Search for properties of the missing Moore graph

M. Mačaj and J. Širáň

SGT in Rio
December 3th 2008

Moore graphs

Single graph Γ with maximum degree k and diameter d is a *Moore graph* if

$$|\Gamma| = 1 + k + k(k-1) + k(k-1)^2 + \cdots + k(k-1)^{d-1}.$$

Moore graphs with diameter 2 are strongly regular graphs with parameters $(k^2+1, k, 0, 1)$, i.e., k-regular graph on k^2+1 vertices such that

$$a \sim b \Rightarrow |N(a) \cap N(b)| = 0 \text{ and } a \not\sim b \Rightarrow |N(a) \cap N(b)| = 1. \quad (1)$$

Moore graphs

Theorem. A. J. Hoffman, R.R. Singleton (1960) *Moore graph with $d = 2$ exists only if k is equal to* 2, 3, 7 *or (maybe)* 57.

Theorem. E. Bannai, T. Ito (1973), **R.M. Damerell (1973)** *Nontrivial Moore graphs exist only for $d = 2$.*

- $k = 2$, $v = 5$: a pentagon

- $k = 3$, $v = 10$: the Petersen graph

- $k = 7$, $v = 50$: the Hoffman-Singleton graph

- $k = 57$, $v = 3250$: ???

The missing Moore graph

From now on, let Γ be a Moore graph of valency 57 and diameter 2 and X a group of automorphisms of Γ.

Lemma. *The eigenvalues of* Γ *are* $\lambda_0 = k = 57$, $\lambda_1 = r = 7$ *and* $\lambda_2 = s = -8$. *Their multiplicities are* 1, $f = 1729$ *and* $g = 1520$, *respectively.*

The eigenspace for an eigenvalue λ_i will be denoted V_i.

Known properties of $\mathrm{Aut}(\Gamma)$

Theorem. M. Aschbacher (1971) $\mathrm{Aut}(\Gamma)$ *is not a rank* 3 *group.*

Theorem. D. Higman (??) $|\mathrm{Aut}(\Gamma)|$ *is not divisible by* 4*. In particular,* $\mathrm{Aut}(\Gamma)$ *is solvable and* Γ *is not vertex transitive.*

Theorem. A.A. Makhnev , D.V. Paduchikh (2001) *If* $|\mathrm{Aut}(\Gamma)|$ *is even, then* $|\mathrm{Aut}(\Gamma)| \leq 550$*.*

Lemma. $|\mathrm{Aut}(\Gamma)|$ *divides* $2 \cdot 5^6 \cdot 3^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 19 = 33699206250$*.*

Linear representations of groups

Let G be a finite group and F be a field. A *linear representation* of G over F is any homomorphism $R : G \to \mathsf{GL}(V, F)$, where V is a finite-dimensional linear space over F. A *character* of R is the mapping $\rho : G \to F$, $g \mapsto \mathsf{Tr}\, g^R$.

A subspace U of V is R-*invariant* if for any $g \in G$ we have $U^{g^R} = U$. Linear representation R is *irreducible* if V has only trivial R-invariant subspaces.

Characters and combinatorics

Theorem. D. Higman *Let* χ_i *be the character of the projection of* Aut(Γ) *onto the eigenspace* V_i *(*$i = 0, 1, 2$*). Let* $x \in \mathrm{Aut}(\Gamma)$ *and let* $a_i(x) = |\{v \in \Gamma;\ d(v, v^x) = i\}|$ *(*$i = 0, 1, 2$*). Then*

$$(a_0(x), a_1(x), a_2(x))^T = \begin{pmatrix} 1 & 1 & 1 \\ 57 & 7 & -8 \\ 3192 & -8 & 7 \end{pmatrix} (\chi_0(x), \chi_1(x), \chi_2(x))^T.$$

Corollary. $\chi_1(x) = (8a_0(x) - a_1(x) + 50)/15$ *is an integer.*

$\mathbb{Q}$-linear representations of groups

Rational classes of a finite group G are equivalence classes of

$$x \sim y \Leftrightarrow \exists z \in G: \ \langle x \rangle = \langle y \rangle^z.$$

Theorem. *Every character of $\mathbb{Q}$-linear representation of G is constant on rational classes of G and the number of irreducible $\mathbb{Q}$-linear representation of G is equal to the number of rational classes of G.*

Theorem. *Let ρ be a character of a $\mathbb{Q}$-linear representation of G. Let $\rho_1, \rho_2, \ldots \rho_m$ be the $\mathbb{Q}$-irreducible characters of G and let $x_1, \ldots, x_m$ be representatives of rational classes of G. Then the system*
$$\begin{pmatrix} \rho_1(x_1) & \rho_2(x_1) & \ldots & \rho_m(x_1) & | & \rho(x_1) \\ \rho_1(x_2) & \rho_2(x_2) & \ldots & \rho_m(x_2) & | & \rho(x_2) \\ \vdots & \vdots & & \vdots & | & \vdots \\ \rho_1(x_m) & \rho_2(x_m) & \ldots & \rho_m(x_m) & | & \rho(x_m) \end{pmatrix}$$
of linear equations has an solution in $\mathbb{N}_0$.

$x \in \mathsf{Aut}(\Gamma)$, $|x| = pq$, $p < q$

pq	$a_0(x)$	$a_0(x^p)$	$a_0(x^q)$	$a_1(x)$	$a_1(x^p)$	$a_1(x^q)$
6	2	10	56	$4 + 90k$	0	112
10	1	5	56	$102 + 150k$	$10 + 150l$	112
10	6	50	56	$62 + 150k$	$100 + 150l$	112
14	7	9	56	$84 + 210k$	$98 + 210l$	112
14	14	16	56	$28 + 210k$	$42 + 210l$	112
14	21	23	56	$182 + 210k$	$196 + 210l$	112
14	28	30	56	$126 + 210k$	$140 + 210l$	112
14	35	37	56	$70 + 210k$	$84 + 210l$	112
14	42	44	56	$14 + 210k$	$28 + 210l$	112
22	1	5	56	222	220	112
15	0	0	10	$5 + 75k + 225m$	$50 + 75k$	0
35	1	16	50	$42 + 105k$	$147 + 105k$	175
55	5	5	5	55	55	385

Adjacency matrix of an automorphism group

Lemma. *Let X be an automorphism group of Γ having orbits $O_1, O_2, \ldots, O_m$ of size $s_1, s_2, \ldots, s_m$, respectively. Let $a \in O_i$. Then the number $b_{i,j} = |N(a) \cap O_j|$ does not depend on a and the matrix $B = \|b_{i,j}\|$ satisfies:*
1) $s_i b_{i,j} = s_j b_{j,i}$;
2) $B^2 + B - 56I = (1, 1, \ldots, 1)^T (s_1, s_2, \ldots, s_m)$,
3) eigenvalues of B belong to $\{57, 7, -8\}$.

Corollary.

$$Tr(B) \equiv 80 - 8m \mod 15. \qquad (2)$$

Additional ingredients

- Sylow's theorems
- subgroups lattices
- small groups libraries
- computations in GAP

New results

Theorem. M.M., J. Širáň 2008 *Size of* Aut(Γ) *is at most* 375. *In particular,*

- *if* $|\operatorname{Aut}(\Gamma)|$ *is odd, then* $|G| \in \{1, 3, 5, 7, 11, 13, 15, 19, 21, 25, 27, 35, 39, 45, 55, 57, 75, 81, 125, 135, 147, 171, 275, 375\}$;

- *if* $|\operatorname{Aut}(\Gamma)|$ *is even, then* $|G| \in \{2, 6, 10, 14, 18, 22, 38, 50, 54, 110\}$.

Thank You