Cayley graphs in the degree/diameter problem

Jozef Širáň

Open University and Slovak University of Technology

AGTIW, 19 January 2021

A likely motivation question at IBM Research Labs in the late 1950's:

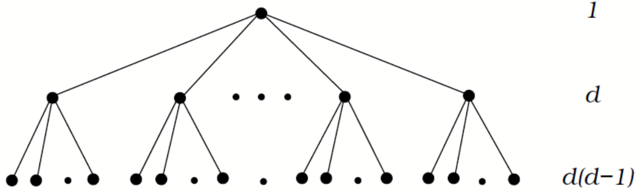
A processor network is to be built such that each processor communicates directly with at most d *other processors via a hardware link and every pair of distinct processors can communicate either directly or by means of at most one intermediate processor. What is the largest number* $n(d, 2)$ *of processors in such a network?*

This translates into the question of determining the largest $n(d, 2)$ for which there exists a graph of maximum valency d and diameter 2.

There is an obvious extension to finding the largest order $n(d, k)$ of a graph of maximum degree d and diameter k – the (d, k)-graphs – but let us begin with $k = 2$; even this one has generated great mathematics.

It turns out that there is a straightforward upper bound on $n(d, 2)$, the so-called Moore bound $M(d, 2)$, named after E. F. Moore (Bell Labs).

The largest order $M(d, 2)$ of a graph of max valency d and diameter 2?



Conclusion: The Moore bound for the pair $(d, 2)$ is $M(d, 2) = d^2 + 1$.

Theorem [Hoffman and Singleton, 1960] *The Moore bound $M(d, 2)$ can be attained only if $d \in \{2, 3, 7\}$ and, possibly, for $d = 57$.*

Proof. A beautiful illustration of combining elementary observations by the following two facts from linear algebra about square matrices:

Fact 1: The trace $\mathrm{tr}(A)$ is equal to the sum of eigenvalues in $\mathrm{Sp}(A)$.

Fact 2: If $B = f(A)$ for some polynomial f, then $\mathrm{Sp}(B) = f(\mathrm{Sp}(A))$.

Observation: An adjacency matrix A of a Moore graph of diameter 2, valency d and order $n = d^2 + 1$ satisfies: $A^2 + A - (d-1)I = J$.

F2 applied to $B{=}J{=}f(A)$: If $d \neq \lambda \in \mathrm{Sp}(A)$, then $\lambda^2 + \lambda - (d{-}1) = 0$.

Surprise 1: The matrix A (dim $n{=}d^2{+}1$) has only 3 eigenvalues! d, r_1, r_2

If r_1, r_2 are irrational, they must be of the same multiplicity; invoking F1, $0 = d + (r_1 + r_2)(n-1)/2 = d - d^2/2$, so that $(d, n) = (2, 5)$ or $(0, 1)$.

If $r_1, r_2 = (-1 \pm \sqrt{4d-3})/2$ are rational, then they must be integers!

So, $4d - 3 = s^2$ and $r_1, r_2 = (-1 \pm s)/2$. If r_1 has multiplicity m, then $0 = d + m(-1{+}s)/2 + (n{-}1{-}m)(-1{-}s)/2$; and a few substitutions give

Surprise 2: $s^5 + s^4 + 6s^3 - 2s^2 + (9 - 32m)s - 15 = 0$ giving, for $d \geq 2$, (d, n): $(3, 10)$ (Petersen), $(7, 50)$ (Hoffman-Singleton), $(57, 3250)$ (?).

The Moore bound for general degree and diameter:

$$n(d,k) \le M(d,k) = 1 + d + d(d-1) + \ldots + d(d-1)^{k-1} \approx d^k \text{ for } d \to \infty$$

Theorem. *For $d \ge 3$, $k \ge 3$ we have $n(d,k) < M(d,k)$; equivalently, there are no Moore graphs of diameter larger than two.*
[Hoffman+Singleton 1960 (k=3), Bannai+Ito 1973, Damerell 1973]

[Bermond+Bollobás 81] *For any c, are there $d, k \ni n(d,k) < (M(d,k) - c$?*

[Exoo+Jajcay+Mačaj+Š 2019] *For any given $d \ge 3$ and $c \ge 2$ there exists a set $\mathcal{S}$ of natural numbers of asymptotic density one such that, for every $k \in \mathcal{S}$, each vertex-transitive (d,k)-graph has order $< M(d,k) - c$.*

[Jajcay+Filipovski 2021] *If $\neg[\mathrm{B+B}]$, then for every d and all sufficiently large even k the largest (d,k)-graphs would have to be Ramanujan graphs.*

Lower bounds on $n(d,k)$? A number of available constructions ... but:

How close to the Moore bound can one get by Cayley graphs?

Largest order of a vertex-trans. (Cayley) (d,k)-graph: $\mathrm{vt}(d,k)$, $\mathrm{Cay}(d,k)$

Diameter 2

[Šiagiová+Š 2011] *For any* $d \in D = \{2^{2m} + 2^{m+2}-6;\ m\geq 1\}$ *there exists a Cayley* $(d,2)$ *graph of order* $> d^2 - 6\sqrt{2}d^{3/2}$*:* $\limsup_d \mathrm{Cay}(d,2)/d^2 = 1$.

Construction: Let $F = GF(q)$ for $q = 2^{2m}$ and take $G = F^+ \rtimes F^*$ with $(a,b)(c,d) = (a+bc, bd)$ for $a,c \in F^+$, $b,d \in F^*$; $X = \{(b,b^2);\ b \in F^*\}$.

- For 'most' $\alpha \in F^+,\ \beta \in F^*$ the equation $(\alpha,\beta) = (x,x^2)(y,y^2)$ has a solution in G. Make a $\mathrm{Cay}(G, X \cup S)$ of diam 2, where $|S| = 2^{m+2}-6$.

The set D of degrees is sparse... a nice counterpart for almost all degrees:

[Abas 2016] *For every prime* $p \equiv 1 \bmod 10$ *there is a Cayley graph for the group* $(C_p^2) \rtimes (C_{10}^2 \rtimes C_2)$ *of order* $200p^2$*, degree* $17p-1$ *and diameter* 2*. Results on density of primes* $\Rightarrow$ $\mathrm{Cay}(d,2) > 0.684d^2$ *for all* $d \geq 360756$.

Winner: Quotients of incidence graphs of projective planes by polarity, with $n(q+1,2) = q^2+q+1$ for q a prime power, $\Rightarrow$ $\liminf_d n(d,2)/d^2 = 1$.

Aesthetical drawback: Not even regular, and not a spanning subgraph of any vertex-transitive graph of degree $q+5$ [Bachratý+Š 2015].

Diameter 3

[Bachratý+Šiagiová+Š 2019] *For* $q = 2^{2n+1}$ *we have a Cayley* (d,k)*-graph of order* $q^2(q-1)$*,* $d \le q+4\lceil\sqrt{q}\rceil+3$ *and* $k=3$*:* $\limsup_d \mathrm{Cay}(d,3)/d^3 = 1$*.*

Outline: W_q – generalised quadrangle in $\mathrm{PG}(3,q)$, with lines of $\mathrm{PG}(3,q)$ isotropic w.r.t. a 4-dimensional skew-symmetric bilinear form over $\mathrm{GF}(q)$; incidence by containment. [Tits '62]: W_q admits a polarity π iff $q=2^{2n+1}$.

Letting $f(x,y) = x^{\omega+2} + xy + y^{\omega}$ for $\omega = 2^{m+1}$, the set of matrices

$$M(r;a,b) = \begin{pmatrix} 1 & f(a,b) & a & b \\ 0 & r^{\omega+2} & 0 & 0 \\ 0 & (a^{\omega+1}+b)r & r & a^{\omega}r \\ 0 & ar^{\omega+1} & 0 & r^{\omega+1} \end{pmatrix}$$

form a group G of collineations acting on $\mathrm{I}(W_q)/\pi$, with $|G| = q^2(q-1)$, a subgroup of the Suzuki group $Sz(q) = {}^2B_2(q)$ fixing the point $[0,1,0,0]$ in the Suzuki-Tits ovoid $\Omega = \{[0,1,0,0]\} \cup \{[1,f(x,y),x,y];\ x,y \in \mathrm{GF}(q)\}$.

G has a regular orbit on $(\mathrm{I}(W_q)/\pi)\setminus\Omega \Rightarrow$ a subgraph A_q of degree $q-1$. Extend A_q to a Cayley graph for G of diam 3 and deg $\le q+4\lceil\sqrt{q}\rceil+3$. □

Diameter $k \geq 4$

Temptation: Keep using generalized ℓ-gons to construct Cayley graphs of diameter 5, degree $q + o(q)$ and order $q^5 - o(q^5)$ from a suitable regular group on a subgraph obtained from a generalised hexagon $H(q)$ factored by a polarity; these exist iff $q = 3^{2n+1}$. The corresponding Ree-Tits ovoid is fixed by the Ree group ${}^2G_2(q)$; simple group; order $q^3(q^3+1)(q-1)$. Unfortunately, by the classification of maximal subgroups of Ree groups [Levchuk and Nuzhin '85], ${}^2G_2(q)$ has no subgroup of order $O(q^5)$, $q \to \infty$.

Cayley record holders for $k \geq 4$ [Macbeth-Šiagiová-Š-Vetrík 2009, Macbeth-Šiagiová-Š 2011]: $\liminf_{d\to\infty} \mathrm{Cay}(d,k)/M(d,k) \geq k/3^k$.

Construction: $m \geq 2$, $G = \mathbb{Z}_{m^k-1} \rtimes \mathbb{Z}_k$, $(u,y)(v,z) = (u + m^y v, y+z)$. Trick: For any $x \in \mathbb{Z}_{m^k-1}$ there exist $x_0, x_1, \ldots, x_{k-1} \in [-t,t]$, $t = \lfloor \frac{m}{2} \rfloor$, with $x = x_0 m^0 + x_1 m^1 + \ldots + x_{k-1} m^{k-1}$. Let $s = \lfloor \frac{k}{2} \rfloor$, $a_i = (i,1) \in G$, $b_i = (im^s, 0) \in G$, $i \in [-t,t]$. Finally, let $X = \left(\cup_{-t}^{+t} \{a_i, a_i^{-1}, b_i\}\right) \setminus \{b_0\}$. $\mathrm{Cay}(G,X)$ has diameter k, degree $d = 6\lfloor \frac{m}{2} \rfloor + 2$ and order $k(m^k - 1)$.

Comparing record holders in various categories

For Cayley graphs we saw that $\liminf_{d\to\infty} \mathrm{Cay}(d,k)/M(d,k) \geq k3^{-k}$

But [Faber+Moore+Chen 1993]: $\liminf_{d\to\infty} \mathrm{vt}(d,k)/M(d,k) \geq 2^{-k}$

Digraphs $\Gamma_{\delta,k}$: vertices are k-strings of distinct symbols from a $(\delta+1)$-set, where $3 \leq k \leq \delta$; arcs $x_1x_2\ldots x_k \to x_2\ldots x_k y$ for $y \neq x_1,\ldots,x_k$ and $x_1x_2\ldots x_k \to x_1x_2\ldots\hat{x}_i\ldots x_k x_i$ for $1 \leq i \leq k-1$. Forgetting directions in $\Gamma_{\delta,k}$ gives undirected vertex-transitive (d,k)-graphs for $d = 2\delta-1$, ...

But but: For (d,k) such that $0.31d \leq k \leq (d+2)/2$ the largest currently known Cayley (d,k)-graphs beat the corresponding vertex-transitive ones.

Ultimate winner [Canale+Gomez 2005]: $\liminf_{d\to\infty} n(d,k)/d^k \geq 1.45^{-k}$

for $d \equiv -1,0,1$ mod 8, and with 1.57^{-k} on rhs for $d \equiv -1,0,1$ mod 6; a very complex method using 'shuffle exchange product' of graphs.

A challenge for Cayley-ists...

Instead of a conclusion ... an interesting connection, and a few apologies ...

A subset B of a group G is an h-basis of G if $B^h = G$. $\Rightarrow$ $|B| \geq |G|^{1/h}$

[Rohrbach 1937] Is it true that for every $h \geq 2$ there is a $c_h \geq 1$ such that *every* finite group G admits an h-basis B satisfying $|B| \leq c_h |G|^{1/h}$?

[Kozma+Lev 1994] If every composition factor of G is alternating or cyclic, then G has a h-basis B such that $|B| \leq (2h-1)|G|^{1/h}$ for each h.

For deg/diam in undirected graphs one needs B symmetric – no results!

My apologies for not having mentioned:

- results in the degree/diameter problem for bipartite graphs, circulants, Abelian Cayley graphs, directed graphs, mixed graphs, hypergraphs, ...
- results for various families of Cayley graphs by M. Abas, D. Bevan, G. Erskine, E. Loz, H. Macbeth, J. Šiagiová, J. Tuite, T. Vetrík,..., R. Lewis
- authors of a number of computer-aided results listed in wiki tables ...

THANK YOU.