\| \leq 2\sqrt{q}$.*

Proof. We are not going to give all details, parts of this proof can be found with more details in [12, ch. 5], a detailed proof appears in [16]. The continuous spectrum of the Laplacian Δ on $L_2^0(D_g)$ is well known from the theory of Eisenstein series ([5, §8] for example). It is exactly the segment $[-2q^{1/2}, 2q^{1/2}]$ (see also a direct computation for the case of $\Gamma(1)$ in [4]).

It is left to show that if $\lambda \neq \pm(q+1)$ is an eigenvalue of Δ, then $|\lambda| \leq 2\sqrt{q}$. Let ρ be a continuous irreducible unitary representation of $G_{1/x}$ in $(H, <,>)$. Assume ρ is of class one, i.e. there is a $v \in H$ s.t $\|v\| = 1$, and $G_{O_{1/x}} \cdot v = v$. $f_\rho(g) = <gv, v>$ is called the spherical function of ρ ($f_\rho : G_{1/x} \to \mathbb{C}$). Since at most one such v can exist [10, ch. IV], f_ρ is well defined.

Let $U = G_{O_{1/x}} \begin{pmatrix} 1 & 0 \\ 0 & 1/x \end{pmatrix} G_{O_{1/x}}$, 1_U its characteristic function, and define the convolution $(f * h)(x) = \int_{G_{1/x}} f(xy^{-1})h(y)dy$. There is a unique $\mu \in \mathbb{C}$ such that $f_\rho * 1_U = \mu f_\rho$, and ρ is denoted by ρ^μ. For more details see [10, ch. IV].

Lemma 1. *μ is an eigenvalue of the Laplacian Δ of $\Gamma(g)\backslash G_{1/x}/G_{O_{1/x}}$ iff the representation ρ^μ appears in the (right) regular representation $R_{G_{1/x}}$ of $G_{1/x}$ in $L_2(\Gamma(g)\backslash G_{1/x})$. Moreover, if $\mu \neq \pm(q+1)$ then ρ^μ is not one dimensional.*

Proof. The proof is almost the same as in [12, ch. V] ∎

Let $g(x)=\prod_{i=1}^{s} g_i(x)^{d_i}$, where $g_i \in \mathbb{F}_q[x]$ are irreducible, and $g_i \neq g_j$ for $i \neq j$. Let

$$K_r = \begin{cases} \mathrm{Ker}\{G_{O_r} \xrightarrow{\alpha_i} PGL_2(O_r/r^{d_i}O_r)\} & r = g_i \quad 1 \leq i \leq s \\ K_r = G_{O_r} & r \neq g_i \end{cases}$$

where:

$$\alpha_i \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a \bmod g_i^{d_i} & b \bmod g_i^{d_i} \\ c \bmod g_i^{d_i} & d \bmod g_i^{d_i} \end{pmatrix}.$$

Let $K=\prod_{f \neq 1/x} K_f$ and $H=G_k G_{1/x} K$.

Lemma 2. $|G_k \backslash G_{\mathbb{A}} / K : G_k \backslash H / K| < \infty$.

Proof. Let $K^1=\prod_{f \neq 1/x} G^1_{O_f}$, clearly $G^1_{1/x}K^1$ is a nonempty open subset of $G^1_{\mathbb{A}}$. $G_{1/x}$ is not compact, so by the Strong Approximation Theorem ([17]) $G^1_k G^1_{1/x}$ is dense in $G^1_{\mathbb{A}}$, so

$$G^1_{\mathbb{A}} = G^1_k G^1_{1/x} K^1. \tag{3}$$

Since $|\prod_{f \neq 1/x} G_{O_f} : K| < \infty$, and by the Strong Approximation Theorem [17] $k^*_{\mathbb{A}} = k^* k^*_{1/x} \prod_f O^*_f$, it is clear that H contains a finite index subgroup of $G^1_{\mathbb{A}} k^*_{\mathbb{A}} = G_{\mathbb{A}}$, (since $G_r = PSL_2(k_r)k^*_r$ for any place r). Hence $|G_{\mathbb{A}} : H| < \infty$, and also $|G_k \backslash G_{\mathbb{A}} / K : G_k \backslash H / K| < \infty$. ∎

Since $G_k \cap K = \Gamma(g)$

$$G_k \backslash H / K \cong \Gamma(g) \backslash G_{1/x}$$

as $G_{1/x}$ modules (by multiplication from the right), and

$$|G_k \backslash G_{\mathbb{A}} / K : \Gamma(g) \backslash G_{1/x}| < \infty.$$

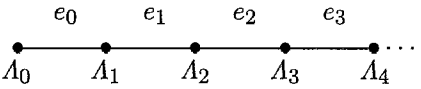
Therefore, for every irreducible representation $\tau_{1/x}$ of the (right) regular representation of $G_{1/x}$ in $L_2(\Gamma(g)\backslash G_{1/x})$, there is an irreducible sub-representation $\delta = \otimes_f \delta_f$ of the regular representation of $G_{\mathbb{A}}$ in $L_2(G_k \backslash G_{\mathbb{A}})$, such that $\delta_{1/x} = \tau_{1/x}$.

Assume now that $\mu \neq \pm(q+1)$ is an eigenvalue of the Laplacian on the diagram $\Gamma(g)\backslash G_{1/x}/G_{O_{1/x}}$. By lemma 1, ρ^μ (which is not one dimensional) appears in the regular representation of $G_{1/x}$ in $L_2(\Gamma(g)\backslash G_{1/x})$, and hence $\delta = \otimes_f \delta_f$ with $\delta_{1/x} = \rho^\mu$ appears in the regular representation of $G_{\mathbb{A}}$ in $L_2(G_k \backslash G_{\mathbb{A}})$. By the theorem of Drinfeld [3], ρ^μ is a principle series representation, i.e. $|\mu| \leq 2\sqrt{q}$. ∎

3. The structure of D_g

Let $\Lambda_m = \begin{pmatrix} x^m & 0 \\ 0 & 1 \end{pmatrix}$, $e_m = \Lambda_m \Lambda_{m+1}$ for $m = 0,1,2,3,\ldots$, and X_1 is the following infinite path in the tree $G_{1/x}/G_{O_{1/x}}$.

X_1:



Let $\Gamma_0 = PGL_2(\mathbb{F}_q)$, $B_0 = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma(1) \middle| a,d \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}$, and for every $m \geq 1$

$$\Gamma_m = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma(1) \middle| a,d \in \mathbb{F}_q^*, \text{degree}(b) \leq m \right\}.$$

Theorem 3.1. [18, §2.1.6] *In the action of $\Gamma(1)$ on the tree $G_{1/x}/G_{O_{1/x}}$:*

(a) *X_1 is a fundamental domain for $\Gamma(1)\backslash G_{1/x}/G_{O_{1/x}}$.*

(b) *For every $m \geq 0$, Γ_m is the stabilizer of Λ_m, and $\Gamma_m \cap \Gamma_{m+1}$ is the stabilizer of the edge e_m. In particular, B_0 is the stabilizer of e_0, and Γ_m of e_m for $m \geq 1$.*

Let $g = g_1^{d_1} g_2^{d_2} \cdots g_s^{d_s}$ the decomposition of $g(x) \in \mathbb{F}_q[x]$ into distinct irreducible prime powers, where $\text{degree}(g_i) = n_i$, $\sum_{i=1}^s d_i n_i = \text{degree}(g) = n \geq 2$. Since $\Gamma/\Gamma(g) \cong \prod_{i=1}^s PGL_2(\mathbb{F}_q[x]/g_i^{d_i}\mathbb{F}_q[x])$ it is easy to see that $|\Gamma/\Gamma(g)| = q^{3n} \prod$, where from now on

$$\prod \stackrel{\text{def}}{=} \prod_{i=1}^{s} (1 - 1/q^{2n_i}).$$

In order to understand the structure of $D_g = (X_g, w)$ it is convenient to look at X_1 as the quotient of X_g by $\Gamma(1)/\Gamma(g)$.

$$T = G_{1/x}/G_{O_{1/x}} \xrightarrow{\pi_1} X_g = \Gamma(g)\backslash G_{1/x}/G_{O_{1/x}} \xrightarrow{\pi_2} X_1 = \Gamma(1)\backslash G_{1/x}/G_{O_{1/x}}$$

where π_1 is the projection through the action of $\Gamma(g)$, π_2 is the projection through the action of $\Gamma(1)/\Gamma(g)$, and $\pi = \pi_2 \circ \pi_1$ is the projection through the action of $\Gamma(1)$.

Since X_1 is a tree, we can identify it with an isomorphic copy in X_g. Let $S \subseteq X_g$ be a maximal subtree of X_g and assume $X_1 \subseteq S$, S can be identified with an isomorphic copy in T. If $e = (u,v) \in X_g$ is not in S, identify it with some $\tilde{e} = (u,\tilde{v}) \in T$ such that $\pi_1(\tilde{v}) = v$. From now on when we will talk for example about Λ_1 in T, e_i in X_g, or $v \in X_g$ as a vertex of T, we mean through this identification.

Definition 3.2 A vertex $v \in X_g$ (edge $e \in X_g$) is called *a vertex (an edge) of level* i, if $\pi_2(v) = \Lambda_i$ ($\pi_2(e) = e_i$), and

$$L_i \stackrel{\text{Def}}{=} \{v \in X_g \mid v \text{ is of level } i\}.$$

Let $*$ stand for one of the three: (i) $\Gamma(1)$ in its action on T. (ii) $\Gamma(g)$ in its action on T. (iii) $\Gamma(1)/\Gamma(g)$ in its action on X_g. Denote

$$Stab_*(v) \stackrel{\text{Def}}{=} \{\gamma \in * \mid \gamma v = v\}.$$

The weights of D_g. By Theorem 3.1 $Stab_{\Gamma(g)}(\Lambda_i)=\Gamma_i\cap\Gamma(g)$. If v is another vertex in L_i, $Stab_{\Gamma(1)}(v)=h^{-1}\Gamma_i h$ for some $h\in\Gamma(1)$, since $\Gamma(1)$ is transitive on L_i. But $\Gamma(g)$ is normal in $\Gamma(1)$ so

$$Stab_{\Gamma(g)}(v) = h^{-1}\Gamma_i h\cap\Gamma(g) = h^{-1}(\Gamma_i\cap\Gamma(g))h = h^{-1}Stab_{\Gamma(g)}(\Lambda_i)h.$$

From the definition in (2) we see that for every $x_i\in L_i$

$$w(x_i)^{-1} = |\Gamma_i\cap\Gamma(g)| = \begin{cases} 1 & i<n \\ q^{i-n+1} & i\geq n. \end{cases} \tag{4}$$

For the same reasons if e_i is an edge of level i

$$w(e_i)^{-1} = \begin{cases} |B_0\cap\Gamma(g)| & i=0 \\ |\Gamma_i\cap\Gamma(g)| & i>n \end{cases} = \begin{cases} 1 & i<n \\ q^{i-n+1} & i\geq n. \end{cases} \tag{5}$$

The vertices of D_g. $\Gamma/\Gamma(g)$ acts transitively on L_i, and the stabilizer of Λ_i is $\Gamma_i\Gamma(g)/\Gamma(g)\cong\Gamma_i/(\Gamma_i\cap\Gamma(g))$, so we can identify L_i with

$$(\Gamma/\Gamma(g))/(\Gamma_i\Gamma(g)/\Gamma(g))\cong\Gamma/\Gamma_i\Gamma(g). \tag{6}$$

Since $|\Gamma/\Gamma(g)|=q^{3n}\prod$, and

$$|\Gamma_i| = \begin{cases} q(q^2-1) & i=0 \\ q^{i+1}(q-1) & i>0 \end{cases}, \qquad |\Gamma_i\cap\Gamma(g)| = \begin{cases} 1 & i<n \\ q^{i+1-n} & i\geq n \end{cases},$$

we get

$$|L_i| = \begin{cases} \frac{q^{3n}\prod}{q(q^2-1)} & i=0 \\ \frac{q^{3n}\prod}{q^{i+1}(q-1)} & n>i>0 \\ \frac{q^{2n}\prod}{q-1} & i\geq n. \end{cases} \tag{7}$$

The edges of D_g. $\Gamma(1)/\Gamma(g)$ acts transitively on the edges of level i, $Stab_{\Gamma(1)/\Gamma(g)}(e_i) = (\Gamma_i\cap\Gamma_{i+1})\Gamma(g)/\Gamma(g)$, and again the edges of level i can be identified with

$$(\Gamma/\Gamma(g))/\{([\Gamma_i\cap\Gamma_{i+1}]\Gamma(g))/\Gamma(g)\}\cong\Gamma/\{(\Gamma_i\cap\Gamma_{i+1})\Gamma(g)\}. \tag{8}$$

From (6) and (8), the edges of level i coming out from a vertex $a\Gamma_i\Gamma(g)\in L_i$ (a vertex $b\Gamma_{i+1}\Gamma(g)\in L_{i+1}$) are exactly the cosets of $(\Gamma_i\cap\Gamma_{i+1})\Gamma(g)$ in $a\Gamma_i\Gamma(g)$ (in $b\Gamma_{i+1}\Gamma(g)$), and their number is the same for every vertex of level i (of level $i+1$).

The edges of level i coming out from $1\Gamma_i\Gamma(g)$ (going to L_{i+1}) are therefore identified with

$$(\Gamma_i\Gamma(g))/\{(\Gamma_i\cap\Gamma_{i+1})\Gamma(g)\}\cong\Gamma_i/\{\Gamma_i\cap([\Gamma_i\cap\Gamma_{i+1}]\Gamma(g))\}, \tag{9}$$

and those coming out from $1\Gamma_{i+1}\Gamma(g)$ (going to L_i) are identified with

$$\Gamma_{i+1}/\{\Gamma_{i+1}\cap([\Gamma_i\cap\Gamma_{i+1}]\Gamma(g))\}. \tag{10}$$

We will now distinguish between the following three cases:

$i=0$:

$\Gamma_0\cap\Gamma_1=B_0$, $\Gamma_0\cap\Gamma(g)=\{1\}$. By (9) there are $|\Gamma_0/B_0|=q+1$ edges coming out from Λ_0 going to level one. Since $\Gamma_1\cap\Gamma(g)=\{1\}$, by (10) there are $|\Gamma_1/B_0|=q$ edges coming out from Λ_1 going to L_0. So, between levels 1 and 0, we have an interesting bipartite graph (all weights are 1) which concentrates the vertices of L_1 into those of L_0, where $|L_0|=\frac{q}{q+1}|L_1|$.

$0<i<n-1$:

$\Gamma_i\cap\Gamma_{i+1}=\Gamma_i$, $\Gamma_i\cap\Gamma(g)=\{1\}$. By (9), from every vertex of level i there is $|\Gamma_i/\Gamma_i|=1$ edge going to L_{i+1}. Since $\Gamma_{i+1}\cap\Gamma(g)=\{1\}$, by (10) from every vertex of level $i+1$ there are $|\Gamma_{i+1}/\Gamma_i|=q$ edges going to L_i. The graph between levels i and $i+1$ is simply a "q to 1" collapsing of L_i on L_{i+1} (note that $|L_{i+1}|=\frac{1}{q}|L_i|$).

$i\geq n-1$:

The number of edges coming out from a vertex of level i, going to L_{i+1}, is again $|\Gamma_i/\Gamma_i|=1$ by (9). But here $\Gamma_i\Gamma(g)=\Gamma_{i+1}\Gamma(g)$ so by (10) the number of edges coming out from a vertex of level $i+1$ going to L_i is also $|\Gamma_{i+1}/\Gamma_{i+1}|=1$. We see that from level $n-1$ on, the diagram D_g continues simply by gluing an infinite ray which is similar to X_1, (but with weights as in (4) and (5)), to every vertex of level $n-1$.

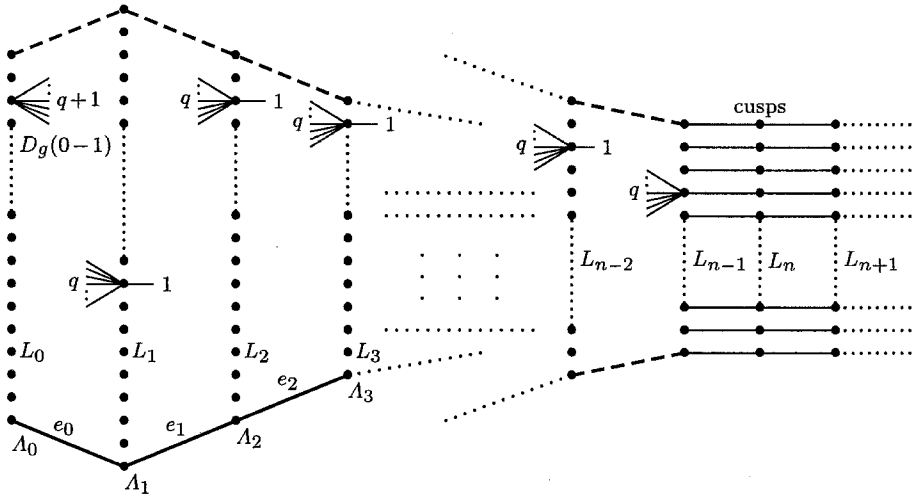


Fig. 1. The diagram D_g

Remark 3.3 Let $R=\mathbb{F}_q[x]/g(x)\mathbb{F}_q[x]$ be represented as polynomials of degree smaller than $n=\text{degree}(g)$, $H=PGL_2(R)$, $H_0=PGL_2(\mathbb{F}_q)$, and for $i>0$

$$H_i=\left\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\in H\,\middle|\, a,d\in\mathbb{F}^*,\text{degree}(b)\leq\min\{i,n-1\}\right\}.$$

Since $\Gamma/\Gamma(g) \cong H$, it is easy to see that our diagram $D_g = (V, E, w)$ is as follows: L_i can be identified with H/H_i, edges exist only between two successive levels, and for $hH_i \in L_i$ and $kH_{i+1} \in L_{i+1}$

$$(hH_i, kH_{i+1}) \in E \Leftrightarrow hH_i \cap kH_{i+1} \neq \phi \Leftrightarrow hH_i \cap kH_{i+1} = \text{a coset of } H_i \cap H_{i+1}.$$

Clearly, the edges of level i which come out from hH_i (going to $|L_{i+1}|$) are exactly the cosets of $H_i \cap H_{i+1}$ in hH_i, and these coming out from kH_{i+1} (going to L_i) are the cosets of $H_i \cap H_{i+1}$ in kH_{i+1}. This describes the structure of D_g (inside the finite group $PGL_2(R)$), in a way which seems to be the easiest to construct effectively.

4. The bounded concentrators

The diagram D_g between levels 0 and 1, is a graph in the usual sense (all the weights are 1), denote it by $D_g(0-1)$.

For any set S of vertices, let 1_S denote the characteristic function of S, $N(S)$ the set of neighbors of S, and $N_i(S)$ the set of neighbors in level i. For a function f on X_g and the Laplacian Δ, let $\Delta_i f$ be the part of Δf supported on L_i (i.e. $\Delta f \cdot 1_{L_i}$). Our main tool is the following lemma:

Lemma 4.1. *For every* $S \subseteq L_1$, $\frac{|N_0(S)|}{|S|} \geq \frac{q|L_1|}{(q-3)|S|+4|L_1|}$.

Proof. Since $\sum_{v \in L_0} \Delta_0 \left(\frac{1_S}{|S|} - \frac{1_{L_1}}{|L_1|}\right)(v) = 0$, $\Delta_0 \left(\frac{1_S}{|S|} - \frac{1_{L_1}}{|L_1|}\right)$ is orthogonal to $\Delta_0 \left(\frac{1_{L_1}}{|L_1|}\right)$ which is constant on L_0, hence

$$\|\Delta_0 \left(\frac{1_S}{|S|}\right)\|^2 = \|\Delta_0 \left(\frac{1_{L_1}}{|L_1|}\right) + \Delta_0 \left(\frac{1_S}{|S|} - \frac{1_{L_1}}{|L_1|}\right)\|^2 =$$

$$= \|\Delta_0 \left(\frac{1_{L_1}}{|L_1|}\right)\|^2 + \|\Delta_0 \left(\frac{1_S}{|S|} - \frac{1_{L_1}}{|L_1|}\right)\|^2 = \frac{q(q+1)}{|L_1|} + \|\Delta_0 \left(\frac{1_S}{|S|} - \frac{1_{L_1}}{|L_1|}\right)\|^2.$$

But if f is supported on L_1 then $\|\Delta_0(f)\|^2 = \|\Delta(f)\|^2 - \|\Delta_2(f)\|^2$, and by Theorem 2.1 $\left\|\Delta_0|_{L_2^0(D_g)}\right\| \leq 2\sqrt{q}$, hence

$$\|\Delta_0 \left(\frac{1_S}{|S|}\right)\|^2 \leq \frac{q(q+1)}{|L_1|} + 4q\left(\frac{1}{|S|} - \frac{1}{|L_1|}\right) = \frac{1}{|S|}\left(\frac{(q^2-3q)|S| + 4q|L_1|}{|L_1|}\right).$$

(This may be improved by estimating $\|\Delta_2 \left(\frac{1_S}{|S|} - \frac{1_{L_1}}{|L_1|}\right)\|^2$). Since $1_{N_0(S)}/|N_0(S)|$ is of minimal norm among all the functions f such that f is supported on $N_0(S)$, and $\sum_v f(v)w(v) = 1$, and $\Delta_0 \left(\frac{1_S}{q|S|}\right)$ is one like this, we get

$$\frac{1}{|N_0(S)|} = \|\frac{1_{N_0(S)}}{|N_0(S)|}\|^2 \leq \frac{1}{q^2}\|\Delta_0 \left(\frac{1_S}{|S|}\right)\|^2 \leq \frac{1}{|S|}\left(\frac{(q-3)|S| + 4|L_1|}{q|L_1|}\right)$$

which gives the required result. ∎

Proposition 4.2. *If $q \geq 4$, or $q=3$ and $g(x)$ is irreducible of degree greater than 2, then $D_g(0-1)$ is connected.*

Proof. If not, there is a set $S \subseteq L_1$, $|S| \leq \frac{|L_1|}{2}$ s.t. $|N_0(S)| = \frac{q}{q+1}|S|$ which for $q>3$ is impossible by lemma 4.1. For the case of $q=3$ see remark 4.3. ∎

Remark 4.3 It is not hard to see that $D_g(0\text{–}1)$ is connected iff $PGL_2(R)$ is generated by H_0 and H_1 (the notations are as in remark 3.3). This condition is true for $q \geq 3$ when g is irreducible (if $q=3$ we also need that degree$(g) \geq 3$), since in this case we know that the only subgroup of $PGL_2(R)$ that contains H_0 and H_1, is $PGL_2(R)$ itself [8, th. 2.8.4]. This means that for $|S| \leq \frac{|L_1|}{2}$, $\frac{|N_0(S)|}{|S|} > \frac{q}{q+1}$, and for $q=3$ this is better than what we get by lemma 4.1. (Even the improvement suggested in the proof of lemma 4.1 when applied to the case $q=3$, would give a weaker result when $|S| = |L_1|/3$). What is actually done in lemma 4.1, is to use the bound of $\left\|\Delta|_{L_2^0(D_g)}\right\|$ for the Laplacian of $D_g(0\text{–}1)$, instead of bounding it directly. This way, for $q=3$ we get only the trivial bound $\frac{q}{q+1}$ (which is obtained simply by counting the edges). For $q=2$ it is even worse than this. To get better results an argument in which the whole structure of D_g (not only levels 0,1 and 2) play a role is needed, but we have not been able to find one.

Proposition 4.4.

(a) *For $q \geq 5$, $D_g(0-1)$ is an $\left(\frac{q^{3n-2}\prod}{q-1}, \frac{q}{q+1}, q, \frac{q-4}{q-3}\right)$-bounded concentrator.*

(b) *When $q \geq 5$ is fixed, and degree$(g) \to \infty$, we get an infinite family of $\left(m, \frac{q}{q+1}, q+1, \frac{q-4}{q-3}\right)$ bounded concentrators with $m \to \infty$ linearly.*

Proof. (a) The first three parameters come out from the structure of D_g which is discussed in section 3, and the fourth is by lemma 4.1. ∎

Proposition 4.5. *Using these bounded concentrators for $q = 5$, one gets linear families of (n,d)-superconcentrators with $n \to \infty$, $d=66$.*

Proof. Immediate by combining the result of Theorem A of section 1 and Proposition 4.4. ∎

Remark 4.6 Of course one can cut D_g at any level $i > 1$ and have bounded concentrators again, but the sharpest ratio between inputs and outputs results when cutting after level 1. Even for $q=2,3,4$ one gets b.c. when cutting at higher levels.

Remark 4.7 An argument of N. Pippenger shows that for $q=2$, $D_g(0-1)$ is not a bounded concentrator with reasonable parameters.

Proof. Choose some vertex $u_0 \in L_0$. Choose one of its three neighbors in L_1, let us say this is v_0. v_0 has only one more neighbor in L_0, let us say it is u_1. Repeat this double step by choosing a neighbor $v_1 \in L_1$ of u_1, etc. After not more than $O(\log_2 |L_0|)$ such double steps with suitable choices of the neighbors in L_1, we will come back to one of the u_i-s creating a non trivial cycle. (Since for any graph $G=$

(V,E) in which each vertex is at least of degree k, the girth (i.e., the length of the shortest cycle) is less or equal to $2\log_k|V|$). Throwing out irrelevant vertices we may assume that this cycle is made of $\{u_0,\ldots,u_t\}\subset L_0$ and $\{v_0,\ldots,v_t\}\subset L_1$.

But u_0 still has one unused neighbor in L_1, call it v_{t+1}. Continue the process above from v_{t+1} on, until you get a new cycle or you come back to one of $u_1,\ldots,u_t$. Again this will happen after not more than $O(\log_2|L_0|)$ steps, otherwise you have used more than $|L_0|+|L_1|$ vertices. Since you visit a vertex $v\in L_1$ once at most, but you visit u_0 and one more vertex of L_0 twice, if we denote by S_i the set of vertices you ever visit in $L_i, i=0,1$, we have

$$|N_0(S_1)| = |S_0| < |S_1|$$

so $D_g(0-1)$ is not an $(2^{3n-2}\Pi, 2/3, 2, 4\log_2(2^{3n-1}\Pi/3))$ bounded concentrator. ∎

Questions 4.8

(a) For $q=3,4$ we do not know if $D_g(0-1)$ are good bounded concentrators. If they are so, we get superconcentrators with density 45 for $q=4$, and 28 for $q=3$! Note that by a counting argument Pippenger proved the existence of $(m,2/3,6,1/2)$-b.c. for m large enough, and therefore the existence of s.c. with density 39 (see also [2]). It is clear that the truth is better than what we have by lemma 4.1 (see remark 4.3), but we cannot prove that this is enough to have the required bounded concentrators.

(b) For many purposes it is important to have explicit $(*,\theta,*,\alpha)$-b.c. with a sharp ratio θ. (For example, in the hashing algorithm of Siegel [19], for an integer k and $c<1$, an $\left(n^k, \frac{1}{n^{k-c}}, 2+\frac{k}{c}, \frac{n^{c^2/k}}{2^{e^2}}\right)$-b.c. is used, after proving its existence by a counting argument.)

For $a\in L_1$, we say that it belongs to the vertex (cusp) $b\in L_{n-1}$, if the unique path going from a to level $n-1$ through $L_2, L_3, \ldots$ (not using L_0), ends at b. Look at the following bipartite graph: $I=L_0, O=L_{n-1}$ and an edge exists between $a\in L_0$ and $b\in L_{n-1}$ iff for some $c\in L_1$ which belongs to b, (a,c) is an edge in D_g. It is not hard to see that this graph is $q+1$ regular in the inputs. We have reasons to believe that D_g distributes L_0 uniformly on the cusps, so that this graph is an $\left(\frac{q^{3n}\prod}{q(q^2-1)}, \frac{q+1}{q^{n-1}}, q+1, \alpha\right)$-b.c. for some non trivial α. Is it so?

Acknowledgments. I wish to thank my advisors A. Lubotzky and E. Shamir for fruitful discussions and encouragement. N. Pippenger is gratefully acknowledged for valuable comments.

References

[1] N. Alon, Z. Galil, and V. Milman: Better expanders and superconcentrators, *J. of Alg.* **8** (1987), 337–347.

[2] L. A. Bassalygo: Asymptotically optimal switching circuits, *Problems Information Transmission* **17** (1981), 206–211.

[3] V. G. DRINFELD: The proof of Peterson's Conjecture for $GL(2)$ over global field of characteristic p, *Functional Analysis and its Applications* **22** (1988), 28–43.
[4] I. EFRAT: Automorphic spectra on the tree of PGL_2, *Enseign. Math.* **37** (2) (1991), 31–34.
[5] S. GELBART: *Automorphic Forms on Adele Groups*, Princeton University Press, Princeton 1975.
[6] O. GABER, and Z. GALIL: Explicit construction of linear sized superconcentrators, *J. of Comp Sys. Sci.* **22** (1981), 407–420.
[7] I. M. GELFAND, M. I. GRAEV, and I. I. PYATETSKII-SHAPIRO: *Representation Theory and Automorphic Functions*, W. B. Saunders Com., 1969.
[8] D. GORENSTEIN: *Finite Groups*, Chelsea, 1980.
[9] M. KLAWE: Limitations on explicit constructions of expanding graphs, *SIAM J. Comp.* **13** (1984) 155–156.
[10] S. LANG: $SL_2(R)$, Springer-Verlag, New-York, 1985.
[11] A. LUBOTZKY, R. PHILLIPS, and P. SARNAK: Ramanujan graphs, *Combinatorica* 8(3) 1988, 261–277.
[12] A. LUBOTZKY: *Discrete Groups, Expanding Graphs and Invariant Measures*, Birkhauser Progress in Math, 1994.
[13] G. A. MARGULIS: Explicit construction of concentrators, *Problems of Inform. Transmission* (1975), 325–332.
[14] M. MORGENSTERN: Ramanujan diagrams, *SIAM J. of Discrete Math.*, November 1994.
[15] M. MORGENSTERN: Existence and explicit construction of $q+1$ regular Ramanujan graphs for every prime power q, *J. Combinatorial Theory*, Series B, **62** (1) (1994), 44–62.
[16] M. MORGENSTERN: Ramanujan Diagrams and Explicit Construction of Expanding Graphs, *Ph.D. Thesis, Hebrew Univ. of Jerusalem*, 1990.
[17] G. PRASAD: Strong approximation for semi-simple groups over function fields, *Ann. of Math.* **105** (1977) 553–572.
[18] J. P. SERRE: *Trees*, Springer-Verlag, 1980.
[19] A. SIEGEL: On universal classes of fast high performance hash functions, their time-space tradeoff, and their applications, *30th Annual IEEE conference on Foundations of Computer Science*, (1989), 20–25.
[20] R. M. TANNER: Explicit concentrators from generalized n-gons, *SIAM J. of Alg. Disc. Math.* **5** (1984), 287–294.

Moshe Morgenstern

Department of Mathematics
The Hebrew University, Jerusalem, Israel.
morgen@sunrise.huji.ac.il