Improved lower bounds on the degree-diameter problem

Tao Zhang
joint work with Gennian Ge

Guangzhou University

July 8, 2018

Outline

Degree-diameter problem

- In a graph Γ, the *distance* $d(u, v)$ from a vertex u to another vertex v is the length of a shortest u-v path in Γ.
- The largest distance between two vertices in Γ is the *diameter* of Γ.
- Let $\Gamma = (V, E)$ be a graph of maximum degree d and diameter k. According to the famous Moore bound, Γ has at most $1 + d + d(d-1) + \cdots + d(d-1)^{k-1}$ vertices. When the order of V equals $1 + d + d(d-1) + \cdots + d(d-1)^{k-1}$, the graph Γ is called a *Moore graph*.
- Except $k = 1$ or $d \leq 2$, Moore graphs are only possible for $d = 3, 7, 57$ and $k = 2$.

Problem

Given positive integers d and k, find the largest possible number $N(d, k)$ of vertices in a graph with maximum degree d and diameter k.

$N(d,2)$

- Moore bound: $N(d,2) \leq d^2+1$.
- Erdős et al. (Networks, 1980): $N(d,2) \leq d^2-1$ for $d \geq 4,\ d \neq 7,57$.
- Brown's graphs (Can. Math. Bull., 1966): $N(d,2) \geq d^2-d+i$ for all d such that $d-1$ is a prime power and $i=2$ for $d-1$ even and $i=1$ for $d-1$ odd.
- Širáň et al. (2010): $N(d,2) \geq d^2-2d^{1.525}$ for all sufficiently large d.

Cayley graphs

- Let G be a multiplicative group with the identity element e and $S \subseteq G$ such that $S^{-1} = S$ and $e \notin S$. Here $S^{-1} = \{s^{-1} : s \in S\}$. The Cayley graph $\Gamma(G, S)$ has a vertex set G, and two distinct vertices g, h are adjacent if and only if $g^{-1}h \in S$.
- A Cayley graph is always regular, and its degree equals $|S|$.
- The diameter of a Cayley graph $\Gamma(G, S)$ is k if and only if k is the smallest integer such that all elements in G appear in $\{\Pi_{i=1}^{k} s_i : s_i \in S \cup \{e\}\}$.

Problem

Given positive integers d and k, find the largest possible number $C(d, k)$ ($AC(d, k)$) of vertices in a Cayley graph (Abelian Cayley graph, respectively) with maximum degree d and diameter k.

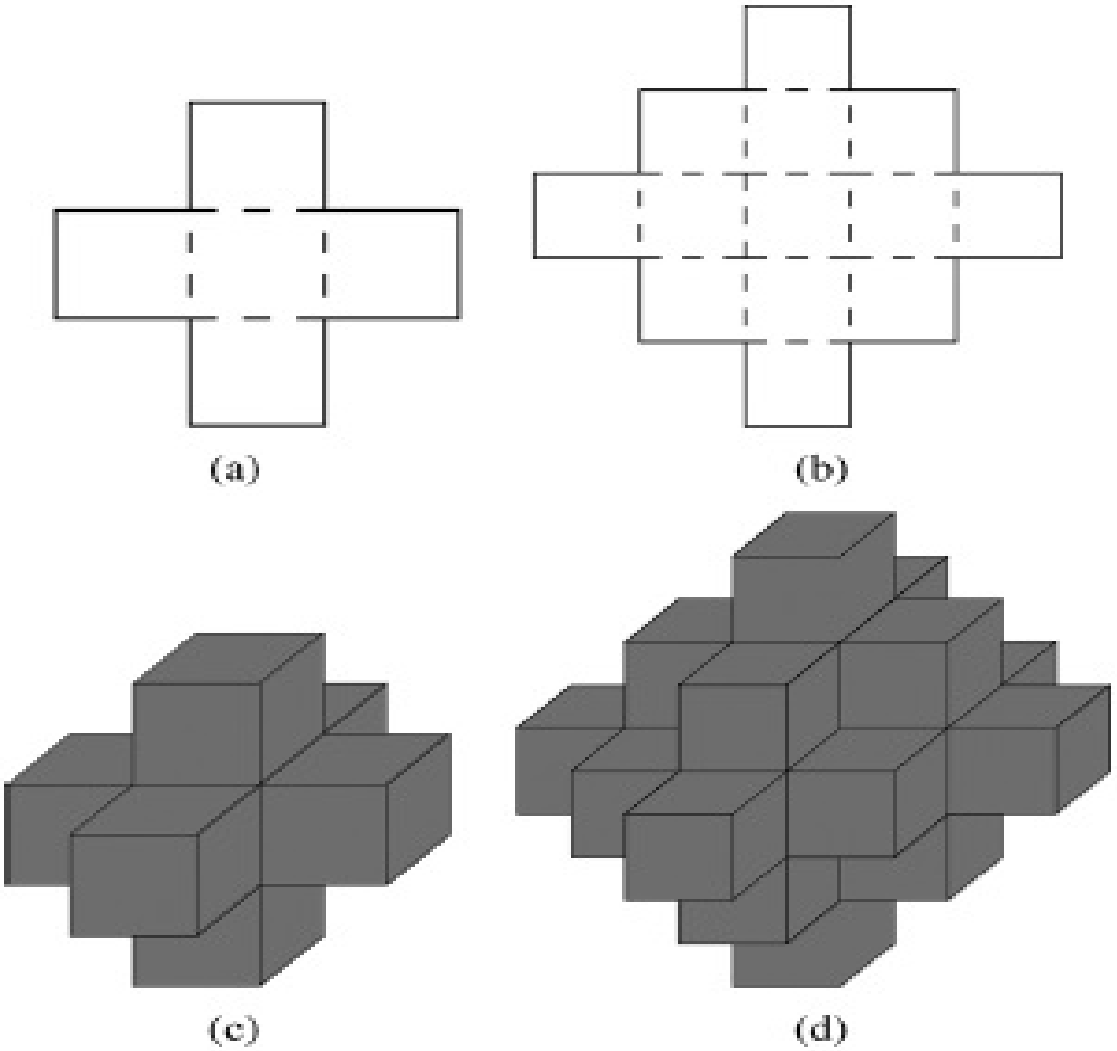
Cayley graphs

- Abas (EJC, 2016): $C(d,2) > 0.684d^2$ for every integer $d \geq 360756$.
- Stanton et al. (SIAM Rev., 1970): $AC(d,k) \leq \frac{d^k}{k!} + O(d^{k-1})$ for $d \to \infty$ and fixed k.
- Dougherty and Faber (SIAM DM, 2004): $AC(d,k) \geq (\frac{d}{k})^k + O(d^{k-1})$.
- Pott and Zhou (JGT, 2017): $AC(d,2) \geq \frac{25}{64}d^2 - 2.1d^{1.525}$.

Abelian Cayley graphs and lattice tilings by Lee spheres

- For $V \subset \mathbb{Z}^n$ and $x \in \mathbb{Z}^n$, $V + x = \{v + x : v \in V\}$.
- A collection $\mathfrak{T} = \{V + l : \ l \in L\}$, $L \subseteq \mathbb{Z}^n$ of copies of V constitutes a tiling of $\mathbb{Z}^n$ by V if $\mathfrak{T}$ forms a partition of $\mathbb{Z}^n$.
- If L further forms a lattice, then $\mathfrak{T}$ is called a *lattice tiling* of $\mathbb{Z}^n$.
- Lee sphere: $S(n, r) = \{x \in \mathbb{Z}^n : d_L(x, 0) = |x_1| + \cdots + |x_n| \leq r\}$.
- C is a perfect Lee code with radius r in $\mathbb{Z}^n$ (denoted by $PL(n, r)$-code) if $\{S(n, r) + c : c \in C\}$ constitutes a tiling of $\mathbb{Z}^n$ by $S(n, r)$.
- C is a linear $PL(n, r)$-code if $\{S(n, r) + c : c \in C\}$ forms a lattice tiling of $\mathbb{Z}^n$.

Lee spheres



Golomb-Welch conjecture

In 1968, Golomb and Welch constructed $PL(1, r)$-codes, $PL(2, r)$-codes and $PL(n, 1)$-codes explicitly. In the same paper, they also proposed the following conjecture.

Conjecture (Golomb-Welch conjecture)

For $n \geq 3$ and $r \geq 2$, there does not exist $PL(n, r)$-code.

- In 1970, Golomb and Welch proved the nonexistence of $PL(n, r)$-codes for given n and $r \geq r_n$, where r_n has not been specified.
- Improvements by Post (1975), Lepisto (1981), Horak, Kim (2017).
- Roughly speacking, for given n, if $r \geq \sqrt{2n}$ then there is no $PL(n, r)$.

Golomb-Welch conjecture

A special case of the Golomb-Welch conjecture, the nonexistence of linear $PL(n, r)$-codes, can be converted into an algebraic combinatorics problem.

Theorem (Horak, AlBdaiwi 2012)

Let $S \subseteq \mathbb{Z}^n$ such that $|S| = m$. There is a lattice tiling of $\mathbb{Z}^n$ by translates of S if and only if there are both an abelian group G of order m and a homomorphism $\phi : \mathbb{Z}^n \mapsto G$ such that the restriction of ϕ to S is a bijection.

Abelian Cayley graphs and linear perfect Lee codes

Corollary

There is a linear $PL(n, r)$-code if and only if there are both an abelian group G and a homomorphism $\phi : \mathbb{Z}^n \mapsto G$ such that the restriction of ϕ to $S(n, r)$ is a bijection.

There exists a linear $PL(n, r)$-code if and only if there exists an abelian Cayley graph with degree $2r$, diameter n and vertices $|S(n, r)|$.

Conjecture

For $d \geq 2$ and $k \geq 3$, $AC(2d, k) < \sum_{i=0}^{min\{k,d\}} 2^i \binom{k}{i} \binom{d}{i}$.

Outline

$AC(d,2)$

Theorem

Let q be a prime power with $q \geq 13$ and $d = 24q - 2$. Then $AC(d,2) \geq \frac{27}{64}(d+2)^2$.

Proof

- Let w be a primitive element in $\mathbb{F}_{243}$.
- $T = \{w^{22i} : i \in [0,10]\}$.
- $T \cup (-T) \cup \{\pm x \pm y : x, y \in T, x \neq y\} \cup \{0\} = \mathbb{F}_{243}$.
- Let $G = \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_{243}$ be an abelian group with multiplication $(x_0, x_1, i) \cdot (y_0, y_1, j) = (x_0 + y_0, x_1 + y_1, i + j)$, where $x_0, x_1, y_0, y_1 \in \mathbb{F}_q$ and $i, j \in \mathbb{F}_{243}$.
- For $a \in \mathbb{F}_q$, let $D_a = \{(x, ax) : x \in \mathbb{F}_q\}$.
- Then $D_a + D_b = \mathbb{F}_q \times \mathbb{F}_q$ for $a \neq b$.

$AC(d,2)$

Proof (Continued)

- Denote $T=\{t_1,t_2,\ldots,t_{11}\}$ and $\mathbb{F}_q=\{a_1,a_2,\ldots,a_q\}$. Define

$$D=((D_{a_{12}},0)\cup(D_{a_{13}},0))\bigcup_{i=1}^{11}((D_{a_i},t_i)\cup(D_{a_i},-t_i))\setminus\{(0,0,0)\}.$$

- $$(D_{a_{12}},0)+(D_{a_{13}},0)=\mathbb{F}_q\times\mathbb{F}_q\times\{0\},$$
$$(D_{a_{12}},0)+(D_{a_i},\pm t_i)=\mathbb{F}_q\times\mathbb{F}_q\times\{\pm t_i\},$$
$$(D_{a_i},\pm t_i)+(D_{a_j},\pm t_j)=\mathbb{F}_q\times\mathbb{F}_q\times\{\pm t_i\pm t_j\}\text{ for }i\neq j.$$

- Hence $(D\cup\{(0,0,0)\})+(D\cup\{(0,0,0)\})$ covers all the elements in G.

$AC(d,2)$

Corollary

For sufficiently large degree d,

$$AC(d,2) \geq \frac{27}{64}d^2 - 3.9d^{1.525}.$$

proof

- Let $p \geq 13$ be an odd prime.
- Let T (G, resp.) be the defining set (group, resp.) of the Cayley graph in above Theorem.
- Then $|T| = 24p - 2$ and the graph has $243p^2$ vertices.
- For any integer $d \in [24p - 2, 243p^2 - 1]$, we can choose and add $(d - |T|)$ elements in G to T to get a new set T' such that $|T'| = d$ and $T' = T'^{-1}$.
- Clearly the Cayley graph $\Gamma(G, T')$ is still of diameter 2.

$AC(d,k)$

Theorem

Let q be a prime power and $d = 11q - 5$. Then $AC(d,4) \geq (\frac{3}{11})^4(d+5)^3(d-6)$.

Proof

- Let $H = \mathbb{F}_q^* \times (\mathbb{F}_q)^3 \times (\mathbb{Z}_3)^4$ be an abelian group with multiplication $(x, x_0, x_1, x_2, i_0, i_1, i_2, i_3) \cdot (y, y_0, y_1, y_2, j_0, j_1, j_2, j_3) = (xy, x_0 + y_0, x_1 + y_1, x_2 + y_2, i_0 + j_0, i_1 + j_1, i_2 + j_2, i_3 + j_3)$, where $x, y \in \mathbb{F}_q^*, x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{F}_q$ and $i_0, i_1, i_2, i_3, j_0, j_1, j_2, j_3 \in \mathbb{Z}_3$.

$AC(d,k)$

Proof (Continued)

$A=\{a(x)=(x,x,0,0,1,0,0,0):x\in\mathbb{F}_q^*\}$, $B=\{b(x)=(x,0,x,0,0,1,0,0):x\in\mathbb{F}_q^*\}$,
$C=\{c(x)=(x,0,0,x,0,0,1,0):x\in\mathbb{F}_q^*\}$, $D=\{d(x)=(x,0,0,0,0,0,0,1):x\in\mathbb{F}_q^*\}$,
$E=\{e(x)=(1,x,0,0,0,0,0,0):x\in\mathbb{F}_q^*\}$, $F=\{f(x)=(1,0,x,0,0,0,0,0):x\in\mathbb{F}_q^*\}$,
$G=\{g(x)=(1,0,0,x,0,0,0,0):x\in\mathbb{F}_q^*\}$,
$a=(1,0,0,0,1,0,0,0)$, $b=(1,0,0,0,0,1,0,0)$,
$c=(1,0,0,0,0,0,1,0)$.

- Define $T'=A\cup B\cup C\cup D\cup E\cup F\cup G\cup\{a,b,c\}$ and $T=T'\cup T'^{-1}$.
- $|T|=11q-5$.

$AC(d,k)$

Proof (Continued)

- $$a(x)a(y)^{-1}f(z)g(w) = (xy^{-1}, x-y, z, w, 0, 0, 0, 0),$$
  $$d(x)d(y)^{-1}f(z)g(w) = (xy^{-1}, 0, z, w, 0, 0, 0, 0),$$
  $$e(x)f(y)g(z) = (1, x, y, z, 0, 0, 0, 0),$$

- $$\{(xy^{-1}, x-y, z, w, 0, 0, 0, 0) : x, y \in \mathbb{F}_q^*,\ z, w \in \mathbb{F}_q\} \cup$$
  $$\{(xy^{-1}, 0, z, w, 0, 0, 0, 0) : x, y \in \mathbb{F}_q^*,\ z, w \in \mathbb{F}_q\} \cup$$
  $$\{(1, x, y, z, 0, 0, 0, 0) : x, y, z \in \mathbb{F}_q\}$$
  $$= \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \times \{0\} \times \{0\} \times \{0\} \times \{0\}.$$

$AC(d,k)$

Theorem

Let q be a prime power, k be an integer and $d=(3k-1)q-k-1$. Then $AC(d,k)\geq(\frac{3}{3k-1})^k(d+k+1)^{k-1}(d-2k+2)$.

Corollary

For sufficiently large degree d,

$$AC(d,k)\geq(\frac{3}{3k-1})^k d^k+O(d^{k-0.475}).$$

$C(d,2)$

Theorem

Let $n=2m$, where m is an odd integer. Let $G=\mathbb{Z}_n\times\mathbb{Z}_n\times\mathbb{Z}_2$ be a group with multiplication $(i_0,i_1,i)\cdot(j_0,j_1,j)=(i_0+j_i,i_1+j_{1-i},i+j)$, where $(i_0,i_1,i),(j_0,j_1,j)\in\mathbb{Z}_n\times\mathbb{Z}_n\times\mathbb{Z}_2$. If there exists a subset $T\subseteq G$ such that

1. *at least one of $\{(m,0,0),(0,m,0)\}$ is contained in T;*
2. *if $(i,j,0)\in T$, then $i+j\equiv 1 \pmod 2$;*
3. *$(T\cup T^{-1})\cdot(T\cup T^{-1})\supseteq G$,*

then for any odd prime $p>4|T|$, there exists a Cayley graph of diameter two, degree $(2|T|+1-\epsilon-\rho)p-1$, and of order $2p^2n^2$, where $\epsilon=|T\cap\{(m,0,0),(0,m,0)\}|$ and $\rho=\min\{1,|T\cap\{(i,n-i,1):i\in[0,n-1]\}|\}$.

$C(d,2)$

Proof

Let $H = \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_2$ be a group with multiplication
$(x_0, x_1, i_0, i_1, i) \cdot (y_0, y_1, j_0, j_1, j) =$
$(x_0 + (-1)^{i_0} y_i, x_1 + (-1)^{i_1} y_{1-i}, i_0 + j_i, i_1 + j_{1-i}, i + j)$.
We divide T into five subsets:

$$
\begin{aligned}
T_1 &= \{(m,0,0)\},\\
T_2 &= \{(i_z, n-i_z, 1)\},\\
T_3 &= \{(0,m,0)\} \cap T,\\
T_4 &= \{(i,j,0) : \ (i,j,0) \in T, (i,j,0) \neq (m,0,0), (0,m,0)\}\\
&= \{(t_i, s_i, 0) : \ i \in [1,l]\},\\
T_5 &= \{(i,j,1) : \ (i,j,1) \in T, (i,j,1) \neq (i_z, n-i_z, 1)\}\\
&= \{(u_i, v_i, 1) : \ i \in [1,k]\}.
\end{aligned}
$$

$C(d,2)$

Proof

Define

$$
\begin{aligned}
X_1 &= \{A(x) = (x, a_1x, m, 0, 0) : x \in \mathbb{F}_p\},\\
X_2 &= \{B(x) = (x, -x, i_z, n - i_z, 1) : x \in \mathbb{F}_p\},\\
X_3 &= \{C(x) = (x, 0, 0, m, 0) : \ (0, m, 0) \in T, x \in \mathbb{F}_p\},\\
X_4 &= \{D_i(x) = (x, a_{i+1}x, t_i, s_i, 0) : \ x \in \mathbb{F}_p, i \in [1, l]\},\\
X_5 &= \{E_i(x) = (x, a_{i+l+1}x, u_i, v_i, 1) : \ x \in \mathbb{F}_p, i \in [1, k]\},\\
X &= X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5.
\end{aligned}
$$

$\Rightarrow (X \cup X^{-1}) \cdot (X \cup X^{-1}) \supseteq H.$

$C(d,2)$

Let $G = \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$ be a group with multiplication $(i_0, i_1, i) \cdot (j_0, j_1, j) = (i_0 + j_i, i_1 + j_{1-i}, i + j)$. Let

$$T = \{(5,0,0),(0,0,1),(1,0,1),(5,0,1),(1,3,1),(1,7,1),(5,2,1),(3,2,0),(4,1,0)\}.$$

we have:

Corollary

Let $p > 36$ be an odd prime and $d = 17p - 1$. Then there exists a Cayley graph of diameter two, degree d, and of order $\frac{200}{289}(d+1)^2$.

Corollary

For sufficiently large degree d,

$$C(d,2) \geq \frac{200}{289}d^2 - 5.4d^{1.525}.$$

THANK YOU