Automorphism groups, isomorphism, reconstruction (Chapter 27 of the Handbook of Combinatorics)

László Babai*
Eötvös University, Budapest,
and
The University of Chicago

June 12, 1994

Contents

*Section 2 was written in collaboration with Wilfried Imrich

Note. While this chapter contains a substantial amount of material on infinite graphs, its focus is on finite graphs. Therefore all graphs will be **finite**, unless otherwise stated. Exceptions are Sections 3.6, 3.7, and 3.11, where graphs are generally infinite, and Sections 3.9, 3.10, 5.3, where a main theme is the interplay between finite and infinite.

Surveys. A portion of the material discussed in this chapter is covered in two survey articles on automorphism groups of graphs: Cameron [Cam83] and Babai–Goodman [BG93]. Chapter 12 of Lovász [Lov79a] is a nice introduction to the subject. A beautiful treatment of the basics of higher symmetry is Biggs [Big74]. Brouwer, Cohen, Neumaier [BCN89] is a

monumental yet enjoyable work on distance-transitivity and related subjects with detailed up-to-date information. Much of our current knowledge on graph isomorphism testing is summarized in Babai, Luks [BL83]. The general concept of reconstruction (invertibility of various constructions) is illustrated in Chapter 15 of Lovász [Lov79a]. Recent surveys on the Kelly-Ulam graph reconstruction conjecture include Bondy [Bon91], Ellingham [Ell88] (see also [BH77]).

0 Introduction

0.1 Graphs and groups

A study of graphs as geometric objects necessarily involves the study of their symmetries, described by the group of automorphisms. Indeed, there has been significant interaction between abstract group theory and the theory of graph automorphisms, leading to the construction of graphs with remarkable properties as well as to a better understanding and occasionally a construction or proof of nonexistence of certain finite simple groups. On the other hand, in contrast to classical geometries, most finite graphs have no automorphisms other than the identity (asymmetric graphs), a fact that is largely and somewhat paradoxically responsible for its seeming opposite: every (finite) group is isomorphic to the automorphism group of a (finite) graph.

The study of graphs via their symmetries is rooted in the classical paradigm, stated in Felix Klein's *"Erlanger Programm",* that geometries are to be viewed as domains of a group action. Although graphs, as incidence structures, may seem to be degenerate geometries, we note that any incidence structure (such as a projective plane) can be represented by a graph. (The *Levi graph* L of an incidence structure S is a bipartite graph; its vertices correspond to the points and lines of S; and adjacency of vertices of L corresponds to point-line incidence in S.) Such representations preserve symmetry and allow fruitful generalizations (such as "generalized polygons", Chap. 13, Sec. 7).

In this chapter we try to illustrate the variety of ways in which groups and graphs interact. The effect of powerful results of group theory (such as the Feit–Thompson theorem on the solvability of groups of odd order) will be evident already in the introductory Sec. 1.1. Consequences of the *Classification of Finite Simple Groups* (CFSG) are required for some of the results in Sec. 4.3 and for the analysis of some of the algorithms in Sections 6.6, 6.7. Many of the results surveyed in Sec. 5 critically depend on the CFSG. On the other hand, some results of graph theoretic nature have played a role in the classification theory itself, as illustrated in Sections 3.5 and 5.1.

In spite of these connections, *the treatment of the subject will mostly be kept on an elementary level*, requiring little more than basic group theory. The main theme of Sec. 3 is the surprisingly strong effect of modest symmetry assumptions on the combinatorial parameters of a graph.

We try also to illustrate some of the links of the subject to areas not immediately seen to relate to groups. Sections 1.6, 7.2 illustrate this point within combinatorics. Several connections to topology are explored in Section 3 (see esp. Sections 3.6 and 3.7). Random walks feature in Sec. 3.8; linear algebra is visited briefly in Sections 1.5, 3.8, 3.12, 7.2.

Strong links have been forged to model theory (Sec. 5.3) and to the theory of algorithms (Sec. 6.6, 6.7). Some of the remote sources of motivation include algebraic topology (Sec. 3.11), differential geometry (Secs. 3.6, 3.7), and even a classical discovery in quantum mechanics (Sec. 1.5).

0.2 Isomorphisms, categories, reconstruction

Isomorphisms of graphs are bijections of the vertex sets preserving adjacency as well as non-adjacency. In the case of directed graphs, orientations must be preserved; in the case of graphs with colored edges and/or vertices, we agree that colors, too, must be preserved. Similar definitions apply to hypergraphs. In the case of incidence structures consisting of "points" and "lines", linked by incidence relations, we think of an isomorphism as a pair of bijections (one between the points, another between the lines), so that the pair preserves incidence. This view should be applied to graphs as well if multiple edges are allowed.

Automorphisms of the graph $X = (V, E)$ are $X \to X$ isomorphisms; they form the subgroup $\mathrm{Aut}(X)$ of the symmetric group $\mathrm{Sym}(V)$. Automorphisms of directed graphs, etc., are defined analogously.

The questions of *reconstruction* are, broadly speaking, questions of invertibility of certain isomorphism preserving operations on structures. A category in which all morphisms are isomorphisms is called a Brandt groupoid. Let $\mathcal{C}$, $\mathcal{D}$ be two Brandt groupoids and $F : \mathcal{C} \to \mathcal{D}$ a functor. Hence $X \cong Y$ implies $F(X) \cong F(Y)$. We call F *weakly reconstructible* if the converse also holds: $F(X) \cong F(Y)$ implies $X \cong Y$. We say that F is *strongly reconstructible* if for every pair X, Y of objects of $\mathcal{C}$, F induces a bijection between the sets $\mathrm{Iso}(X, Y)$ and $\mathrm{Iso}(F(X), F(Y))$ of isomorphisms. In this case, $\mathrm{Aut}(X) \cong \mathrm{Aut}(F(X))$ for every object X. We also say that, within the class $\mathcal{C}$, the object X is (weakly, strongly) reconstructible from $F(X)$.

A classical example is the reconstructibility of a multiset of direct irreducible finite groups from their direct product (unique direct factorization, R. Remak – O. Yu. Schmidt, cf. Baer [Bae47]). The category $\mathcal{C}$ consists of the multisets of direct irreducible finite groups with the natural notion of isomorphism. Let F associate the direct product of the members of such a multiset X with X. This functor is weakly but not strongly reconstructible. (To see the latter, consider the pair $\{\mathbb{Z}_p, \mathbb{Z}_p\}$.)

Homomorphisms of graphs are defined as adjacency preserving maps, i.e., a map $f : V_1 \to V_2$ is a homomorphism of the graph $X_1 = (V_1, E_1)$ to the graph $X_2 = (V_2, E_2)$ if $(f(x), f(y)) \in E_2$ whenever $(x, y) \in E_1$. It is not required that nonadjacency be preserved; therefore a bijective homomorphism is not necessarily an isomorphism. It is easy to see that the chromatic number of the graph X is the smallest (cardinal) number m such that the set $\mathrm{Hom}(X, K_m)$ of $X \to K_m$ homomorphisms is nonempty. The set $\mathrm{End}(X) = \mathrm{Hom}(X, X)$ forms a monoid (semigroup with identity) under composition: the *endomorphism monoid* of X. $\mathrm{Aut}(X)$ consists of the invertible elements of $\mathrm{End}(X)$. The class of graphs together with the homomorphisms forms a *category*. These concepts extend naturally to directed graphs (orientation of edges must be preserved), graphs with colored vertices and/or edges (homomorphisms preserve color by definition); and to general relational structures involving relations of arbitrary arities.

The interconnections of these areas are manifold. The algorithmic problem of deciding whether or not two given graphs are isomorphic is equivalent to determining the automorphism group, and specific automorphism information for certain classes of graphs made it possible to use group theory to surprising depth in the analysis of graph isomorphism algorithms. Isomorphism rejection tools include graph invariants, i. e., functions F such that $X \cong Y$ implies $F(X) = F(Y)$. The construction of combinatorial, algebraic, and topological structures with prescribed automorphism groups and endomorphism monoids usually amounts to constructing strongly reconstructible functors. Reconstruction itself is an isomorphism problem, and automorphism groups have played a role in its study. Finally, establishing reconstructibility of certain functors is a useful tool in determining the automorphism groups of certain derived structures.

1 Definitions, examples

In this section, we collect some illustrative facts about automorphism groups of graphs and their interplay with reconstruction type problems.

We start with the simplest examples. A graph and its complement have the same automorphisms. The automorphism group of the complete graph K_n and the empty graph $\overline{K}_n$ is the symmetric group S_n, and these are the only graphs with doubly transitive automorphism groups. The automorphism group of the cycle of length n is the dihedral group D_n (of order $2n$); that of the directed cycle of length n is the cyclic group $\mathbb{Z}_n$ (of order n). A path of length ≥ 1 has 2 automorphisms. The automorphism group of a graph is determined by the automorphism groups and the isomorphisms of its connected components: if $X_1, \ldots, X_k$ are pairwise nonisomorphic connected graphs, and X is the disjoint union of m_i copies of X_i, $i = 1, \ldots, k$, then

$$\mathrm{Aut}(X) = \mathrm{Aut}(X_1) \wr S_{m_1} \times \cdots \times \mathrm{Aut}(X_k) \wr S_{m_k}. \tag{1}$$

The wreath products occurring here realize their imprimitive action (cf. Chap. 12).

1.1 Measures of symmetry

A graph is *vertex-transitive* if its automorphism group acts transitively on the set of vertices. Such a graph is necessarily regular; the union of a 3-cycle and a 4-cycle show that the converse does not hold. If the group acts transitively on edges, the graph is *edge-transitive*. A vertex-transitive graph need not be edge-transitive. (Example: triangular prism.) If X is an edge-transitive graph without isolated vertices, and X is not vertex-transitive, then it must be bipartite, with the group acting transitively on each color class. The complete bipartite graphs $K_{m,n}$ with $m \neq n$ show that this can indeed happen. *Regular* graphs with edge but not vertex-transitive automorphism groups are not so easy to construct (cf. [Fol67, Bou69, Bou72, Tit75, Kli81]).

A *flag* in a graph X is an ordered pair (v, e) where v is a vertex and e is an edge incident with v. If $\mathrm{Aut}(X)$ is transitive on flags then X is *flag-transitive*. This means transitivity on the set of ordered pairs of adjacent vertices. For graphs without isolated vertices, flag-transitivity implies both vertex and edge-transitivity. Again, the converse is

false (cf. [Hol81, Cam83]). If, however, X has *odd degree*, then vertex and edge-transitivity imply flag-transitivity.

A graph X is *vertex-primitive* if $\mathrm{Aut}X$ is a primitive group. Vertex-primitivity by definition implies vertex-transitivity, but it does not imply edge-transitivity. (Take a cycle of prime length $p \geq 7$ and add all chords of length 2). For a graph X, let $X^{(t)}$ denote the graph obtained by joining a pair of vertices of X if their distance in X is t. If X is vertex-primitive and not empty then $X^{(t)}$ is connected for every $t \leq \mathrm{diam}(X)$. In particular, nonempty bipartite graphs X of order ≥ 3 are never vertex-primitive (since $X^{(2)}$ is disconnected).

A graph is *distance-transitive* if $\mathrm{Aut}(X)$ is transitive on the set of ordered pairs of vertices at distance t for every $t \leq \mathrm{diam}(X)$. Nice examples are the Platonic solids (Figure 1 in Chap. 1, Sec. 1), Heawood's, Petersen's, and Coxeter's graphs (Figures 4,8,9 in Chap. 1, Secs. 1 and 4).

Vertex-primitivity is a very severe restriction on the automorphism group, as seen by the following deep result previously known as the "Sims conjecture" [Sim67].

THEOREM 1.1. (CAMERON, PRAEGER, SAXL, SEITZ [CPSS83]) *There exists a function f such that if a vertex-primitive digraph has out-degree k then the vertex-stabilizer in the automorphism group has order $\leq f(k)$.*

This result immediately implies that there is only a finite number of vertex-primitive distance-transitive graphs of any fixed degree. However, this second statement remains valid even without the vertex-primitivity condition (see Section 5.2).

The automorphism group of a finite *tournament* T has *odd order,* since otherwise it would contain an involution (an element of order two), which would then illegally reverse at least one edge. This harmless looking observation implies, by the Feit-Thompson Theorem, that $\mathrm{Aut}(T)$ is *solvable,* a fact with far reaching consequences, including algorithmic ones (cf. the end of Sec. 6.6). Here we state an immediate corollary (cf. Chap. 12 for the definitions).

PROPOSITION 1.2. *Let T be a tournament with n vertices.* (a) *If T is vertex-transitive then n is odd.* (b) *If T is vertex-primitive then n is an odd prime power.*

PROOF: Part (a) is straightforward: the in- and out-degrees must be equal. As for part (b), let N be a minimal normal subgroup of $\mathrm{Aut}(T)$. Then N is transitive (since $\mathrm{Aut}(T)$ is primitive); it is abelian (since $\mathrm{Aut}(T)$ is solvable); and it is characteristically simple (i.e. the direct product of isomorphic simple groups) (since it is minimal). Therefore $N \cong \mathbb{Z}_p^k$ ($k \geq 1$, p prime). A transitive abelian group being regular, we conclude that $n = |N| = p^k$. (We note that T is a Cayley digraph of N.) □

While there is no hope to classify all flag-transitive graphs, a simple description of all edge-transitive tournaments exists. (For directed graphs, edge- and flag-transitivity mean the same.) Let $q = p^k$ be an odd prime power, $q \equiv -1 \pmod 4$. The *Paley tournament* $P(q)$ has the field $GF(q)$ for its vertex set; an edge goes from x to y ($x \neq y$) if $x - y$ is a square. The group of affine transformations $x \mapsto ax + b$ ($a, b \in GF(q), a \neq 0$ a square) acts transitively on the edges of $P(q)$.

THEOREM 1.3. (KANTOR [KAN69]) (a) *Every edge-transitive tournament with $n > 2$ vertices is Paley.* (b) $\mathrm{Aut}(P(q))$ *consists of the affine semilinear transformations* $x \mapsto ax^\alpha + b$ *where* $a, b \in GF(q)$, $a \neq 0$ *is a square, and* $\alpha : x \mapsto x^{p^j}$ $(0 \leq j \leq k-1)$ *is an automorphism of* $GF(q)$.

PROOF: Let T be edge-transitive. Since $n > 2$, T must be vertex primitive and therefore $n = p^k$, p an odd prime. The stabilizer of a vertex x acts transitively on the tournament induced by the $(n-1)/2$ out-neighbors of x; hence $n \equiv -1 \pmod 4$. Let N be a minimal normal subgroup of $G = \mathrm{Aut}(T)$; then, as before, N can be identified with the vertex set of T. Let $\tau : x \mapsto x^{-1}$ $(x \in N)$; then τ is an *antiautomorphism* of T (reverses every edge). Therefore G has index 2 in the doubly transitive group $H = \langle G, t\rangle$. All solvable doubly transitive groups have been determined by Huppert (cf. [Hup57]); apart from a finite number of exceptions of degrees $3^2, 5^2, 7^2, 11^2, 23^2, 3^4$, they all are subgroups of the group $\Gamma A_1(p^k)$ of semiaffine (affine semilinear) transformations of $GF(p^k)$. The exceptional cases are ruled out because k must be odd (since $n \equiv -1 \pmod 4$). This, in particular, proves part (b). $\mathrm{Aut}(P(p^k))$ is the unique subgroup of index 2 in $\Gamma A_1(p^k)$, hence $G \leq \mathrm{Aut}(P(p^k))$. Since both G and $\mathrm{Aut}(P(p^k))$ have rank 3 (cf. Chap. 12), either T or its converse agrees with $P(p^k)$, which is self-converse. □

The r^{th} *residue digraph* $P(q, r)$ is defined for prime powers q and integers $r \geq 2$ such that $r|(q-1)$. The vertex set of $P(q, r)$ is $GF(q)$; an edge joins x to y if $x - y$ is a r^{th} power in $GF(q)$. This digraph is undirected if either q or $(q-1)/r$ is even. (The *Paley graphs* are the quadratic residue graphs ($r = 2$; $q \equiv 1 \pmod 4$). The *Clebsch graph* is $P(16, 3)$.) The affine linear group $A_1(q)$ is flag-transitive on $P(q, r)$. It is not true in general that $\mathrm{Aut}(P(q, r))$ is semiaffine; e.g. if $q = q_0^2$ and $r = q_0 + 1$ then $P(q, r)$ is a disjoint union of cliques; if $q = q_0^4$ and $r = q_0 + 1$, then the neighbors of 0 form a quadric and the graph admits the orthogonal group. However, the Paley graphs have semiaffine automorphism groups. This is a consequence of the following theorem of Carlitz [Car60] and McConnel [McC63] : *Let q be a prime power, $r|q-1$, and let f be a map of $GF(q)$ to itself such that for every $x, y \in GF(q)$, $x \neq y$, the element $(x-y)^{-1}(f(x) - f(y))$ is an r^{th} power. Then f is semiaffine.* (See also [BL73b].)

A stronger result holds when q is a prime.

THEOREM 1.4. *If X is an edge-transitive regular graph of prime order without isolated vertices then X is either complete or an r^{th} residue graph for some $r|(p-1)/2$. In the latter case,* $\mathrm{Aut}(X) = A_1(q)$.

PROOF: X cannot be bipartite (p is odd), hence it is vertex-transitive and (being a Cayley graph of the abelian group $\mathbb{Z}_p$, cf. Cor. 3.6), in fact, flag-transitive. Let $G = \mathrm{Aut}(X) \leq S_p$. If G is not solvable, then it is doubly transitive (cf. [Bur11]; cf. also [Hup67, p.609]), hence X is complete. If G is solvable then $G \leq A_1(p)$ (Galois; see Huppert[Hup67, p.163]). A glance at the structure of $A_1(p)$ completes the proof. □

Graphs with higher degrees of symmetry will be discussed in Section 5. *Distance-transitive* graphs have been defined above. We define another important class here.

An s-arc in a graph is a sequence $(x_0, \ldots, x_s)$ of vertices such that: (a) x_{i-1} and x_i are adjacent; (b) $x_{i-1} \neq x_{i+1}$. — The graph X is *s-arc-transitive,* if $\mathrm{Aut}(X)$ acts transitively on the set of s-arcs. (Note: 1-arc-transitivity is the same as flag-transitivity.) Distance-transitivity implies $\lfloor g/2 \rfloor$-arc-transitivity, where g is the *girth.*

Often we are interested in the action of some subgroup $G \leq \mathrm{Aut}(X)$ on vertices, edges, flags, etc. If this action is transitive (regular), we say that G is vertex-transitive (vertex-regular, resp.), etc., on X.

Graphs with relatively low degrees of symmetry are easy to construct. Every Cayley graph (see Section 2) is vertex transitive. There is an abundance of edge-transitive digraphs and even of 2-arc-transitive graphs, as indicated by the following result. A map $f : (V, E) \to (W, F)$ between two finite digraphs is a k-fold *covering* if f is a homomorphism (maps vertices to vertices, edges to edges, and preserves incidences); every vertex and edge of (W, F) has exactly k preimages; and f is a local isomorphism, i.e. x and $f(x)$ have the same indegree (out-degree, resp.) for every $x \in V$.

THEOREM 1.5. ([BAB85]) (a) *Every finite regular digraph has infinitely many edge-transitive finite covering digraphs with the same number of connected components.* (b) *Every finite regular graph has infinitely many 2-arc-transitive finite covering graphs with the same number of connected components.*

It follows by a result of Godsil [God82] that *the minimal polynomial of every digraph divides that of an edge-transitive digraph,* hence the adjacency matrices of infinitely many edge-transitive digraphs are not diagonalizable.

Although graphs with higher symmetry are much more difficult to construct (cf. Sec. 4), covering graphs are helpful in moving from an isolated example to infinitely many.

THEOREM 1.6. ([BIG74, CH. 19]) *A finite connected s-arc-transitive graph has infinitely many finite connected s-arc-transitive covering graphs.*

1.2 Reconstruction from line graphs

We illustrate the point made in the last sentence of the introduction by a classical example.

THEOREM 1.7. (WHITNEY [WHI32]) *Connected graphs X with ≥ 5 vertices are strongly reconstructible from their line graphs $L(X)$ (within the class of all graphs).*

(Whitney proved the result for finite graphs; it was extended to infinite graphs by Bednarek [Bed85], using Rado's selection principle (Chap. 42, Sec. 3).) In other words, every isomorphism $L(X) \to L(Y)$ is induced in the natural way by a unique isomorphism $X \to Y$ (cf. Lovász [Lov79a, p.507]). This, in particular, means that if the connected graph X has at least 5 vertices then $\mathrm{Aut}(X) \cong \mathrm{Aut}(L(X))$.

COROLLARY 1.8. *Let P denote the Petersen graph.* (a) $\mathrm{Aut}(P) \cong S_5$. (b) *$P$ is distance transitive and 3-arc-transitive.*

PROOF: The complement of P is $L(K_5)$. □

One can generalize this result to the *Kneser graphs* $KG(n,r)$ ($n \geq 2r+1$). Recall that the vertex set of $KG(n,r)$ is the set of r-subsets of an n-set; disjoint subsets correspond to adjacent vertices.

PROPOSITION 1.9. (a) *For $n \geq 2r+1$, $\mathrm{Aut}(KG(n,r)) \cong S_n$.*
(b) *$KG(n,r)$ is distance-transitive.*
(c) *The "odd graph" $O_k = KG(2k-1, k-1)$ is exactly 3-arc-transitive.*

For the proof of part (a), we have to consider a reconstruction problem for hypergraphs. The line graph $L(H)$ of the hypergraph $H = (V,E)$ has vertex set E; two members of E are adjacent in $L(H)$ if they intersect. — For a set A, let $[A]^r$ denote the complete r-uniform hypergraph on A, consisting of all r-subsets of A. The Kneser graph $KG(n,r)$ is the complement of $L([A]^r)$ where $|A| = n$. Part (a) of Proposition 1.9 is thus an immediate consequence of the next observation.

PROPOSITION 1.10. (BERGE, FOURNIER [BER72, FOU74]) *The complete r-uniform hypergraphs with $\geq 2r+1$ vertices are strongly reconstructible from their line graphs.*

PROOF: By the Erdős-Ko-Rado Theorem (see Chap. 24), the largest cliques of $L([A]^r)$ are in one-to-one correspondence with the elements of A. This guarantees that every isomorphism $L([A]^r) \to L([B]^r)$ is induced by a bijection $A \to B$. □

This is a special case of the following sufficient condition of reconstructibility.

THEOREM 1.11. (P.L. ERDŐS, Z. FÜREDI [EF80]) *Let H be an r-uniform hypergraph on n vertices. If $n \geq 2r+1$ and every vertex of H has degree greater than*

$$v(n,r) = \binom{n-1}{r-1} - \binom{n-r-1}{r-1} + 1,$$

then H is strongly reconstructible from $L(H)$.

The degree bound $v(n,r)$ is tight for every $r \geq 2$ and $n > 2r^2$. The quantity $v(n,r)$ comes from the Hilton–Milner theorem (Chap. 24, Theorem 5.8). In the particular case when all pairs of edges intersect in at most one point, the bound of Theorem 1.11 can be greatly improved.

THEOREM 1.12. *Let H be an r-uniform hypergraph on n vertices such that every pair of edges intersects in at most one point. If every vertex of H has degree greater than $r^2 - r + 1$, then H is strongly reconstructible from $L(H)$.*

The proof follows immediately from DEZA's Theorem [Dez73] (cf. [Lov79a, Probl. 13.17]): If every pair of edges of an r-uniform hypergraph $H = (V,E)$ has exactly λ points in common then either H is a sunflower (all edges have the same λ points in common), or $|E| \leq r^2 - r + 1$.

COROLLARY 1.13. *Let S, S_1 and S_2 be Steiner triple systems of order ≥ 15. Then:* (a) $\mathrm{Aut}(L(S)) \cong \mathrm{Aut}(S)$. (b) *If $S_1 \ncong S_2$ then $L(S_1) \ncong L(S_2)$.*

We shall use part (a) of this corollary to construct strongly regular graphs with arbitrary prescribed automorphism groups (Theorem 4.3). Part (b) implies the existence of a large number of *isospectral graphs*: nonisomorphic graphs with the same characteristic polynomial. The existence of such families shows that the characteristic polynomial, though a useful invariant of graphs, is far from complete. (A *complete* invariant $F(X)$ is one from which X is (weakly) reconstructible.)

COROLLARY 1.14. *For infinitely many values of n, there exists a set of $n^{\frac{1}{2}n(1+o(1))}$ isospectral graphs on n vertices.*

Indeed, the parameters of the strongly regular graph $L(S)$ (Chap. 15) and therefore its spectrum are uniquely determined by the number of vertices $n = v(v-1)/6$, where v is the number of vertices of the Steiner triple system S. The estimate of the number of Steiner triple systems required, $v^{\frac{1}{6}v^2(1+o(1))}$, is due to Alekseiev [Ale74] and R.M. Wilson [Wil74], combined with van der Waerden's Permanent Conjecture (now the theorem of Egorychev and Falikman (see Chap. 22, Sec. 16.1).

A more direct proof of Corollary 1.14 (also based on the Permanent Conjecture) uses Latin Square graphs (LSG's). The LSG associated with a $k \times k$ Latin square (LS) (Chap. 14) has k^2 vertices corresponding to the cells of the Latin square; two cells are adjacent in the graph if they are in the same row, or in the same column, or they have the same entry. For $k \geq 5$, the only k-cliques in an LSG are those corresponding to rows, columns, and identical entries. From this it is easy to deduce that (for $k \geq 5$) the LS is strongly reconstructible from its LSG. (Isomorphisms of Latin squares have to be defined carefully: row indices, column indices, and entries play interchangeable roles; so the automorphism group is a subgroup of $S_k \wr S_3$.)

1.3 Automorphism groups: reduction to 3-connected graphs

Probably the first nontrivial class of graphs of which the automorphism groups have been studied are finite trees (Jordan, 1869). The first observation is that every tree has a *center*, which is either a vertex or an edge and is fixed under every automorphism. This reduces the problem to rooted trees (the root is fixed by definition). Automorphism groups of rooted trees can be determined recursively: delete the root, designate its neighbors to be roots of the remaining branches, and apply formula (1) to the forest of rooted trees obtained. The conclusion:

PROPOSITION 1.15. (JORDAN, 1869) *The finite group G is isomorphic to the automorphism group of a finite tree if and only if $G \in \mathcal{W}$, where the class $\mathcal{W}$ of finite groups is defined inductively as follows:* (a) $\{1\} \in \mathcal{W}$; (b) *if $G, H \in \mathcal{W}$ then $G \times H \in \mathcal{W}$;* (c) *if $G \in \mathcal{W}$ and $m \geq 2$ then $G \wr S_m \in \mathcal{W}$.*

In fact, not only the abstract group structure but the permutation action of the automorphism groups of trees can be deduced from these considerations. The action defined by the result occurs on the leaves of the tree.

Using the block-cutpoint tree T of a 1-connected graph X, similar considerations reduce the determination of $\mathrm{Aut}(X)$ to the automorphism groups of its blocks via a slight generalization of wreath products. If the root of T is a cutpoint, we split it and combine, via eqn. 1, the groups of the (rooted) components. If the root is a block, we assign colors to the vertices of that block to indicate the isomorphism type of the incident branch; apply an arbitrary color preserving automorphism to the block, and move the branches in a wreath-product-like fashion (Robinson [Rob70]).

A canonical decomposition of 2-connected graphs to their 3-connected "components" also exists.

We briefly indicate the idea. Let us call a multigraph *basic* if it is either 3-connected or a cycle or it has just two vertices and a set of ≥ 2 parallel edges between them. A "bipolar multigraph" is a multigraph with two distinct specified endpoints. A bipolar multigraph is basic if it becomes a basic multigraph after adding a new edge joining the two endpoints.

Let us now take a basic graph, and repeat the following construction: simultaneously replace every edge by a basic bipolar multigraph.

The result is that every 2-connected graph arises in a canonical way in this manner. Canonicity means that all isomorphisms between two 2-connected graphs induce isomorphisms of each corresponding level of this construction (and in particular it induces an isomorphism of the rooted trees representing the hierarchy of the basic graphs used).

Such a canonical hierarchy of basic graphs is referred to as the decomposition to 3-connected components.

A generalization of wreath products [Bab75] allows a description of the automorphism group of a 2-connected graph in terms of the automorphism groups of its 3-connected components with the edges of these components colored and oriented appropriately.

A very efficient (linear time) algorithm for the canonical decomposition to 3-connected components was given by Hopcroft and Tarjan using breadth-first search [HT73]; a parallelizable algorithm was found by Miller and Ramachandran [MR92].

Problems of great depth arise in the study of the automorphism groups of infinite trees. Tits [Tit70]) studied the full automorphism groups of (vertex-colored) trees. Groups acting on trees without inverting an edge have been characterized by H. Bass and J.-P. Serre. This theory will be touched upon in Sections 3.7 and 3.11.

1.4 Automorphism groups of planar graphs

Finite planar graphs form one of the few comparatively rich classes of graphs of which the automorphism groups have been satisfactorily determined, both from the algebraic (Babai [Bab75]) and the algorithmic (Hopcroft, Tarjan [HT72]; Hopcroft, Wong [HW74]) points of view.

Every finite group of isometries of the Euclidean 3-space has a fixed point and can therefore be identified with a group of isometries of the 2-sphere. Every sense-preserving transformation is a *rotation,* and every sense-reversing transformation is a *rotary inversion*,

i.e. a rotation followed by a central inversion.

There are two infinite families and 3 sporadic examples of finite *rotation groups* of the 2-sphere: the rotation groups of the regular k-gonal pyramids (the cyclic group $\mathbb{Z}_k$), the regular k-gonal prisms (the dihedral group D_k), the tetrahedron (the alternating group A_4), the cube (S_4), and the dodecahedron (A_5) (see the Figures in Chap. 1, Sec. 1). The list is understood to include the degenerate cases $k \leq 2$.

The finite *isometry groups* of the 2-sphere, other than the rotation groups, can be obtained in one of two ways as follows. Each rotation group G can be extended to $G \cup G\tau \cong G \times \mathbb{Z}_2$ where $\tau = -I$ is the central inversion. Moreover, if G is a rotation group with a subgroup H of index 2, then the group $G^* = H \cup (G \setminus H)\tau$ is another isometry group. Note that $G^* \cong G$, but the geometric realization is different: for instance, from the rotation group of the cube we obtain the full isometry group of the tetrahedron. (See e.g. Fejes-Tóth [FT65], Coxeter [Cox61].)

THEOREM 1.16. *Every 3-connected planar graph X has an embedding on the sphere such that all automorphisms are realized by isometries of the sphere.*

This is a consequence of Whitney's theorem [Whi32] that 3-connected planar graphs are uniquely embeddable on the 2-sphere (cf. Chapter 2), combined with the fact that all finite homeomorphism groups of the 2-sphere are topologically equivalent to a group of isometries (Kerékjártó [Ker21]; Eilenberg [Eil34]). A stronger version of Theorem 1.16 was obtained by P. Mani:

THEOREM 1.17. (MANI [MAN71]) *Every 3-connected planar graph X can be realized as the 1-skeleton of a convex polytope P in $\mathbb{R}^3$ such that all automorphisms of X are induced by isometries of P.*

Polyhedral groups are the isometry groups of convex polytopes and their subgroups. Viewed in their action on $\mathbb{R}^3$, they coincide with the finite isometry groups listed above. Either of the above results, combined with the reduction process indicated in the previous section, yields a description of the automorphism groups of planar graphs in terms of generalized wreath products of symmetric groups and polyhedral groups. Two easily stated consequences: If X is planar then $\mathrm{Aut}X$ has a subnormal chain $\mathrm{Aut}(X) = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = 1$ such that each quotient group G_{i-1}/G_i is either cyclic or symmetric or A_5. If X is 2-connected and $|\mathrm{Aut}(X)|$ is odd then $\mathrm{Aut}(X)$ is cyclic (Babai [Bab75]). We conjecture that the first of these statements remains valid for graphs embeddable on an arbitrary fixed surface Σ (cf. Chap. 5) with A_5 replaced by a finite list, depending on Σ (cf. Babai [Bab73, Bab74a]).

1.5 Matrix representation. Eigenvalue multiplicity

A mechanical system is often represented by a self-adjoint operator A; and its symmetries by a group G of unitary operators (acting on a real or complex Hilbert space H). The fact of symmetry is expressed by the equation $AP = PA$ for each $P \in G$. If H has finite dimension (or more generally, its spectrum is discrete), then it is the orthogonal direct sum of the eigensubspaces $H_\lambda = \{u \in H : Au = \lambda u\}$ for all eigenvalues λ of A.

If the operators B and C commute, then the eigensubspaces of B are invariant subspaces for C. In particular, one can refine the decomposition $H = \sum^{\oplus} H_\lambda$ to an orthogonal decomposition into subspaces, irreducible under the action of G. This way each irreducible constituent of G falls into an eigensubspace, forcing "degeneracies" (multiple eigenvalues) to occur, and more importantly, the vectors in an orthonormal base of H are classified according to the irreducible constituents of G. This approach, introduced in a seminal 1927 paper of Eugene P. Wigner [Wig27] has since been used extensively both in classical and in quantum mechanics (cf. Wigner [Wig59], Hamermesh [Ham62]). The classification of eigenvibrations of molecules using the character tables of their symmetry groups (also due to Wigner, cf. Schonland [Sch65]) is particularly instructive because in this case $\dim H < \infty$ and the matrix A is a variant of the "adjacency matrix of the molecule".

Let now X denote a graph with edges weighted with real numbers; and let A be its adjacency matrix; so the entry $a_{i,j}$ is the weight of the edge $\{i, j\}$. Then A is a symmetric real matrix which acts on the space $H = \mathbb{R}^n$ (n is the number of vertices). The automorphisms of A are represented by precisely those permutation matrices P which commute with A.

Reversing Wigner's approach, we shall indicate how to use spectral information on A to infer properties of the group $G = \mathrm{Aut}(X)$. Let $\lambda_1, \ldots, \lambda_m$ be the eigenvalues of A; let m_i be the multiplicity of λ_i ($\sum m_i = n$). Let G_i denote the restriction of G to the eigensubspace H_{λ_i}. Then G is a subdirect product of the G_i. (A *subdirect product* is a subgroup of the direct product which projects *onto* each factor.) This proves part (a) of the following result.

THEOREM 1.18. *Let $G = \mathrm{Aut}(X)$ for an edge-weighted graph X with eigenvalue multiplicities $m_1 \leq \ldots \leq m_t$.* (a) [God78] *G is the subdirect product of groups $G_1, \ldots, G_t$, where G_i is a subgroup of the orthogonal group $O(m_i)$;* (b) [God78] *$|G_i| \leq n^{m_i}$;* (c) [God78] *if X is vertex-primitive then $|G| \leq n^{m_2}$;* (d) [BGM82] *if X is vertex-transitive then $|G| \leq n^{m_{t-1}}$; and more generally, the restriction of G to any of its orbits has order $\leq n^{m_{t-1}}$.*

To see part (b), let S be the projection of the trivial basis of $H = \mathbb{R}^n$ to H_{λ_i}; and let $S' \subseteq S$ be a base of H_{λ_i}. Then each member of G_i is determined by its restriction to S' which is a map $S' \to S$. The number of such maps is $\leq n^{m_i}$. Part (c) follows by observing that the projection of the V to each eigensubspace defines an invariant partition of V. Hence if X is vertex-primitive of degree $d \geq 1$ then this partition must be trivial and G acts faithfully on each eigensubspace of dimension $\neq 1$. But the only one-dimensional eigensubspace of a vertex-transitive graph is the one corresponding to $\lambda = d$. Part (d) is less immediate; an algorithmic version of it is used in [BGM82] to deduce an $n^{m+O(1)}$ algorithm for testing isomorphism of graphs with eigenvalue multiplicity bounded by m.

Part (a), too, has some appealing consequences. Let $m = m_t$ be the maximum multiplicity of eigenvalues. Noting that $O(1) \cong \mathbb{Z}_2$, we see that *if all eigenvalues of a graph are distinct, then its automorphism group is an elementary abelian 2-group* (Mowshowitz, Petersdorf–Sachs, 1969, cf. [CDS80]). Further, *if $m \leq 3$ then $\mathrm{Aut}(X)$ is solvable.* This is immediate for $m = 2$ since every finite subgroup of $O(2)$ is cyclic or dihedral; but among the finite subgroups of $O(3)$, there are two nonsolvable ones: the group of rotations of the

icosahedron ($\cong A_5$) and its full group of congruences ($\cong A_5 \times \mathbb{Z}_2$). These were ruled out by Cameron [Cam83] via a closer look at the characters of A_5. □

Our last remark concerns factors of the characteristic polynomial. Let $G \leq \mathrm{Aut}(X)$ for some weighted digraph X and consider the weighted quotient graph $Y = X/G$. The vertices of X/G are the orbits of G; the weight of the directed edge (A, B) of Y is the sum of weights of all edges (u, v) for some fixed $u \in A$ over all $v \in B$. It is easy to see that the characteristic polynomial of Y divides that of X. In particular, *if the characteristic polynomial of a digraph X is irreducible then X is asymmetric* ($|\mathrm{Aut}(X)| = 1$) (Mowshowitz, cf. [CDS80]).

1.6 Asymmetry, rigidity. Almost all graphs. Unlabelled counting

An excellent exposition of the subject of this section is given by Bollobás [Bol85, Ch. IX].

A graph is called *asymmetric* if it has no nontrivial automorphisms; it is called *rigid* if it has no nontrivial endomorphisms. (Some authors use the term "rigid" to describe what we call asymmetric.) Construction of asymmetric or rigid graphs and other structures with given properties is often the basis of the construction of such structures with given automorphism group or endomorphism monoid, resp. (Cf. Sec. 4.1.) A notable result in this area is that *there exists a rigid graph on every infinite vertex set* (Vopenka, Pultr, Hedrlin [VPH65], cf. [HL69]). Finite rigid graphs exist on n vertices for any $n \geq 10$ [HP65]; asymmetric graphs exist for $n \geq 6$. Asymmetry/rigidity is actually the typical behaviour of finite graphs. It was proved by Pólya [Pól37], Erdős and Rényi [ER63] that *a random graph is asymmetric* with probability $1 - \binom{n}{2}2^{-n-2}(1 + o(1))$. The dominant part of the error-term comes from the graphs which admit a transposition automorphism (a pair P of vertices with identical neighborhood outside P). The asymptotic expansion can be continued to include terms describing the probabilities of automorphisms with bounded supports. A strong algorithmic version of this result will be mentioned in Sec. 6.4.

It is not difficult to upgrade the proof to yield that almost all graphs are rigid. In this case the error term is $O(n^2(3/4)^{-n})$, dominated by the possiblity that the neigborhood of some vertex v includes the neighborhood of some vertex w, allowing an endomorphism $w \mapsto v$ while fixing all other vertices.

Although n-vertex asymmetric trees exists for every $n \geq 7$, random trees are typically not asymmetric. Indeed for any finite rooted tree T, almost all labeled trees have T as a limb (Schwenk [Sch73]). In particular, large numbers of cherries (pairs of pendant vertices with a common neighbor) occur almost always.

Nontrivial trees (and more generally, bipartite graphs, and indeed perfect graphs) are never rigid (they can be mapped to their largest clique).

E. M. Wright refined the "almost sure asymmetry" results to show that asymmetry is typical for graphs with density above the *connectedness threshold* (cf. Chap. 6):

THEOREM 1.19. (WRIGHT [WRI71]) *Let $m(n) = \frac{1}{2}n \ln n + n\psi(n)$. Then the probability that a random graph with n vertices and $m(n)$ edges is asymmetric tends to 1 if $\psi(n) \to \infty$ assuming $m(n) \leq \frac{1}{2}\binom{n}{2}$; and this probability tends to 0 if $\psi(n) \to -\infty$.*

The reason of the second statement is obvious: those graphs have, with probability approaching 1, an unbounded number of isolated vertices. If we rule out this possibility, even sparser graphs will be typically asymmetric: for fixed $r \geq 3$, the probability that a random r-regular graph is asymmetric tends to 1 (Bollobás [Bol82], McKay and Wormald [MW84], [Wor86]).

The results establishing "almost always asymmetry" mentioned above are valid for labeled as well as for unlabeled graphs; the latter is a substantially stronger statement with important consequences to counting unlabeled objects. We shall formalize the connection below.

Let $\mathcal{C}$ be a class of finite graphs (or digraphs, or other structures), closed under isomorphisms, and let $\mathcal{C}(n)$ be the set of those members of $\mathcal{C}$ with vertex set $[n] = \{1, \ldots, n\}$. Let $\mathcal{P}$ be a graph property (i.e. an isomorphism-closed class of graphs). We say that "almost all labeled members of $\mathcal{C}$ have property $\mathcal{P}$" if $\lim_{n\to\infty} |\mathcal{P} \cap \mathcal{C}(n)|/|\mathcal{C}(n)| = 1$. The term "almost all unlabeled members of $\mathcal{C}$" is used analogously except that isomorphism classes rather than individual graphs are counted. This annoying distinction disappears if almost all *unlabeled* members of $\mathcal{C}$ are asymmetric: under this condition, any graph property will hold for almost all unlabeled members of $\mathcal{C}$ if and only if it holds for almost all *labeled* members.

The statement that "almost all unlabeled members of $\mathcal{C}$ are asymmetric" is equivalent to the following:

$$\text{"the expected number of automorphisms of a random labeled member of } \mathcal{C} \text{ is } 1 + o(1)." \tag{2}$$

This equivalence follows from the observation that the *number of unlabeled graphs* (isomorphism classes) in $\mathcal{C}(n)$ is exactly $|\mathcal{C}(n)|\alpha(n)/n!$, where $\alpha(n) = \sum_{X\in\mathcal{C}(n)} |\mathrm{Aut}(X)|/|\mathcal{C}(n)|$ is the expected order of the automorphism group of a random labeled member of $\mathcal{C}$. (This follows from the Orbit Counting Lemma, a.k.a. "Burnside's Lemma", see Chap. 21, Lemma 14.3.)

By the results mentioned, (2) is valid for the class of all graphs, for graphs with $m(n)$ edges as in Wright's theorem ($\psi \to \infty$), as well as for regular graphs of given degree $r \geq 3$.

Structures satisfying stronger regularity constraints are often difficult to count. It seems likely, for instance, that almost all strongly regular graphs are asymmetric, but this may be difficult to prove. It has been shown, however, that almost all (unlabeled) members of the following two classes of strongly regular graphs are asymmetric: the line graphs of Steiner triple systems, and the Latin square graphs (cf. Sec. 4.1) [Cam], [Bab79a].

While almost all graphs are asymmetric, one might be interested in what can be said about the graphs known to admit some automorphisms. Related questions will be considered in Sections 4.3 and 4.4; here we mention a result of P. J. Cameron [Cam80b].

THEOREM 1.20. (CAMERON) *For a finite group G let $\mathcal{C}(G)$ be the class of those graphs X admitting a group isomorphic to G as a subgroup of* $\mathrm{Aut}(X)$. *Let $a_n(G)$ denote the proportion of those n-vertex labeled members of $\mathcal{C}$ which have* $\mathrm{Aut}(X) \cong G$. *Then* (i) *the limit $a(G) := \lim_{n\to\infty} a_n(G)$ always exists and is rational;* (ii) *$a(G) = 1$ iff G is the direct product of symmetric groups;* (iii) *for infinitely many groups, including all abelian groups*

with exponent ≥ 3, $a(G) = 0$; (iv) *For metabelian groups, the values of* $a(G)$ *are dense in* $[0, 1]$.

While almost all finite graphs are asymmetric, the situation changes to its opposite when we consider countably infinite graphs. Let us generate a random graph on a countably infinite vertex set by deciding independently and with probability 1/2 whether or not to join two vertices. Then with probability 1, we obtain a graph isomorphic to one specific graph, R, the Rado graph [ER63], discussed in Sec. 5.3. We should mention that $|\mathrm{Aut}(R)| = 2^{\aleph_0}$, and "almost all" automorphisms of R are conjugates (cf. Theorem 3.17).

More generally, *the number of automorphisms of a countable graph* (or any countable structure over a locally finite language, cf. Sec. 5.3) *is always finite, countable, or* $2^{\aleph_0}$. A countable graph (structure) X has $2^{\aleph_0}$ automorphisms if and only if every finite subset of $V(X)$ is pointwise fixed by some nontrivial automorphism.

2 Graph products

In this section we introduce the most important graph products, indicate their combinatorial significance, and address their automorphism and factoring problems.

Given two graphs $X_i = (V_i, E_i)$ $(i = 1, 2)$, a *product graph* $Y = (W, F) = X_1 * X_2$ can be defined in a variety of sensible ways. Those four which appear most frequently in the literature are the lexicographic, the Cartesian, the categorical, and the strong products. In each case, $W = V_1 \times V_2$ (Cartesian product). Each of the products is associative, and three of the four are commutative in the sense that the map $(v_1, v_2) \mapsto (v_2, v_1)$ is an isomorphism between $X_1 * X_2$ and $X_2 * X_1$. (The lexicographic product is not commutative.) The 1-vertex graph is a (two-sided) identity in three cases (exception: the categorical product; in that case it is natural to admit loops and the one-vertex graph with a loop becomes the identity). We say that a graph P is a *prime* with respect to a product and a class $\mathcal{C}$ of graphs if P is not isomorphic to the product of two non-identity graphs within $\mathcal{C}$ and is not itself the identity.

Next we define the adjacency relation in each product. Let $u_i, v_i \in V_i$ and $(i = 1, 2)$ $w = (u_1, u_2)$, $z = (v_1, v_2) \in W$. Then w and z are adjacent (a) in the *lexicographic product* $Y = X_1[X_2]$ if either $(u_1, v_1) \in E_1$ and $u_2 \neq v_2$, or $u_1 = v_1$ and $(u_2, v_2) \in E_2$; (b) in the *Cartesian product* $Y = X_1 \times X_2$ if either $u_1 = v_1$ and $(u_2, v_2) \in E_2$ or $u_2 = v_2$ and $(u_1, v_1) \in E_1$; (c) in the *categorical product* $Y = X_1 \cdot X_2$ if $(u_1, v_1) \in E_1$ and $(u_2, v_2) \in E_2$; (d) the edge set of the *strong product* $X_1 \otimes X_2$ is the union of the edge sets of the Cartesian and the categorical products.

Observe that the n-cube is the Cartesian product of n copies of K_2; more generally, Cartesian products of paths are grids. *Hamming graphs* can be defined as isometric subgraphs of Cartesian products of complete graphs (cf. Graham and Winkler [GW85]).

Categorical products are the products in the category theoretic sense. They give rise to some of the deepest structural questions (cf. [McK71], [Jón81]). Strong products, their close relatives, are tamer in many ways.

Lexicographic products occur naturally in combinatorial constructions; we shall mention examples below.

Some graph invariants of certain products are easily computed from those of the factors; others pose important open questions. We mention two of the latter kind. The first one concerns the *chromatic number* $\mathrm{chr}(Y)$ *of the categorical product* $Y = X_1 \cdot X_2$. Since Y has a homomorphism to each factor, clearly $\mathrm{chr}(Y) \leq \min\{\mathrm{chr}(X_1), \mathrm{chr}(X_2)\}$. HEDETNIEMI's conjecture asserts that for finite graphs we have equality here (cf. [GL74]). (This is false for uncountably infinite graphs [Haj85].)

The second problem concerns the *independence number* $\alpha(Y)$ *of the strong product* $Y = X_1 \otimes X_2$. Clearly $\alpha(Y) \geq \alpha(X_1)\alpha(X_2)$ (supermultiplicativity). Let $X^k = X \otimes \ldots \otimes X$ denote the k^{th} strong power of the graph X. Supermultiplicativity implies that the limit $\Theta(X) = \lim_{k\to\infty}(\alpha(X^k))^{1/k}$ always exists; this quantity is the *Shannon capacity* of X (Chap. 31, Sec. 6; cf. [Knu94]). Its value is unknown even for as simple a graph as C_7, the cycle of length 7. Even the case of C_5 was open for decades; it was solved by Lovász as a special case of the following result: *If X is a vertex-transitive self-complementary graph with n vertices then $\Theta(X) = \sqrt{n}$* [Lov79b]. (This class includes the Paley graphs (Sec. 1.1).)

Cartesian products of cycles occur as Cayley graphs of abelian groups. Their genus has been studied in this context (cf. Sec. 3.9).

Some useful observations regarding the *lexicographic product:* (1) both the *independence number* $\alpha(X)$ and the *clique number* $\omega(X)$ are multiplicative under lexicographic products (this fact has a curious application to constructive Ramsey graphs [Abb72]). The following inequality holds for the chromatic number of the lexicographic product (Linial and Vazirani) [LV89]:

$$(\mathrm{chr}(X_1) - 1) \cdot \mathrm{chr}(X_2)/\ln|V(X_1)| \leq \mathrm{chr}(X_1[X_2]) \leq \mathrm{chr}(X_1) \cdot \mathrm{chr}(X_2). \tag{3}$$

Sometimes the study of vertex-transitive graphs reduces to the study of Cayley graphs via the following observation: *If X is vertex-transitive then both $X[K_m]$ and $X[\overline{K}_m]$ are Cayley graphs for a suitable m* [Sab64]. (Examples include the study of isoperimetry, cf. Theorems 3.38, 3.41.

Among the nicely behaved parameters we mention the *spectrum.* Let $\{\lambda_i\}$ and $\{\mu_j\}$ be the multisets of eigenvalues of X_1 and X_2, resp. Then $\{\mu_j + |X_2|\lambda_i\}$, $\{\lambda_i + \mu_j\}$, $\{\lambda_i\mu_j\}$, and $\{\lambda_i\mu_j + \lambda_i + \mu_j\}$ are the respective multisets of eigenvalues of the lexicographic, Cartesian, categorical, and strong products. All these products share a base of orthonormal eigenvectors consisting of the pairwise Kronecker products of the orthonormal eigenbases of each factor. The Kronecker product of the adjacency matrices of X_1 and X_2 is the adjacency matrix of their categorical product.

2.1 Prime factorization, automorphism group

Now we turn to the problem of *unique prime factorization* (UPF). We recommend the insightful survey by W. Imrich [Imr93] for more detail.

For commutative products of finite graphs, UPF is equaivalent to the *common refinement property.* We say a graph G has the common refinement property with respect to a product, if for any two representations $\prod_{i\in I} A_i \cong \prod_{j\in J} B_j$ of G there exist graphs $C_{i,j}$ which satisfy $A_p \cong \prod_{j\in J} C_{p,j}$ and $B_q \cong \prod_{i\in I} C_{i,q}$.

Let $V = V_1 \times \cdots \times V_k$ be a Cartesian product decomposition of the vertex set V. For $v \in V$, let V_i^v denote the set of vertices differing from v in the ith coordinate only. Suppose this decomposition of V corresponds to a decomposition of the graph $X = (V, E)$ with respect to some commutative product; and $V = W_1 \times \cdots \times W_\ell$ corresponds to another decomposition. We say that the *strict common refinement property* (s. c. r.) holds if the intersections $V_i^v \cap W_j^v$ with at least two vertices are exactly the $C_{i,j}^v$ with respect to the factors of a common refinement. We say that X has the s. c. r. property w .r. to a certain product if any pair of product decompositions of X has this property. In this case it follows that the multiset of prime factors is *strongly reconstructible*. In particular, X has UPF $X = \prod X_i$ and $\mathrm{Aut}(X)$ is obtained from $\mathrm{Aut}(X_i)$ via equation (1) at the beginning of Section 1.

For disconnected graphs, UPF does not hold for any of our commutative products, as seen from the identity $(1 + x + x^2)(1 + x^3) = (1 + x^2 + x^4)(1 + x)$. (Plug in a connected prime graph for x and interpret $+$ as disjoint union.)

2.2 The Cartesian product

The product of connected graphs is connected.

Every connected graph has UPF in a strong sense (Sabidussi [Sab60]) which we now state. Every Cartesian product decomposition $X = Y_1 \times \cdots \times Y_k$ of the graph X induces an equivalence relation $\sigma(Y_1, \ldots, Y_k)$ on $E(G)$; eqivalent edges correspond to edges of the same Y_i. It turns out that if X is connected then the intersection of two such *product relations* is a product relation again. The UPF corresponds to the intersection σ_X of all product relations. The strict common refinement property for connected graphs follows immediately, implying UPF and eqn. (1) for the prime factors.

Several algorithms are known to construct the UPF. The simplest one is due to Feder [Fed92] and runs in $O(mn)$ ($m = |E|$, $n = |V|$). The most efficient algorithm, found by Aurenhammer, Hagauer and Imrich [AHI92], runs in $O(m \log n)$.

Unique prime factorization holds for infinite graphs as well, and extends to the *weak* Cartesian product of infinitely many connected graphs (Imrich). For this result and for the connections between prime factorization and *isometric embeddings* into Cartesian products we refer to Imrich [Imr89].

2.3 The categorical product; cancellation laws

First of all we have to admit loops so we at least have an identity graph for this product (single vertex with a loop). The categorical product of two connected graphs is bipartite iff at least one of them is bipartite; and it is disconnected iff both factors are bipartite. Disconnected products cause non-unique prime factorizations; however, the connected non-bipartite graphs have UPF in the class of graphs with loops [McK71]. However, the strict refinement property does not hold, not even its consequence, eqn. (1).

A graph is *thin* if no pair of vertices has precisely the same set of neighbors. All factors of connected, non-bipartite thin graphs have the same properties. *The strict common refinement property holds for connected, non-bipartite thin graphs*, with its usual consequences: UPF and eqn. (1) for prime decomposition [McK71].

The inference $A \cdot C \cong B \cdot C \Rightarrow A \cong B$ is called *cancellation*. The cancellation law is an immediate consequence of UPF; however, it may hold even if UPF fails. Lovász proved [Lov71] that for cancellation, it suffices to require that the graphs A and B both have a homomorphism to C. Moreover $A^n \cong B^n$ always implies $A \cong B$. In fact, Lovász [Lov72a] has shown, using an elegant inclusion-exclusion argument, that these statements hold *in any finite category*.

2.4 Strong product

For a simple graph X, let X_0 be the graph obtained by attaching a loop at each vertex. Let Y^0 be obtained by removing all loops from Y. Now for two simple graphs X, Y, we have $X \otimes Y = (X_0 \cdot Y_0)^0$. Thus the strong product can be viewed as a tame special case of the categorical product (imagine a loop at every vertex). It follows that for connected simple graphs, UPF holds. Moreover, the *strict common refinement property* holds for connected graphs with *thin complements*.

The UPF of connected graphs can be found in polynomial time (Feigenbaum, Schäffer [FS92]).

2.5 Lexicographic product

This product is *right-distributive* with respect to disjoint unions (all other products discussed are distributive). It distributes complementation: $\overline{X[Y]} \cong \overline{X}[\overline{Y}]$. The only pairs of graphs which *commute* with respect to the lexicographic product are (K_n, K_m), $(\overline{K}_n, \overline{K}_m)$, and X^n, X^m for any X. Moreover the following *cancellation law* holds for finite graphs: if $A[B] \cong X[Y]$ and $|V(B)| = |V(Y)|$ then $A \cong X$ and $B \cong Y$.

Let $X + Y$ denote the disjoint union of the graphs X, Y and set $X \oplus Y = \overline{\overline{X} + \overline{Y}}$ (Zykov sum).

Observe that $\overline{K}_q[X[\overline{K}_q] + \overline{K}_m] \cong (\overline{K}_q[X] + \overline{K}_m)[\overline{K}_q]$, and, by complementation, $K_q[X[K_q] \oplus K_m] \cong (K_q[X] + K_m)[K_q]$. We call these operations *elementary transpositions*. They preserve primality.

THEOREM 2.1. (CHANG [CHA61], IMRICH [IMR71]) *Any two prime factorizations with respect to the lexicographic product can be transformed into each other by elementary transpositions.*

For further references, cf. [Jón81].

Clearly, $\mathrm{Aut}(X[Y]) \leq \mathrm{Aut}(Y) \wr \mathrm{Aut}(X)$ (wreath product in its imprimitive action, cf. Chap. 12): we may apply an automorphism of each copy of Y separately; and then, apply a single automorphism of X. We state a sufficient condition which guarantees equality here.

THEOREM 2.2. (SABIDUSSI) *Let X, Y be finite graphs. Assume X is thin if Y is disconnected and $\overline{X}$ is thin if $\overline{Y}$ is disconnected. Then* $\mathrm{Aut}(X[Y]) = \mathrm{Aut}(Y) \wr \mathrm{Aut}(X)$.

Feigenbaum and Schäffer [FS92] observed that recognizing composite graphs is polynomial-time equivalent to the graph isomorphism problem (Sec. 6) and therefore not known to be solvable in polynomial time.

3 Cayley graphs and vertex-transitive graphs

3.1 Definition, symmetry

In 1878, Cayley introduced a graphic representation of abstract groups. With a group G and a set $S \subseteq G$ of generators he associated what we now call a *Cayley color diagram:* a directed graph with colored edges. The vertex set of the diagram $\Gamma_c(G,S)$ is G. One color corresponds to each member of S; and the vertex $g \in G$ is joined to $sg \in G$ by an edge of color s.

If we ignore colors, we obtain the *Cayley digraph* $\vec{\Gamma}(G,S)$. If in addition we ignore orientation of the edges, we obtain a simple graph: the *Cayley graph* $\Gamma(G,S)$. The degree of its vertices is $|S \cup S^{-1} \setminus \{1\}|$.

The Cayley graph $\Gamma(G,S)$ is connected because S generates G. Cycles in the Cayley graph correspond to relations among the elements of S. In particular, if S is a set of free generators of a free group G then $\Gamma(G,S)$ is a tree. The converse also holds if there are no involutions (elements of order 2) in S. (Involutions correspond to cycles of length 2 in the Cayley diagram, invisible in the Cayley graph.) More generally, if $\Gamma(G,S)$ is a tree then G is a free product of infinite cyclic groups and of cyclic groups of order 2; the members of S generate these free factors.

If no proper subset of S generates G, we call $\Gamma(G,S)$ a *minimal Cayley graph.* Infinite groups do not normally have minimal sets of generators. If S can be linearly ordered such that no element of S is generated by its predecessors, we call $\Gamma(G,S)$ *semiminimal.* Every group possesses semiminimal Cayley graphs.

For $g \in G$, the *right translation* $\rho_g : G \to G$ is defined by $x\rho_g = xg$ $(x \in G)$. The map $\rho : g \mapsto \rho_g \in \mathrm{Sym}(G)$ is the *right regular permutation representation* of G. Its image $G\rho \leq \mathrm{Sym}(G)$ is a regular permutation group (Chap. 12). The following statements regarding the automorphism groups of Cayley diagrams and graphs are easy to verify. (Recall that automorphisms of colored directed graphs preserve colors and orientation by definition.)

Proposition 3.1. (a) $G\rho = \mathrm{Aut}(\Gamma_c(G,S)) \leq \mathrm{Aut}(\Gamma(G,S))$. (b) (Sabidussi [Sab64]) *A graph $X = (G,E)$ is a Cayley graph of the group G if and only if $G\rho \leq \mathrm{Aut}(X)$.*

Cayley graphs are thus vertex-transitive; the converse of this statement is false. Indeed, by 3.1(b), a graph X is Cayley precisely if $\mathrm{Aut}(X)$ contains a regular subgroup. The smallest example of a vertex-transitive graph with no regular subgroup of automorphisms is Petersen's graph. This is the first member $KG_{2,1}$ of the infinite family of Kneser's graphs $KG_{n,k}$. $(n \geq 2, k \geq 1)$, most of which are not even remotely Cayley-like. $KG_{n,k}$ has $\binom{2n+k}{n}$ vertices identified with the set of n-tuples of a $(2n+k)$-set; two vertices are adjacent if the corresponding n-tuples are disjoint (cf. Chapters 4, 24, 34).

Theorem 3.2. ([Kan72],[God80a]) (a) *Kneser's graph $KG_{n,k}$ $(n \geq 2, r \geq 1)$ is a Cayley graph precisely if $n = 2$ and $2n+k$ is a prime power, $2n+k \equiv -1 \pmod 4$, or $n = 3$ and $2n+k \in \{8, 32\}$.*

(b) *If $n \geq 4$ then, with some exceptions, the only transitive proper subgroup of* $\mathrm{Aut}(KG_{n,k})$ *is the one induced by the alternating group A_{2n+k}. Exceptions occur for $n = 5$ when $2n + k \in \{12, 24\}$ and for $n = 4$ when $2n + k \in \{9, 11, 12, 23, 24, 33\}$.*

The proof requires the following result of Livingstone and Wagner. A permutation group $G \leq \mathrm{Sym}(A)$ is t-transitive if it is transitive on the set of ordered t-tuples of distinct elements of A. G is t-homogeneous if it is transitive on the set of t-subsets of A.

THEOREM 3.3. (LIVINGSTONE-WAGNER [LW65]) (a) *If G is t-homogeneous then it is $(t-1)$-transitive.* (b) *If G is t-homogeneous and $t \geq 5$ then G is t-transitive.*

PROOF: of Theorem 3.2. Assume that $KG_{n,k}$ is a Cayley graph of some group $G \leq \mathrm{Aut}(KG_{n,k})$. Then, by Proposition 1.2.3(a), we may view G as a subgroup of S_{2n+k}. Now, G acts regularly on the n-subsets, and is therefore n-homogeneous. By Theorem 3.3, it must be n-transitive if $n \geq 5$. Part (b) now follows because of the nonexistence of nontrivial 4- and 5-transitive permutation groups of degrees other than those listed.

For $n \geq 3$, part (a) follows by inspection of the list of doubly transitive permutation groups (see Chap. 12). (We remark that Kantor's original proof did not rely on the classification theorem.)

Finally, in the case $n = 2$, we observe that $G \leq \mathrm{Aut}(T)$ for some tournament T, and G acts as a regular group on the set of edges of T. It follows by Theorem 1.3 that T must be a Paley tournament, hence $2n + k$ is a prime power and $\equiv -1 \pmod 4$. To see that in this case $KG_{n,k}$ is indeed a Cayley graph, let G be the group of affine transformations $x \mapsto ax + b$, $a, b, x \in GF(2n + k)$, a a square in $GF(2n + k)$. □

As this example shows, it is often not easy to decide whether or not a given vertex-transitive graph is a Cayley graph. If the number of vertices is a prime power, the following partial information is useful.

THEOREM 3.4. (a) *If G is a transitive group of degree p^k, p prime, then the Sylow p-subgroups of G are transitive as well* [Wie64, p.6].

(b) (D. MARUŠIČ [MAR85]) *Every vertex-transitive (di)graph of order p^k, $k \leq 3$, is a Cayley (di)graph. Counterexamples exist for $k \geq 4$.*

Let $\mathcal{V}$ denote the set of those positive integers n for which there exists a connected vertex-transitive graph of order n which is not a Cayley graph. Considerable effort has gone into determining the set $\mathcal{V}$ (see the survey [Pra90]). It is clear that all multiples of a member of $\mathcal{V}$ also belong to $\mathcal{V}$ (the complement of the disjoint union of copies of a non-Cayley vertex-transitive graph is again non-Cayley). So we need to know the minimal members of $\mathcal{V}$ only (w. r. to divisibility). It is not known whether or not such minimal members can have an arbitrarily large number of distinct prime divisors. It is conjectured that almost all vertex-transitive graphs of order n are Cayley graphs.

Cayley graphs are not edge transitive in general. (The triangular prism is an example.) In fact, their automorphism group often coincides with their group of definition (see the GRR problem in Section 4.3). Here is a sufficient condition to guarantee added symmetry.

PROPOSITION 3.5. (FRUCHT [FRU52]) *If a group automorphism $\alpha \in \mathrm{Aut}(G)$ stabilizes the set $S \subseteq G$ then $\alpha \in \mathrm{Aut}(\Gamma(G,S))$.*

COROLLARY 3.6. (a) *If S is an orbit of some subgroup H of $\mathrm{Aut}(G)$ then $\Gamma(G,S)$ is edge-transitive.* (b) *If, in addition, $S = S^{-1}$, then $\Gamma(G,S)$ is flag-transitive.* (c) *An edge-transitive Cayley graph of an abelian group is flag-transitive.*

Note that the added condition in (b) is automatically satisfied if S consists of involutions (elements of order 2). Frucht [Fru52] employed this observation to construct a flag-regular graph of degree 3. Another application is the construction of 2-arc-transitive covering graphs (Theorem 1.5).

3.2 Symmetry and connectivity

The implications of vertex-transitivity to connectivity properties of graphs were discovered by Mader [Mad71a, Mad71b] and Watkins [Wat70]. Their methods and results were generalized to directed graphs by Hamidoune (cf. [Ham81]). We state the directed graph versions; undirected graphs are viewed as digraphs with edges oriented both ways. We note that a weakly connected finite vertex-transitive digraph is automatically *strongly connected* so we may omit the adjective. The *connectivity* $\kappa(X)$ of a strongly connected digraph $X \neq K_n$ is the minimum number of vertices whose deletion destroys strong connectivity. Edge-connectivity is defined similarly.

THEOREM 3.7. *Let X be a finite connected vertex-transitive digraph of out-degree d.*
(a) *The connectivity of X is $\geq \lceil (d+1)/2 \rceil$. If X is undirected then $\kappa(X) \geq \lceil 2(d+1)/3 \rceil$.*
(b) *The edge connectivity of X is d.*
(c) *If X is edge transitive or vertex-primitive, then $\kappa(X) = d$.*

The bounds in part (a) are tight, as shown by the lexicographic product of a (directed or undirected) cycle of length $m \geq 4$ and K_r.

All these results are simple consequences of the theory of atoms, developed by Mader, Watkins, and Hamidoune in the same papers (cf. Chapter 2, Sec. 7.5). A *positive fragment* of a strongly connected digraph X is a subset $F \subset V(X)$ such that the set $X^+(F)$ of out-neighbors of F has cardinality $\kappa(X)$ and $F \cup X^+(F) \neq V(X)$ (so $X^+(F)$ is a minimum cutset). An *positive atom* is a positive fragment of minimum cardinality.

The key result of Mader, Watkins, and Hamidoune is that *if A is a positive atom and F is a positive fragment then either $A \subseteq F$ or $A \cap F = \emptyset$.* (For a simple proof, see [Ham81, Thm.2.1].) In particular, the positive atoms are pairwise disjoint. Consequently, if X is vertex-transitive then the atoms form a system of imprimitivity. From this, the vertex-connectivity results readily follow. For the edge-connectivity result, edge-atoms are introduced and their disjointness proved. (Cf. also Lovász [Lov79a, Ch. 12] for these and related results.)

COROLLARY 3.8. (CAUCHY-DAVENPORT) *Let $\emptyset \neq A, B \subset \mathbb{Z}_p$ (p a prime). Then $|A + B| \geq \min\{p, |A| + |B| - 1\}$.*

PROOF: W.l.o.g., $0 \in B$. Apply part (c) of Theorem 3.7 to the vertex-primitive Cayley digraph $X = \Gamma(\mathbb{Z}_p, B \setminus \{0\})$. Conclude that if $A+B \neq \mathbb{Z}_p$ then $|X^+(A)| \geq \kappa(X) = |B|-1$. Observe, on the other hand, that $X^+(A) = (A+B) \setminus A$. □

For this result and other connections with additive number theory, see [Ham90].

Minimal Cayley graphs do even better than guaranteed by part (a) of Theorem 3.7: *If X is a minimal Cayley graph of degree d then $\kappa(X) = d$* (Godsil [God81a]).

Infinite connected vertex-transitive graphs of arbitrarily large degree may have connectivity as small as 1, as the example of the regular tree of any degree demonstrates. Yet, analogous results exist. Let $\kappa_f(X)$ denote the smallest size of a subset C of the vertex set of a locally finite infinite graph X such that at least one of the connected components of $X \setminus C$ is finite. *If X is connected, vertex-transitive, and it has finite degree d, then* $\kappa_f(X) \geq \lceil 3(d+1)/4 \rceil$ [BW80]. Analogously to the finite case, the proof rests on the disjointness of atoms (finite sets of vertices with κ_f neighbors). We note that if the graph X has just one *end* (cf. Sec. 3.7) then $\kappa(X) = \kappa_f(X)$.

3.3 Matchings, independent sets, long cycles

All graphs in this section are finite. The next question concerns **matchings.**

THEOREM 3.9. (LITTLE, GRANT, HOLTON [LGH75]) *Let X be a connected vertex-transitive graph on n vertices.* (a) *If n is even then X has a perfect matching.* (b) *If n is odd then X is matching critical.* (c) (LOVÁSZ, PLUMMER) *If n is even then X is either bicritical (deletion of any pair of vertices leaves a perfect matching) or elementary bipartite (deletion of any pair of vertices of opposite color leaves a perfect matching).*

PROOF: Let D be the set of those vertices of X which are left uncovered by at least one maximum matching. The Gallai-Edmonds structure theorem (see Chap 3, Sec. 4.3) asserts that if D is not empty then it consists of matching critical components. But if X does not have a perfect matching then, by vertex-transitivity, D is the entire vertex set. This proves (a) and (b). For (c), see [LP86, Theorem 5.5.24]). □

The following two observations on regular uniform hypergraphs come in handy in the analysis of various kinds of subsets of vertex-transitive graphs. (A hypergraph is *regular* of degree d if every vertex is contained in exactly d edges.)

LEMMA 3.10. (REGULAR HYPERGRAPH COUNTING LEMMA) *Let $\mathcal{E}$ and $\mathcal{F}$ be r-uniform and s-uniform regular hypergraphs, resp., on the same set of n vertices.*

(a) *Assume $|E_i \cap F_j| \geq d$ for every $E_i \in \mathcal{E}$, $F_j \in \mathcal{F}$. Then $rs \geq nd$.*

(b) *Assume $|E_i \cap F_j| \leq d$ for every $E_i \in \mathcal{E}$, $F_j \in \mathcal{F}$. Then $rs \leq nd$.*

If $\mathcal{E} = \mathcal{F}$ and $d \neq n$ then under condition (a) we have $r^2 > nd$. On the other hand, if $\mathcal{E} = \mathcal{F}$, $d \neq n$, and $|E_i \cap E_j| \leq d$ for every $E_i, E_j \in \mathcal{E}$, $i \neq j$, then $r^2 < 2nd$.

PROOF: (a) Fix $E_i \in \mathcal{E}$. Count the number of pairs (x, j) such that $x \in E_i \cap F_j$. The result is $r \deg_{\mathcal{F}} \geq d|\mathcal{F}| = dn \deg_{\mathcal{F}} /s$. (b) as well as the $\mathcal{E} = \mathcal{F}$ variants follow analogously. □

As a corollary, we have a tradeoff between $\alpha(X)$, the maximum size of independent sets, and $\omega(X)$, the maximum size of cliques of the graph X, for vertex-transitive graphs. For a generalization in the context of the Shannon capacity of graphs, see Lovász [Lov79b] (cf. Chap. 31, Sec. 6).

COROLLARY 3.11. (L. LOVÁSZ, R. M. WILSON) *If X is a vertex-transitive graph then $\alpha(X)\omega(X) \leq n$.*

PROOF: Indeed, let $\mathcal{E}$ and $\mathcal{F}$ be the hypergraphs consisting of the independent sets and cliques, resp., of maximum size. Each of these two hypergraphs is uniform by definition; they are regular because X is vertex-transitive. Since a clique and an independent set share at most one vertex, the result follows from part (b) of Lemma 3.10. □

We note that Delsarte [Del73] proves the same conclusion under the condition that X is the union of classes in an association scheme (cf. Chap. 15), in particular, if X is strongly regular. This condition does not imply the presense of any automorphisms, nor is it a consequence of vertex-transitivity.

A related observation concerns the connection between the chromatic number $\chi(G)$ and the independence number $\alpha(G)$. Clearly, $\chi(G) \geq n/\alpha(G)$ for all graphs. For vertex-transitive graphs, this inequality is nearly tight, as pointed out to us by M. SZEGEDY.

PROPOSITION 3.12. *If G is a vertex-transitive graph then*

$$n/\alpha(G) \leq \chi(G) \leq n(1 + \ln n)/\alpha(G).$$

Proof (of the rightmost inequality): Let A be an independent set of size $\alpha = \alpha(G)$; then the probability that $m = \lceil \ln n \rceil$ random translates of A (by automorphisms) do not cover $V(G)$ is less than $n \cdot (1 - \alpha/n)^m < n \cdot e^{-\alpha m/n} \leq 1$. □

Another corollary to Lemma 3.10, of interest to the theory of computing, concerns *Boolean functions* $f : 2^X \to \{0, 1\}$. Here, X is a set of n Boolean variables $x_1, \ldots, x_n$, and 2^X represents the set of all possible truth value assignments to X. A partial truth value assignment $y : Y \to \{0, 1\}$ ($Y \subseteq X$) is said to *force* f to 0 if $f(x) = 0$ whenever x is an extension of y. We call such a y a 0-*certificate* for f; its *size* is $|Y|$, the cardinality of the domain of y. We define 1-*certificates* analogously. Let $n_0(f)$ and $n_1(f)$ denote the minimum size of 0-certificates and 1-certificates, resp. For every $x \in 2^X$ there exists a smallest restriction y of x which is an $f(x)$-certificate; let $m(f; x)$ denote its size, and let $N(f) = \max_x m(f; x)$ where the maximum is taken over 2^X. The quantity $N(f)$ is called the *nondeterministic decision-tree complexity* of f. (This is a lower bound on the *deterministic* decision-tree complexity discussed in Chap. 34, Sec. 4.4. Incidentally, the "evasiveness" problems considered there relate symmetry to complexity in a remarkable way.) Clearly, $N(f) \geq \max\{n_0(f), n_1(f)\}$.

Automorphisms of f are those permutations of X which leave f invariant.

COROLLARY 3.13. *If f is a non-constant Boolean function on n variables with transitive automorphism group then $n_0(f)n_1(f) \geq n$. Consequently, $N(f) \geq \sqrt{n}$.*

PROOF: The domains of a 0-certificate and a 1-certificate must intersect. One can thus apply Lemma 3.10 (a) to the hypergraphs formed by an orbit of each kind of domain. □

Our next subject is **long paths** and **cycles.** Only four connected vertex-transitive graphs without Hamilton cycles are known (assuming the number of vertices is $n \geq 3$). Each of them is trivalent; and the first two are *3-arc-transitive* (cf. Sec. 5.1): the Petersen graph (10 vertices), and the Coxeter graph (28 vertices) (see Figa. 8,9 in Chap. 1, Sec. 4). (The automorphism group of the latter is $PGL(2,7)$, see Wong [Won67]; cf. [Big73]). The other two are obtained from these by replacing each vertex by a triangle (30 and 84 vertices, resp.). Each of these four graphs possesses a Hamilton path and none of them is a Cayley graph. A conjecture of Lovász (1969) *not shared* by this author holds that all connected vertex-transitive graphs have Hamilton paths. The problem as to whether all Cayley graphs ($n \geq 3$) have Hamilton cycles appears to first have been stated by E. Rapaport-Strasser [RS59]. In my view these beliefs only reflect that Hamiltonicity obstacles are not well understood; and indeed, vertex-transitive graphs may provide a testing ground for the power of such obstacles. We conjecture that for some $c > 0$, there exist infinitely many connected vertex-transitive graphs (even Cayley graphs) without cycles of length $\geq (1-c)n$.

We mention a useful Hamiltonicity obstacle. A graph is *tough* if, after deletion of any k of its vertices, the remaining graph has $\leq k$ connected components. Obviously, any Hamiltonian graph is tough; being non-tough is a Hamiltonicity obstacle. This obstacle breaks down for vertex-transitive graphs: *every connected vertex-transitive graph is tough.* Indeed, by Theorem 3.7(b), a d-regular connected vertex-transitive graph has edge-connectivity d, a circumstance that immediately implies toughness.

At any rate, the Hamiltonicity conjectures have been confirmed in a number of cases. One notable Hamilton cycle was even patented in 1953: the one constructed by F. Gray for the minimal Cayley graphs of the elementary abelian groups of order 2^d (the d-cube). A large number of papers has since referred to Hamilton cycles in Cayley graphs as "generalized Gray codes". (See the references in [CSW89].)

In the subsequent statements, every graph has $n \geq 3$ vertices.

It is easy to see that every Cayley graph of a finite abelian group is Hamiltonian (J. Pelikán, see [Lov79a, Ex.12.17]). Marušič, Witte, Keating, Dürnberger, and others succeeded in significantly relaxing the condition of commutativity. We refer to the survey by Witte and Gallian [WG84] for details. One of the weakest known *sufficient conditions* for all Cayley-graphs of G to be Hamiltonian is that *the commutator subgroup of G is cyclic of prime power order* (Keating-Witte [KW85]; cf. [Dür85]). Witte proved that *all Cayley digraphs of a p-group have a Hamilton cycle* [Wit86].

So far, no non-solvable group has been shown to have this property. Even the following, less ambitious problem is open: does every finite group have a minimal Cayley graph with a Hamilton cycle?

For several reasons (including, as a curiosity, *campanology*, the study of bell ringing sequences, see White [Whi85]), special classes of Cayley graphs of the symmetric groups are of interest.

THEOREM 3.14. (KOMPEL'MACHER-LISKOVETS [KL75]) *Let T be any connected system of transpositions of n elements. Then the Cayley graph $\Gamma(S_n, T)$ is Hamiltonian.*

The case of adjacent transpositions (see S. M. Johnson [Joh63]) was recently generalized to all finite reflection groups (groups of affine transformations of $\mathbb{R}^n$, generated by a set of reflections) (Conway, Sloane, Wilks [CSW89]).

The situation for Cayley *digraphs* is more complicated. Rankin [Ran48] determined when a Cayley digraph $\vec{\Gamma}(G, S)$ of a finite abelian group G is Hamiltonian provided $|S| = 2$ and gave examples of Cayley digraphs of the alternating groups A_6 and A_7 without Hamilton cycles. J. Milnor gave a class of solvable groups with two generators such that the difference between the order of the group and the longest directed paths in the resulting Cayley digraphs is arbitrarily large (see [WG84]).

Much less is known about vertex-transitive graphs of given order. Trivially, every connected vertex-transitive graph of prime order p is a Cayley graph and is therefore Hamiltonian. Marušič's result (Theorem 3.4(b)) extends this to orders p^2 and p^3.

THEOREM 3.15. (a) *Every connected vertex-transitive graph of order n is Hamiltonian if n has one of the following forms: p, $2p$, with the exception of the Petersen graph* (ALSPACH, [Als79])*; $3p$, p^2, p^3, $2p^2$* (MARUŠIČ [Mar85], [Mar87])*;*

(b) *Every connected vertex-transitive graph of order $4p$ and $5p$ has a Hamilton path* (MARUŠIČ–PARSONS [MP83]).

The only general lower bound on the length of the longest cycles and paths of vertex-transitive graphs is the following. (Nothing better is known for Cayley graphs either.)

PROPOSITION 3.16. ([BAB79B]) *If X is a connected vertex-transitive graph on $n \geq 5$ vertices then X has a cycle of length $> 2\sqrt{n}$.*

We note that 3-connected trivalent graphs have cycles of length $\geq n^{0.69}$ (Jackson [Jac86]) but need not have cycles longer than $n^{0.96}$ (Bondy-Simonovits [BS80]).

The proof of the Proposition is based on the following observation: *If X is a 3-connected regular graph of order $n \geq 4$ then every pair of longest cycles intersects in ≥ 4 vertices.* Now, since every connected vertex-transitive graph of degree ≥ 3 is 3-connected (Theorem 3.7 (a)), an application of the Regular Hypergraph Counting Lemma 3.10 to the vertex sets of the longest cycles completes the proof of Proposition 3.16. □

3.4 Subgraphs, chromatic number

Every graph Y with n vertices is an induced subgraph of some Cayley graph X of any given group of order $\geq cn^2$ ([Bab78b], [BS85], [GI87]). Every Y can be embedded into a Cayley graph of order 2^n such that all automorphisms of Y extend to automorphisms of X. The following more general extension theorem holds.

THEOREM 3.17. (E. HRUSHOVSKI [HRU92]) *Given a finite graph Y and a family $\mathcal{F}$ of isomorphisms between pairs of subgraphs of Y, there exists a finite graph X containing Y as an induced subgraph, such that all elements of $\mathcal{F}$ extend to automorphisms of X.*

Here, X may be required to be flag-transitive. This result has applications to the structure theory of the automorphism group of the Rado graph (countable "random graph", cf. Sec. 5.3). It follows that "almost all" automorphisms of that graph are conjugates ("almost all" in the sense "comeager" (complement of a set of first Baire category [Oxt80]): there exists a *comeager* conjugacy class; cf. Truss [Tru92]).

Not all graphs are subgraphs of *minimal* Cayley graphs. Let $X = \Gamma(G, S)$ be a minimal or semiminimal Cayley graph (cf. Sec.3.1) of the (finite or infinite) group G. Such graphs admit a coloring of the edges with the following properties: (a) every vertex has degree ≤ 2 in each color; (b) at least one of the colors occurring in a cycle occurs at least twice on that cycle. (In the minimal case, each color occurring in a cycle occurs at least twice.)

These properties put constraints on the possible subgraphs. In particular, if X is a minimal Cayley graph then it contains no K_4^- (K_4 minus an edge), and no $K_{2,3}$. If X is semiminimal, it contains no $K_{5,17}$ ([Bab78a]). In both cases it follows that the chromatic number of X is at most countably infinite, according to the following result of Erdős and Hajnal (see Chap. 42, Thm. 6.3.): *If a graph has uncountably infinite chromatic number then it contains $K_{m,\aleph_1}$ for every positive integer m.*

It is an *open problem* whether or not the chromatic number of finite minimal Cayley graphs is bounded. We conjecture it is not. A related stronger conjecture is that for every $\epsilon > 0$ there exist minimal Cayley graphs X such that $\alpha(X) \leq \epsilon|V(X)|$ where $\alpha(X)$ denotes the size of the largest independent set of X.

A strong consequence of constraints (a) and (b) above was deduced by Spencer.

Theorem 3.18. (Spencer [Spe83]) *For every $g \geq 3$ there exists a finite graph Y of girth g such that Y is not a subgraph of any (semi)minimal Cayley graph.*

The proof uses the probabilistic method and does not provide explicit graphs Y. It is not known whether or not such excluded subgraphs of girth 5 and degree 3 exist, even for minimal Cayley graphs. (The Petersen graph is a subgraph of a minimal Cayley graph of a group of order 20.)

Every finite group has a Cayley graph of chromatic number ≤ 4. (This is a consequence of the fact that every finite simple group is generated by ≤ 2 elements.) It is an open question whether or not every infinite group has a Cayley graph of finite chromatic number.

3.5 Neighborhoods, clumps, Gallai–Aschbacher decomposition

In this section we highlight a graph theoretic result that has played a role in the *classification theory of finite simple groups*.

We shall (in this section) consider finite graphs as well as locally finite infinite graphs with uniformly bounded degrees. X will always denote a graph with vertex set V and complement $\overline{X}$; the set of neighbors of $x \in V$ is denoted by $X(v)$. The subgraph induced by $X(v)$ is the *link* at v. We say that X has *constant link* Y if all of its links are isomorphic to Y (a finite graph by the convention above). All vertex-transitive graphs have constant link, and many others, including triangle-free regular graphs and their line graphs. A finite graph Y is a *link graph* if there exists a graph with constant link Y.

Many classes of link-graphs as well as non-link graphs have been found (see [Hel78], [BHM80]). However, [Bul72] asserts that the problem whether or not a given finite graph is a link graph is undecidable. It is shown in [Bul72] and [BC75] that there exist graphs which are links of infinite vertex-transitive graphs but do not occur as links in finite constant-link graphs. By counting certain triangles, Blass, Harary, and Miller [BHM80] show that *if L is the link in a finite vertex-transitive graph and i is an odd number then the number of vertices of degree i in L is even.* This is not true for link graphs in general ([BC75] provides an infinity of examples), nor does it hold for infinite vertex-transitive graphs. Hell [Hel78] observes that if a (finite or infinite) vertex-transitive graph X has an *asymmetric* link then X is a Cayley graph (in fact a GRR, cf. Sec.4.3). He also shows that the link of a Cayley graph has an even number of vertices of degree one.

The following fairly general result is implicit in [Asc76].

THEOREM 3.19. *Assume both X and $\overline{X}$ are connected. Then at least one of the links of X, say Y, has the property that $\overline{Y}$ has a unique largest connected component.*

A stronger result holds for vertex-primitive graphs.

THEOREM 3.20. (M. ASCHBACHER, B. FISCHER) *Let X be a vertex-primitive graph other than the complete graph. Let Y be the graph induced by the neighborhood of a vertex in X. Then the complement of Y is connected.*

The proof of these theorems rests on a purely graph theoretical result, part of which was discovered by Gallai [Gal71] in the context of the *characterization of transitively orientable graphs.*

A subset $C \subseteq V$ is called a *clump* if for each $w \in V \setminus C$, if w has a neighbor in C then $X(w) \supseteq C$. The *trivial* clumps are V, $\emptyset$, and the singletons. A *proper clump* is a clump other than V. A *maximal* clump is a proper clump not properly contained in any other clump.

We begin with two easy observations. (a) If C, D are clumps and $C \cap D \neq \emptyset$ then $C \cup D$ is a clump. (b) If both X and its complement $\overline{X}$ are connected then V is not the union of two proper clumps. It is immediate from these that *maximal clumps are pairwise disjoint*, which proves part (i) of the following result.

THEOREM 3.21. (GALLAI–ASCHBACHER DECOMPOSITION) *Assume both X and $\overline{X}$ are connected. Let $C_1, \ldots, C_m$ be the maximal clumps of X. Then* (i) [Gal71, Asc76] *$(C_1, \ldots, C_m)$ form a partition of V.* (ii) [Asc76] *Let N_i be the set of common neighbors of C_i. (By definition, $C_i \cap N_i = \emptyset$.) Then there exists i such that the subgraph induced by N_i in the complement of X is connected.*

To see how Theorem 3.20 follows, we observe that the maximal clumps form a system of imprimitivity for $\mathrm{Aut}(X)$; therefore if X is vertex-primitive then each C_i is a singleton.

The proof of assertion (ii) is nontrivial. For $v \in V$, consider the components of the subgraph of $\overline{X}$ induced by $X(v)$. Let M be a maximal such component (considering all $v \in V$). By definition, M induces a connected subgraph of $\overline{X}$. Let C be the set of common neighbors of M. One can prove that C is a maximal clump, and M is the set of common

neighbors of C. This completes the proof of Theorem 3.21; and together with (i) above we also see that the choice of M among the components of $X(v)$ in $\overline{X}$ must be unique (since any other component is a subset of C, the unique maximal clump containing v). □

Gallai [Gal71] gives the following equivalent definition of the above decomposition. Let us say that two edges are equivalent if they together form an induced path of length 2. Take the transitive closure of this relation to obtain the *Gallai equivalence*. If both X and $\overline{X}$ are connected, then there will be a unique Gallai class of edges which spans the entire X. The components of the complement of this class can be grouped together in a unique way to produce the maximal clumps; two such components will belong to the same class if they have the same neighborhood in X.

The role of Theorem 3.20 in the *classification of finite simple groups* is explained by Aschbacher [Asc76]. He shows how B. Fischer's celebrated "3-transpositions theorem" [Fis71] follows from it; in fact, the result arose from one of Fischer's lemmas. A set of *3-transpositions* is a set S of elements of order 2 in a group G such that for any pair $g, h \in S$, the order of gh is ≤ 3. Fischer characterized those almost simple groups which are generated by a conjugacy class of 3-transpositions. These include all the symmetric groups, certain classical (symplectic, orthogonal, unitary) groups, plus three sporadic groups discovered in the process (named $M(22)$, $M(23)$, and $M(24)$). ($M(24)$ is not simple; like the symmetric groups, it has a simple subgroup of index 2. Cf. [Asc80].)

Fischer's central result was that the action of G by conjugation on S is a rank 3 permutation group. This is derived from considering the vertex-transitive graph with vertex set S, joining two elements if they commute. G is shown to act as a primitive group on this graph; and Theorem 3.20 is invoked. □

Godsil [God80b] considers the link L of X together with the link L^* of $\overline{X}$, the *dual link*. He gives the following remarkable characterization: *if X is finite, vertex-transitive, both the link L and the dual link L^* are disconnected but at least one of them has no isolated vertices, then $X \cong L(K_{3,3})$.* He also characterizes the case when both L and L^* have isolated vertices. In this latter case, $\mathrm{Aut}(X)$ always has an element of the form (12)(34). These results are central to his solution of the GRR problem (cf. Sec.4.3).

3.6 Rate of growth

Note. Throughout this section, X will denote an *infinite, connected, locally finite* graph. (A graph is locally finite if all vertices have finite degree.)

Certain properties of groups are best expressed in graph theory language. A foremost example is the **growth rate** of finitely generated infinite groups.

For a graph X, let $B(n, x)$ denote the *ball of radius n* about the vertex x, i.e. set of vertices at distance $\leq n$ from x. For a vertex-transitive graph, set $f(n) = |B(n, x)|$. This function has a property resembling log-concavity.

Proposition 3.22. (Gromov [Gro81]) *If X is vertex-transitive, then $f(n)f(5n) \leq (f(4n))^2$.*

Proof: Let Y be a maximal system of vertices in $B(3n, x)$ pairwise at distance $\geq 2n+1$. Now the disjoint balls $B(n, y) : y \in Y$ are contained in $B(4n, x)$, hence $|Y|f(n) \leq f(4n)$.

On the other hand, the balls $B(2n, y) : y \in Y$ cover $B(3n, x)$, and therefore the balls $B(4n, y) : y \in Y$ cover $B(5n, x)$. This implies $f(5n) \leq |Y| f(4n)$, hence the result. □

X is said to have *growth rate* $g(n)$ if $g(c_1 n) \leq f(n) \leq g(c_2 n)$ for some constants c_1, c_2 and every sufficiently large n. Thus, the growth rate is an equivalence class of functions rather than a function. There is a natural partial order on the equivalence classes; when comparing growth rates, we shall always mean comparison of their equivalence classes.

X is said to have *polynomial growth rate* if its growth rate is bounded by n^c for some constant c; its growth rate is *exponential* if it is bounded from below by c^n for some constant $c > 1$.

For a finitely generated infinite group G, the *growth rate of* G is defined as the growth rate of the Cayley graph $\Gamma(G, S)$ for some finite set S of generators of G. It is easy to see that the growth rate does not depend on the particular choice of S; a change in the generators will only affect the constants c_1 and c_2.

Finitely generated Abelian groups have polynomial growth rates, non-cyclic free groups have exponential growth rates. The following is easy to prove.

PROPOSITION 3.23. (a) *If H is a subgroup of G, then the growth rate of G is greater than or equal to the growth rate of H.*
(b) *If $|G : H|$ is finite then G and H have the same growth rates.*
(c) (GROMOV [GRO81]) *If H is finitely generated and $|G : H|$ is infinite then $f_G(n) \geq n f_H(n)$, where f_G and f_H are the growth functions of the respective groups under appropriately chosen sets of generators.*
(c) (MILNOR, WOLF [MIL68A, WOL68]) *Finitely generated nilpotent groups have polynomial growth rates.*

The Bass-Wolf formula gives the exact growth rates of nilpotent groups. Let G be a finitely generated infinite nilpotent group and let $G = G_1 > G_2 > \ldots > G_m = 1$ be its descending central series. Let d_i be the torsion-free rank of the abelian group G_i/G_{i+1}.

THEOREM 3.24. (BASS, WOLF [BAS72, WOL68]) *The rate of growth of the nilpotent group G is n^d where $d = \sum i d_i$.*

The following very deep result settles a problem raised by Milnor [Mil68a]:

THEOREM 3.25. (GROMOV [GRO81]) *A group has polynomial growth rate if and only if it is nilpotent-by-finite, i.e. it has a nilpotent subgroup of finite index.*

Two important particular cases of this result were established earlier; they are ingredients in Gromov's proof.

THEOREM 3.26. (MILNOR, WOLF, TITS [MIL68A, WOL68, TIT72]) (a) *A finitely generated solvable group G has exponential growth unless G is nilpotent-by-finite.*
(b) *A finitely generated subgroup G of a connected Lie group has exponential growth unless it is nilpotent-by-finite.*

In fact, Tits proves the following stronger statement.

THEOREM 3.27. (TITS [TIT72]) *If L is a Lie group with finitely many components and G is a finitely generated subgroup of L then either:*

(a) *G contains a free group of rank 2 and has therefore exponential growth; or*
(b) *G is solvable-by-finite. In this case it has exponential growth rate unless it is nilpotent-by-finite.*

We give a very rough sketch of the proof of Gromov's Theorem 3.25. Let G be a finitely generated group of polynomial growth. Fix a finite set S of generators. Select a sequence $r_i \to \infty$ of integers. Consider the sequence of metric spaces Γ_i on the set G with distance $d_i(x,y) = \frac{1}{r_i}\text{dist}(x,y)$ where "dist" is the distance in the Cayley graph $\Gamma(G,S)$. The sequence r_i is chosen so as to ensure a fairly regular behavior of the sequence $f(2^j r_i)$, $i = -j, \ldots, j$. This is accomplished with the aid of Proposition 3.22 and using the assumption of polynomial growth. The sequence Γ_i is then nice enough to have a subsequence that converges in an appropriate sense to a metric space Y. Elementary considerations show that Y is locally compact, connected, and locally connected. Moreover, each ball in Y is path-connected. The isometry group L of Y is transitive on Y. The choice of the r_i ensures that the Hausdorff dimension of Y is finite. A celebrated theorem of Montgomery and Zippin [MZ55] now implies that under these conditions, L is a Lie group with a finite number of components. Now a fairly involved argument using the quoted result of Tits (Theorem 3.27(b)) completes the proof. □

Other ingredients of this last part of the proof are the Milnor-Wolf theorem (Theorem 3.26(a)) and the following theorem of Jordan (cf. [Rag72]).

THEOREM 3.28. (JORDAN [JOR95]) *If L is a Lie group with a finite number of components then there exists a number q such that every finite subgroup of L contains an Abelian subgroup of index at most q.*

An appendix to Gromov's paper contains a relatively simple proof of the subcase of the Milnor-Wolf theorem used in Gromov's proof.

Milnor [Mil68a] raised the question whether groups with "intermediate growth rates" (neither polynomial, nor exponential) exist. The positive answer was given by Grigorchuk.

THEOREM 3.29. (GRIGORCHUK [GRI83]) *There exist 2-generated torsion groups with growth rates between 2^{n^α} and 2^{n^β} where $\alpha = 1/2 - \epsilon$ for any $\epsilon > 0$ and $\beta = \log_{32} 31$.*

Vertex-transitive graphs with polynomial growth rates were characterized by V.I. Trofimov.

THEOREM 3.30. (TROFIMOV [TRO85]) *Let X be vertex-transitive. The following are equivalent.*

(a) *X has polynomial growth.*
(b) *The vertex set V under the action of $\text{Aut}(X)$ admits a system of imprimitivity σ with finite equivalence classes such that $\text{Aut}(X/\sigma)$ is finitely generated, nilpotent-by-finite, and the stabilizer of any vertex of X/σ in $\text{Aut}(X/\sigma)$ is finite.*

Here X/σ is the homomorphic image of X under the vertex map $V(X) \to V(X)/\sigma$; hence two equivalence classes are adjacent if they have at least one pair of adjacent representatives.

Related topics are surveyed in [Tro92].

We should mention that these questions were originally motivated by connections between the curvature of a Riemannian manifold and the growth rate of its fundamental group (Milnor [Mil68b]).

3.7 Ends

Note. Throughout this section, X will denote an *infinite, connected, locally finite* graph. (A graph is locally finite if all vertices have finite degree.)

Ends are another important graphic notion for finitely generated infinite groups. (For a detailed account, see Cohen [Coh72].)

The set of *ends* of a connected, locally connected, locally compact Hausdorff space X is defined as the inverse limit of the directed family of the set of components of $X \setminus C$ for all compact subsets C (Hopf [Hop44]). The analogous concept for connected graphs was developed by Halin [Hal64].

Ends of a (connected, infinite, locally finite) graph X can be defined analogously as the inverse limit of the sets of infinite components obtained by deleting finite subsets C of the edge set of the graph X. The ends can also be defined as equivalence classes of one-way infinite paths: two such paths are equivalent if the deletion of no finite set of edges separates their infinite components.

The *ends* of a finitely generated group are defined as the ends of its Cayley graphs. Again, different choices of finite sets of generators result in topologically equivalent sets of ends. Stallings [Sta71] contains important results on ends of groups.

PROPOSITION 3.31. (HOPF [HOP44]) *If X is vertex-transitive then it has 1 or 2 or infinitely many ends. In particular, the same holds for finitely generated infinite groups. Consequently, if X has more than 2 ends then it has exponential growth rate.*

A vertex-transitive graph has *two ends* if and only if it has *linear growth rate.* Groups with two ends have been fully characterized.

THEOREM 3.32. (FREUDENTHAL [FRE45]) *A finitely generated infinite group G has two ends if and only if G has a finite normal subgroup N such that the factor group G/N is either cyclic ($\mathbb{Z}$) or dihedral (the free product $\mathbb{Z}_2 * \mathbb{Z}_2$).*

Groups with infinitely many ends have also been characterized. We note that they have exponential growth rates; the converse is false. Let A be a group, F a subgroup, and $\varphi : F \to A$ an injection. The HNN-extension $G = (A, F, \varphi)$ is generated by A and an additional element x subject to the relations $x^{-1} f x = \varphi(f)$ $(f \in F)$.

THEOREM 3.33. (STALLINGS [STA71]) *A finitely generated group G has infinitely many ends if and only if G is*

(a) *either a free product with amalgamated finite subgroup $G = G_1 *_F G_2$, where F is a finite proper subgroup of each G_i and has index ≥ 3 in at least one of them;*
(b) *or an HNN-extension $G = (A, F, \varphi)$, where F is a finite proper subgroup of A.*

These cases are closely related to group actions on trees. A theory of such actions was developed by Bass and Serre [Ser80]. We quote two special cases.

The group G is said to act *without inversion* on a graph if no element of G inverts any edges. In other words, G preserves an orientation of the graph.

THEOREM 3.34. ([SER80, CH. 4]) (a) *Let G act edge-transitively but not vertex-transitively on a tree T. Let P, Q be two adjacent vertices of X. Then G is the free product of the stabilizers of P and Q amalgamated at their intersection.*
(b) *Every amalgam of two groups acts on a tree in this way.*

THEOREM 3.35. ([SER80, CH. 5.4]) *Let G act edge-transitively and vertex-transitively but without inversions on a tree T. Then G is an HNN-extension of the stabilizer of a vertex. - Every HNN-extension acts on a tree in this way.*

For the general structure theorem, see Sec. 3.11.

M.J. Dunwoody used Theorems 3.34 and 3.35 to give the following remarkable generalization of the Stallings characterization theorem (Theorem 3.33).

THEOREM 3.36. (DUNWOODY [DUN82]) *Let G be a group acting on a connected graph X with ≥ 2 ends. Then G is either an amalgam $G = A *_C B$ or an HNN-extension of a group C, where in each case C contains the stabilizer of two adjacent vertices as a subgroup of finite index.*

The proof is based on the construction of a tree T on which G acts without inversions and so that the factor graph has a single edge. A key tool for the construction of T is the following surprisingly strong statement on the existence of cuts of very special kind.

THEOREM 3.37. (DUNWOODY [DUN82]) *Let $X = (V, E)$ be a connected graph with ≥ 2 ends. Then there exists a nonempty proper subset $A \subset V$ such that*
(a) *the set of edges between A and $V \setminus A$ is finite;*
(b) *for any $g \in G$, either A or $V \setminus A$ is included in either A^g or in $(V \setminus A)^g$.*

In this result, the graph X is not required to be locally finite.

3.8 Isoperimetry, random walks, diameter

The *boundary* of a subset U of the vertex set V of the graph X is the set ∂U of vertices in $V \setminus U$, adjacent to at least one vertex in U. The *isoperimetric ratio* of a set $W \subset V$ is defined as $\epsilon(W) = |\partial(W)|/|W|$. We say that W is *ϵ-expanding* if $\epsilon(U) \geq \epsilon$ for every $U \subseteq W$ $(U \neq \emptyset)$. We call X an *ϵ-expander* if every subset $W \subset V$ with $1 \leq |W| \leq |V|/2$ is ϵ-expanding. A "family of linear expanders" is an infinite sequence of graphs of bounded degree which are ϵ-expanding for some fixed $\epsilon > 0$. ("Linear" refers to the $O(V)$ bound

on the number of edges.) Expanders are treated in detail in Chapter 32. Some Cayley graphs of linear groups turn out to be particularly strong expanders [LPS88b], [Mar88].

Here we shall focus on more modest expansion properties shared by *all vertex-transitive graphs.* The generality of the results is important in applications to the analysis of algorithms in groups (cf. [Bab91a]).

It is easy to see that that the diameter of an ϵ-expander on n vertices can be bounded as

$$\mathrm{diam}(X) < \ln n / \ln(1+\epsilon). \tag{4}$$

For $\epsilon \leq 1/2$, we infer $\epsilon < (4/3)(\ln n/\mathrm{diam}(X))$. It is remarkable that for vertex-transitive graphs, this inequality is tight apart from an $\ln n$ factor.

THEOREM 3.38. ([ALD87, BAB91B, BS92A]) *If X is a vertex-transitive graph of diameter Δ then it is a $2/(2\Delta+1)$-expander.*

D. Aldous's proof (for Cayley graphs) is based on the following observation, due to Erdős and Rényi [ER65] (cf. [BE82]), which we quote in a slightly generalized form ([BS85], [CFS90]).

PROPOSITION 3.39. *Let G be a transitive group acting on a set V, $|V| = n$. Let $A \subseteq V$. Then*

$$(1/|G|)\sum_{g\in G} |A \cap A^g| = |A|^2/n. \tag{5}$$

(A set and its translates are "independent on average".)

It follows by greedy selection that G has a transitive subgroup generated by at most $\log_2 n + \log_2 \ln n + 1$ elements [BS85], and a set of $O(\log n)$ random elements are likely to generate a transitive subgroup ([CFS90]), a fact with implications to efficient manipulation of permutation groups (cf. [BCFS91]).

Let now $X = \Gamma(G,S)$ where $S = S^{-1}$ generates G and assume $\mathrm{diam}(X) = \Delta$. If $|A| \leq |G|/2$ then by (5) there exists $g \in G$ such that $|A \setminus gA| \geq |A|/2$. Aldous observes that $g = h_1 \cdots h_k$ for some $k \leq \Delta$ from which one concludes that $|h_i A \setminus A| \geq |A|/(2\Delta)$ for some some $h_i \in S$, proving a $1/(2\Delta)$ lower bound for Theorem 3.38. □

By Alon's theorem [Alo86] (see Chap. 32, Theorem 3.2) it follows that for vertex-transitive graphs X of degree d and diameter Δ, the eigenvalue gap is $d - \lambda_2 > 1/(2\Delta+2)^2$, where λ_2 is the second largest eigenvalue of X.

This eigenvalue gap is significant in estimating the speed at which a *random walk* over X approaches the uniform distribution. Let us consider a *lazy* random walk on X, in which at every step we flip a coin; if it comes out heads, we don't move, else we move to an adjacent vertex, each neighbor having equal chance of being visited. (This trick eliminates potentially annoying negative eigenvalues from the matrix of transition probabilities.) A direct consequence of the foregoing considerations is the following rapid convergence ([Ald87], [Bab91b]).

COROLLARY 3.40. *Let v_0, v_1 be vertices of a vertex-transitive graph of degree d and diameter Δ with n vertices. After ℓ steps, the lazy random walk, starting at v_0, will be at v_1 with probability $(1/n)(1 \pm \epsilon)$, where*

$$\epsilon \leq n \exp(-\ell/(8d \cdot (\Delta+2)^2)). \tag{6}$$

In particular, if both d and Δ are bounded by $(\log n)^{O(1)}$, then so is the time it takes for the lazy random walk to arrive at a nearly uniformly distributed place.

For specific Cayley graphs (related e.g. to card shuffling), different methods have been used to obtain strong estimates on the time it takes to reach near uniformity [Ald83], [AD87], [Dia88].

While results of this kind necessarily require the graph to have small diameter (cf. (4)), vertex-transitive graphs with large diameter, including infinite graphs, also possess a similar *local expansion* property.

THEOREM 3.41. (LOCAL EXPANSION, [BAB91B, BS92A]) *Let X be a connected (finite or infinite) vertex-transitive graph with vertex set V. Assume that the finite subset $U \subset V$ is within the ball of radius t about some vertex; and $|U| \leq |V|/2$. Then U is a $2/(2t+1)$-expanding set.*

When $X = \Gamma(G, S)$ is a Cayley graph, again a single generator is responsible: $|Ug \setminus U| \geq |U|/(4t)$ for some generator $g \in S$ [Bab91b].

This result is a tool in the rigorous analysis of efficient algorithms for permutation groups [BCFS91]. A further consequence is that in vertex-transitive graphs, random walks *don't get stuck in a corner* for too long. In the theorem below, $X^k(v)$ denotes the ball of radius k about vertex v, and we consider how soon a random walk, starting at v, may be expected to be outside this ball.

THEOREM 3.42. (BABAI [BAB91B]) *Let v be the start vertex of a random walk over a connected vertex-transitive graph X of finite degree d. Assume $|X^{4k}(v)| \leq |V|/2$ Let $\ell \geq ck^2 d \cdot \ln |X^{4k}(v)|$. Then with probability $\geq 1/16$, at a random time chosen uniformly from $\{1, 2, \ldots, \ell\}$, the random walk will be outside $X^k(v)$. (c is an appropriate constant.)*

This result is at the heart of an algorithm which, given a set of generators of a finite group G, constructs *nearly uniformly generated random elements of G* in $O(|\log(G)|^5)$ group operations [Bab91b]. Reducing the exponent 5 would be of great significance, since many algorithms in group theory rely on "randomly chosen" elements from the group (see e.g. [NP92, BB93]). The heuristics currently used to select such elements do not seem amenable to rigorous analysis.

Random walks over locally finite *infinite* graphs such as the d-dimensional grid have been of great interest for their many applications which include approximations for partial differential equations and curvature of Riemannian manifolds (see Kesten [Kes59] and the references in [Tho90], [MGT]). One of the basic qualitative properties of such graphs is whether they are recurrent (random walks return to their start with probability 1) or transient (with positive probability they never return). A classical result of Pólya (1921) (see Feller [Fel68, vol.I,14.7]) asserts that $\mathbb{Z}^2$ is recurrent, while $\mathbb{Z}^3$ is transient. For connections of this theory with electrical currents, see [DS84], [Tho90]. Expansion properties play a critical role in determining transience; if for some fixed $\epsilon > 0$ we have $|\partial U| \geq |U|^{1/2+\epsilon}$ for every finite $U \subset V$ then the graph is transient (Varopoulos [Var85], [Var91]). This result is tight in the sense that $\epsilon = 0$ would not suffice, as the plane grid $\mathbb{Z}^2$ shows.

For Cayley graphs of finitely generated groups, transience/recurrence does not depend on the choice of the set of generators. Transience is inherited by subgroups of finite index; recurrence is inherited by all subgroups.

Thomassen and Woess [TW94] survey a large body of literature on related topics.

Our next subject is the **diameter** of Cayley graphs (cf. [BHK$^+$90] for more references). A regular graph of degree $r \geq 2$ and diameter d has at most

$$n \leq 1 + r + r(r-1) + \ldots + r(r-1)^{d-1} = 1 + r((r-1)^d - 1)/(r-2)$$

vertices, hence $d > \log_{r-1}(n/3)$. The construction of Cayley graphs of given degree and small diameter is motivated, among others, by interconnection network design for parallel computer architectures. Bounds on the diameter with respect to given generators are relevant for puzzles like Rubik's cube: in this case, the question is the diameter of a specific Cayley graph of a group of order 43,252,003,274,489,856,000 with respect to a set of 12 generators. (The diameter is known to be ≥ 19 and a rigorous almost certain probabilistic proof exists that it is no more than 36 (A. Fiat et al. [FMS$^+$89]).)

As noted above, expanders have diameter $O(\log n)$. For its simplicity and small diameter, interconnection network designers favor a Cayley graph which is not an expander: the *cube-connected cycles.* (Cf. Leighton [Lei92].) This is the Cayley graph of the group $\mathbb{Z}_2 \wr \mathbb{Z}_s$ (of order $n = s2^s$), with generators τ, ρ where τ is an involution from the first copy of $\mathbb{Z}_2$, and ρ is a rotation of order s, permuting the s copies of $\mathbb{Z}_2$. The vertices can be represented by $(0,1)$-strings of length s with one position marked. The neighbors of such a marked string are obtained by switching the marked symbol, or moving the mark left or right by one position, viewing the rightmost and leftmost positions adjacent. The graph has degree 3 and diameter $\lfloor 5s/2 \rfloor - 2$, whereas $\log_2 n = s + \log_2 s$.

We note that not all groups of order n with k generators admit Cayley graphs of degree $O(k)$ and diameter $O(\log n)$. Groups with a bounded number of generators and a nilpotent subgroup of bounded index and bounded class of nilpotence require diameter n^c by the Proposition 3.23(c). Using commutator collection, Annexstein and Baumslag obtained the following explicit value.

THEOREM 3.43. ([AB89]) *Let G be a group of order n with a nilpotent subgroup of index t and class ℓ. If S is a set of k generators of G then the diameter of $\Gamma(G,S)$ is at least $(n/t)^c$, where*

$$c = (kt\ell)^{-\ell}/2.$$

(For abelian subgroups, $\ell = 1$.)

THEOREM 3.44. (BABAI-KANTOR-LUBOTZKY [BKL89]) *Every nonabelian finite simple group G of order n has a set S of at most 7 generators such that the diameter of $\Gamma(G,S)$ is $\leq C \log n$ for some absolute constant.*

The Cayley graphs constructed in the proof are unlikely to be expanders; it is not known whether an expander family of bounded degree Cayley graphs of the alternating groups exists, for instance. They have the advantage, however, that, given an element of

G in the natural (matrix) representation of G, there is an efficient algorithm (polynomial in $\log n$) to solve this "generalized Rubik's cube" puzzle, i.e. to compute a path of length $O(\log n)$ to the identity. (The explicit expanders mentioned in Chap. 32 give no clue, how to find such a short path.) As an illustration, we describe the solution for the case $G = SL(2, p)$. With the generators

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad\qquad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

we obtain expanders but no explicit routing. Instead, we choose the generators

$$C = \begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix} \qquad\qquad D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and A. It is easy to see that A and C rapidly generate all strict upper triangular matrices because

$$C^{-1} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} C = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}.$$

Conjugating by D we obtain transposes.

A particularly elegant construction of a Cayley graph of the symmetric group S_n, having diameter $\leq 6.75n \log_2 n$, was given by J-J. Quisquater [Qui86] (cf. [BHK+90]).

If we admit a logarithmic number of generators, the situation becomes favorable for every group. The following result is a consequence of Proposition 3.39 (cf. [BE82] for a short proof).

THEOREM 3.45. (ERDŐS–RÉNYI [ER65]) *Given a group G of order n, there exists a set of $k \leq \log_2 n + \log_2 \ln n + 1$ elements $S = \{g_1, \ldots, g_k \in G\}$ such that every $x \in G$ is representable in the form*

$$x = g_1^{\epsilon_1} g_2^{\epsilon_2} \cdots g_k^{\epsilon_k}, \text{ where } \epsilon_i \in \{0, 1\}.$$

In particular, the diameter of $\Gamma(G, S)$ is $\leq k$.

In estimating the diameter of a Cayley graph, one faces much greater difficulties if the generators are prescribed. We conjecture, that for every finite simple group G and every set S of generators, the diameter of $\Gamma(G, S)$ is at most $(\log |G|)^c$ for some absolute constant c. Even in the case of alternating, or, equivalently, symmetric groups, this has only been verified in very special cases. For permutation groups, the following are known.

THEOREM 3.46. *Let $G \leq S_n$ be generated by the set S. Then the diameter of $\Gamma(G, S)$ is not greater than:*

(a) *$c_k n^2$, if all members of S are cycles of lengths $\leq k$* (Driscoll-Furst [DF87]);
(b) *cn^{2k}, if all members of S have degree $\leq k$* (McKenzie [McK84]);
(c) *$\exp(\sqrt{n \ln n}(1 + o(1)))$, if no assumption on S is made* (Babai-Seress [BS88]).

The bound in (c) is asymptotically tight, as shown by the cyclic group generated by the product of cycles of prime lengths $2, 3, \ldots, p_i$ where $2+3+\ldots+p_i \leq n < 2+3+\ldots+p_{i+1}$. Unfortunately, however, no better bound is known for $G = S_n$ either.

We can do much better if the generators are chosen at random rather than adversarially.

THEOREM 3.47. *Let σ, τ be two randomly selected permutations of a set of n elements and $G = \langle \sigma, \tau \rangle$.*

(a) *With probability $1 - O(1/n)$, $A_n \leq G \leq S_n$* (Dixon [Dix69]). *(The error term is from* [Bab89].*)*

(b) *With probability $1 - o(1)$, the diameter of $\Gamma(G, S)$ is at most $n^{\frac{1}{2}\ln n(1+o(1))}$* (Babai-Hetyei [BH92]).

To appreciate the difficulty of determining the exact diameter with respect to a given set of generators, we mention two results on the computational complexity of this problem. For a permutation group $G \leq S_n$, it is NP-hard to determine the diameter of $\Gamma(G, S)$ even if G is an elementary abelian 2-group (Even, Goldreich [EG81]). For Cayley digraphs of permutation groups, it is a $PSPACE$-complete problem to determine the directed distance of a given pair of group elements (Jerrum [Jer85]).

3.9 Automorphisms of maps

Note. In this section, both finite and infinite graphs will be considered. All surfaces (2-dimensional manifolds) considered are closed (without boundary) and compact, with the significant exception of the plane.

One has to make a distinction between the automorphism groups of *graphs* embeddable on a surface Σ and the automorphism groups of the *maps* defined by specific embeddings $X \subset \Sigma$.

Recall (cf. Chap. 5) that a map is a graph X embedded on a surface Σ such that the components of $\Sigma \setminus X$, the *faces* of the map, are homeomorphic to an open disc. If the surface Σ is compact, X must be finite. *Map-automorphisms* preserve incidences between edges and faces in addition to those between edges and vertices. If v, e, and f denote the number of vertices, edges, and faces, resp., of a map on a compact surface then

$$v - e + f = \chi \tag{7}$$

where $\chi = \chi(\Sigma)$ denotes the Euler characteristic of Σ.

Recall that $\chi \leq 2$ is an integer. If Σ is orientable then χ is even; the quantity $g = 1 - \chi/2$ is the *genus* of Σ; and Σ is homeomorphic to the "sphere with g handles". If Σ is non-orientable then $g' = 2 - \chi$ is its non-orientable genus; and Σ is homeomorphic to the "sphere with g' crosscaps". Thus, orientability and the Euler characteristic characterize all compact surfaces up to homeomorphism.

The compact surfaces of non-negative Euler characteristic are the following: (a) orientable: the sphere ($\chi = 2$) and the torus ($\chi = 0$); (b) non-orientable: the projective plane ($\chi = 1$) and the Klein bottle ($\chi = 0$).

Map-automorphisms extend isomorphically to groups of homeomorphisms of Σ, and conversely: every finite group G acting on a compact surface Σ acts as a *vertex-transitive* group of automorphisms of some map. Unless Σ is the sphere, we may require in addition that every face has at least 3 sides. (For instance, if G is the trivial group and Σ is the torus, we shall have a single vertex with two loops, creating a single four-sided face.)

Each non-orientable surface Σ_1 has an orientable double cover Σ_2, of Euler characteristic $2\chi(\Sigma_1)$. The action of any group G on Σ_1 can be lifted isomorphically to an *orientable* action on Σ_2. The action of G on Σ_2 commutes with the sense-reversing "antipodal map" which switches the pairs of preimages of the covering map $\Sigma_2 \to \Sigma_1$, hence $G \times \mathbb{Z}_2$ acts on Σ_2. These facts follow from the elements of homotopy theory; cf. [Tuc83, p.96].

To understand finite group actions and maps on compact surfaces, we need to look to the three *natural geometries:* the sphere, the Euclidean plane, and the hyperbolic plane. (These are the only simply connected 2-dimensional complete Riemannian manifolds of constant curvature.)

Let G be a finite group of homeomorphisms of the compact surface Σ of Euler characteristic χ. Then Σ admits a G-invariant Riemannian metric of constant curvature. The curvature will be positive, zero, or negative according to the sign of $\chi(\Sigma)$. This makes our surface Σ locally isometric to the corresponding natural geometry.

Moreover, if M is a vertex-transitive map on Σ, invariant under G, without one-sided or two-sided faces, then the metric can be chosen so as to make all egdes geodetic and all faces regular. (Cf. [JS78], and the proof of [ZVC80, Thm. 6.4.7].)

More about the groups and the maps on Σ can be found out by lifting them to $\widetilde{\Sigma}$, the universal covering space of Σ, which is the natural geometry locally isometric to Σ.

We define a *crystallographic group* of a natural geometry as a discrete group of isometries with compact fundamental domain [1].

THEOREM 3.48. *Let G be a finite group acting on the compact surface Σ. Then G lifts to a crystallographic group $\widetilde{G}$ of the natural geometry of its universal cover (sphere, Euclidean plane, or hyperbolic plane).*

(Cf. [ZVC80, Thm. 6.4.7].) The fundamental group $\pi_1(\Sigma)$ is normal in $\widetilde{G}$ and $\widetilde{G}/\pi_1(\Sigma) \cong G$.

An *Archimedean tiling* of a natural geometry is a map of which each face is a regular polygon and the map admits a vertex-transitive group of isometries.

THEOREM 3.49. *A vertex-transitive map M on a compact surface Σ lifts to an Archimedean tiling of the natural geometry of the universal covering surface $\widetilde{\Sigma}$.*

(Cf. the proof of [ZVC80, Thm. 6.4.7].)

One can classify the crystallographic groups of the three natural geometries via canonical codes; each code is associated with a presentation in terms of generators and relations derived from a pair of dual maps. If two such groups are isomorphic as abstract groups then their isomorphisms are also geometrically realizable (Wilkie [Wil66], Macbeath [Mac67], cf. [ZVC80, Theorems 4.5.6–4.7.1]).

[1] This deviates from common usage in the hyperbolic case where compactness is usually not required.

The crystallographic groups of the *sphere* are finite; they are listed in Sec. 1.4. There are 18 individual types and two infinite one-parameter families of *vertex-transitive maps on the sphere*, corresponding to the Platonic and Archimedean solids and the families of prisms and antiprisms.

By the foregoing remarks, we obtain that the finite group actions on the *projective plane* are precisely the actions, on the pairs of antipodal points, of the finite rotation groups of the sphere.

Vertex-transitive maps on the projective plane correspond to centrally symmetric vertex-transitive maps on the sphere and are obtained from them by identifying antipodes.

When $\chi(\Sigma) = 0$, Theorem 3.48 relates G to the classical *crystallographic groups* of the Euclidean plane. These were classified in the last century (Fedorov, 1891). There are (up to natural equivalence) 17 of them (see Coxeter-Moser [CM72, p.44]). Each crystallographic group G is equivalent to a group of isometries of the plane acting transitively on the points of a regular triangular, square, or hexagonal grid. It follows that the index of G is not greater than 12, 8, and 6, resp., in the full group of symmetries of the corresponding grid. Furthermore, G contains a normal subgroup N generated by two linearly independent translations, and the quotient G/N is a subgroup of the dihedral group of degree 6 or 4.

Every *normal* subgroup H of G generated by two linearly independent translations gives rise to a unique action of G/H on the torus $\mathbb{R}^2/H$; this observation describes all finite group actions on the *torus*. (Note, in particular, that all these groups are solvable.)

The situation with the *Klein bottle* is similar except that the normal subgroup $H \triangleleft G$ must be generated by a translation and a *glide-reflection*, i.e. a translation followed by a reflection in an axis parallel to the direction of the translation. This implies severe restrictions on G. One can prove, in particular, that the square of any rotation belongs to H, and the subgroup $T \leq G$ of translations has a subgroup T_1 of index ≤ 2 such that $T_1/(T_1 \cap H)$ is cyclic.

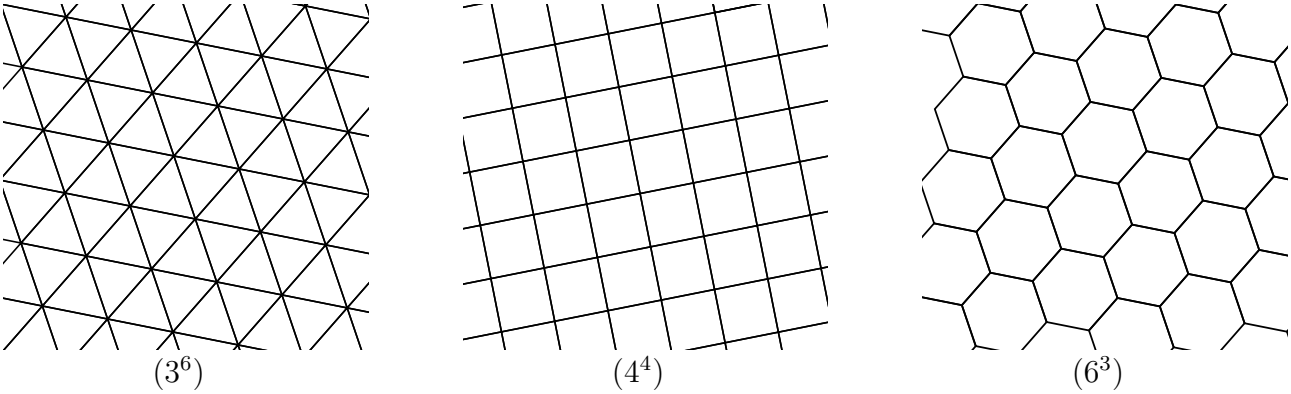
Corollary 3.50. (a) *Let G be a finite group acting on the torus. Then G has an Abelian normal subgroup N with ≤ 2 generators such that $G/N \cong \mathbb{Z}_k$ or D_k, $k = 6$ or $k \leq 4$.*

(b) *Let G be a finite group acting on the Klein bottle. Then $G \cong \mathbb{Z}_n$, D_n, $\mathbb{Z}_{2n} \times \mathbb{Z}_2$, or $D_{2n} \times \mathbb{Z}_2$.*

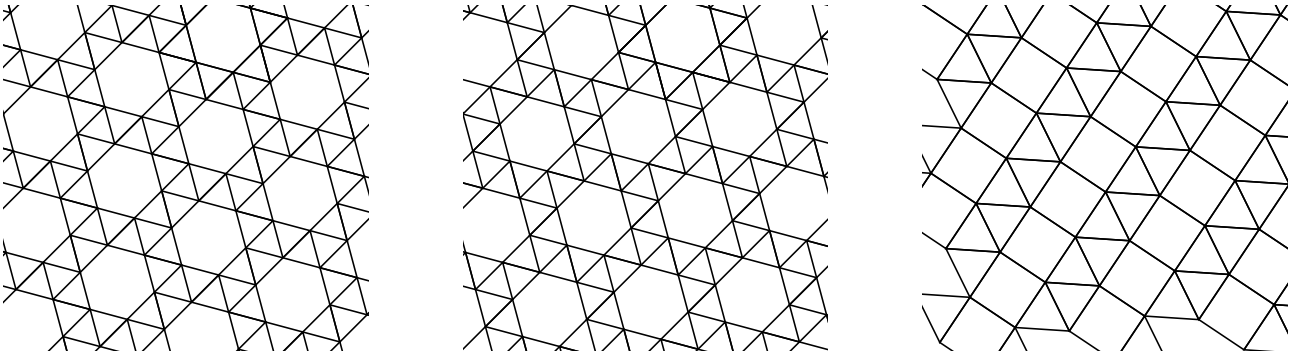
There are 11 types of Archimedean tilings of the Euclidean plane (see the Table). Each of the tilings gives rise to a 2-parameter family of vertex-transitive *toroidal maps*.

The vertex-transitive maps without one-sided and two-sided faces on the Klein bottle form 13 families corresponding in different ways to 6 out of the 11 vertex-transitive Euclidean tilings; each of them have "width 4" in the sense that all vertices belong to 4 straight lines parallel to the glide-reflection axis on the Klein bottle (Thomassen [Tho91], Babai [Bab91c]). In a similar sense, the degenerate cases have "width" 2 or 1 and are also known.

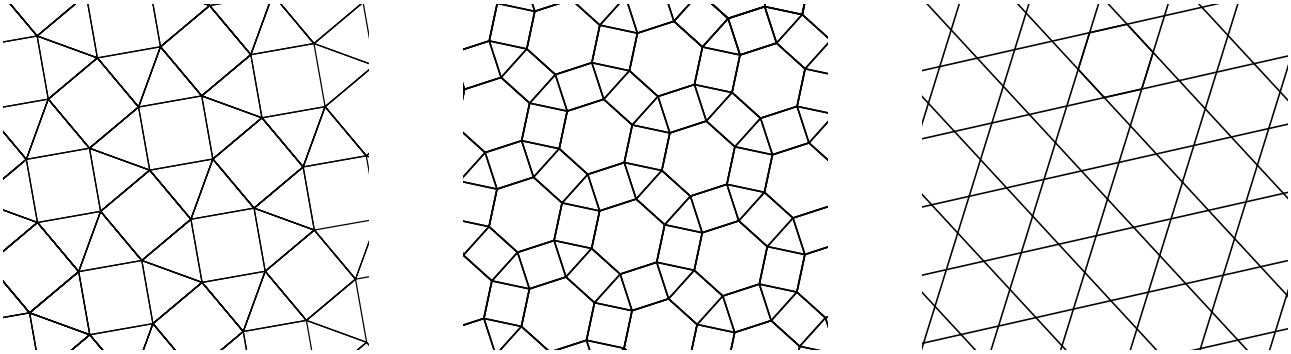
When $\chi(\Sigma) < 0$, the finite groups acting on Σ are quotients of discrete subgroups of $PGL(2, \mathbb{R})$, the isometry group of the hyperbolic plane. A classical theorem of Hurwitz (1893) indicates a drastic change compared to the case $\chi \geq 0$.



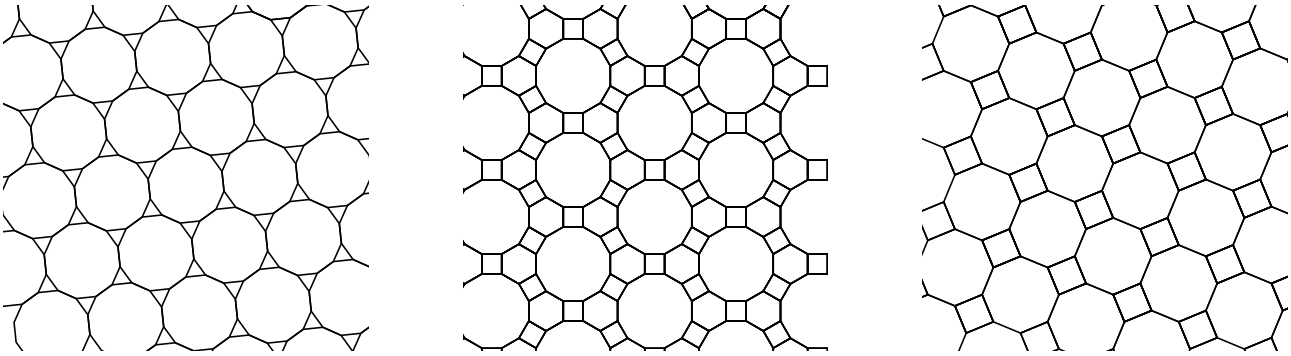
(3^6) (4^4) (6^3)



$(3^4.6)$ $(3^4.6)$ $(3^3.4^2)$



$(3^2.4.3.4)$ $(3.4.6.4)$ $(3.6.3.6)$



(3.12^2) $(4.6.12)$ (4.8^2)

Table: The eleven types of Archimedean tilings of the Euclidean plane (one of them shown in two mirror-symmetrical forms). After Grünbaum–Shephard [GS81, p.144].

THEOREM 3.51. (HURWITZ) *If the finite group G acts on the compact surface Σ of Euler characteristic $\chi < 0$ then $|G| \leq 84|\chi|$.*

For a proof when Σ is orientable, see e.g. [GT87, p.496]. The general case follows by the foregoing remarks. There are infinitely many values of χ where the bound $84|\chi|$ is attained (Conder [Con80]).

The following is a combinatorial generalization of Hurwitz's Theorem. With each vertex of a map we associate a cyclically ordered list containing the number of sides of each face incident with the vertex. We call a map *semiregular* if the cyclic list associated with each vertex is the same (up to inversion).

THEOREM 3.52. ([BAB91C]) *Let M be a semiregular map on a compact surface of Euler characteristic $\chi < 0$. Then M has at most $84|\chi|$ vertices.*

Each homeomorphism ψ of a compact orientable surface Σ of genus g induces an automorphism ψ_* of the first homology group $H_1(\Sigma) \cong \mathbb{Z}^{2g}$ which preserves a skew-symmetric bilinear form $H_1(\Sigma) \times H_1(\Sigma) \to \mathbb{Z}$, defined by the *intersection numbers* of curves, cf. [ZVC80, Prop. 3.6.3]. Another result of Hurwitz (1893) states that if ψ has finite order and $g \geq 2$ then $\psi_* \neq 1$. Consequently, if G is a finite group of homeomorphisms of Σ then G is isomorphic to a subgroup of $\mathrm{Sp}(g, \mathbb{Z})$, the group of $2g \times 2g$ integral symplectic matrices (cf. [ZVC80, Cor. 4.15.3], [Big72]). This result also holds for the homology groups mod n for any $n \geq 3$ (Serre 1960, cf. [ZVC80, Cor. 4.15.15]).

3.10 Embeddings on surfaces, minors

Note. All graphs and groups in this section are finite, except in the last paragraphs (beginning after Theorem 3.60).

Now we turn to the question of classifying the connected vertex transitive graphs embeddable on a given surface. If an embedding of the graph X on the surface Σ creates a map and all automorphisms of X extend to map-automorphisms then we call the embedding *automorphic*. The main difficulty is that embeddings are seldom automorphic. Some of the most surprising results in the area infer the existence of automorphic embeddings from seemingly unrelated asymptotic combinatorial assumptions.

Apart from cycles, vertex transitive graphs have degree ≥ 3 and are therefore 3-connected. For planar graphs this implies unique embeddability on the sphere, hence those embeddings are automorphic, and the list of 18 types plus two infinite one-parameter families mentioned above applies.

For no other surface Σ have the vertex-transitive graphs embeddable on Σ been fully classified. Interest in embedding Cayley graphs on surfaces has been motivated since the last century by the following observation: Cayley graph embeddings help in finding *presentations* (generators and relations) for G.

PROPOSITION 3.53. *Let $X = \Gamma(G, S)$ be embedded on Σ. Let the cycles $C_1, \ldots, C_m$ of X through 1 generate the fundamental group of Σ. Let further $D_1, \ldots, D_{f-1}$ denote all but*

one of the fundamental cycles (face boundaries) of the embedding. Then the C_i and the D_j, regarded as words in the symbols $S \cup S^{-1}$, form a complete set of relations defining G. — If the map is vertex-transitive, only those D_j passing through 1 have to be taken.

PROOF: Every cycle in the Cayley graph indicates a valid relation among the generators. We have to show that every cycle A represents a consequence of the relations listed. We may assume A passes through 1. Then A, as a path on Σ, is homotopic to some product P of the C_i. It follows that AP^{-1} is contractible and therefore representable as a product of the D_j. □

Maschke [Mas96] determined all planar minimal Cayley diagrams. (Recall that we call $\Gamma(G,S)$ and $\Gamma_c(G,S)$ *minimal* if S generates G with no redundant elements.) Nonplanar toroidal minimal Cayley diagrams have been classified by Proulx. Her list contains 11 infinite classes with two generators, 9 infinite classes with 3 generators, 1 infinite class with 4 generators, and 9 sporadic cases (8 with 2 generators, 1 with three). We state the main consequence.

THEOREM 3.54. (PROULX [PRO77]) *All but 3 of the groups admitting a toroidal but no planar Cayley graphs are quotient groups of Euclidean 2-dimensional crystallographic groups and therefore they actually admit automorphically embedded toroidal Cayley graphs.*

The precise set of 3 exceptions (of orders 24, 48 and 48) has been determined by Tucker [Tuc84]. Using in great detail Proulx's analysis, Tucker went on to proving an extension of Hurwitz's theorem to Cayley graphs embeddable on surfaces of negative Euler characteristic.

THEOREM 3.55. (TUCKER [TUC84]) *Let G be a group of order n and $\Gamma(G,S)$ a minimal Cayley graph of G, embeddable on a surface Σ of Euler characteristic $\chi < 0$ but not embeddable on the torus. Then $|G| \leq 84|\chi|$.*

We indicate some of the basic tricks of the Proulx-Tucker theory on a very simple special case.

PROPOSITION 3.56. *Let G be a group of order n where g.c.d. $(n,6) = 1$. Assume G has a minimal Cayley graph X embeddable on a surface Σ of Euler characteristic χ. If $n > -5\chi$, then G is Abelian with two generators and X is toroidal.*

PROOF: Let $X = \Gamma(G,S)$ have degree $d \geq 3$. Since G has no elements of order 3, the girth of G is ≥ 4. Now X has n vertices, $e = nd/2$ edges, and $f \leq nd/4$ faces. Substituting into the Euler equation 7 we obtain

$$n(1 - d/4) \geq \chi.$$

If $d \geq 5$, we infer $n \leq -4\chi$. If $d = 3$ then one of the generators would have to be an involution, impossible. The only remaining case is $d = 4$; hence $e = 2n$ and S consists of 2 elements: $S = \{a, b\}$.

Assume first that the girth of X is ≥ 5. Let f_i denote the number of i-sided faces. We then have $2e = \sum_{i\geq 5} if_i$ and $f = \sum_{i\geq 5} f_i \leq 2e/5 = 4n/5$. Hence

$$\chi = n - e + f \leq n - 2n + 4n/5 = -n/5.$$

We conclude that $n \leq -5\chi$, thus finishing this case.

We may henceforth assume that the girth of X is 4. By minimality, the implied relation of length 4 must be of one of the following types: (a) $a^4 = 1$; (b) $abab = 1$; (c) $aba^{-1}b = 1$; (d) $a^2b^2 = 1$; (e) $aba^{-1}b^{-1} = 1$.

Since G has odd order and S is minimal, only case (e) can actually occur. But then, G is Abelian with two generators, hence it is toroidal. □

While the arguments that count degrees and use the Euler equation generalize to arbitrary vertex transitive graphs, the "relation chasing" that concluded the proof has no analogue. Arguments of a more geometric flavor, however, yield the following.

THEOREM 3.57. (THOMASSEN [THO91], BABAI [BAB91C]) *There exists a function f such that every connected vertex transitive graph X with more than $f(\chi)$ vertices and embeddable on a surface of Euler characteristic χ admits an embedding as a vertex-transitive* map *on a surface of nonnegative Euler characteristic.*

The function f is bounded by $c|\chi|$ where c is an absolute constant ([Tho91]). With the exception of 4 families of "crossed stripe-like" graphs ([Bab91c]), the embeddings guaranteed by the theorem are *automorphic*.

Embeddings of specific Cayley graphs, in particular of complete graphs viewed as Cayley graphs of cyclic groups, have been studied extensively. The original motivation for this was the solution, due mainly to Ringel and Youngs [RY68], of the Heawood map color conjecture. (For details and references, we refer to the monograph of Gross and Tucker [GT87].) Subsequently, the following concept gained popularity.

DEFINITION 3.58. The *genus* of a (finite) group G is the minimum of the genera of those orientable compact surfaces Σ on which some connected Cayley graph of G is embeddable. The *non-orientable genus* of G is the minimum of $(2 - \chi(\Sigma))$ over the corresponding not necessarily orientable surfaces Σ.

Both the orientable and non-orientable genera are monotone for subgroups [Bab77a]. (This follows immediately from Prop. 3.59 below.) It is an open question whether or not the same holds for quotient groups, as conjectured by A. T. White [Whi73]. Jungerman and White were able to determine the precise genus for surprisingly large classes of abelian groups [JW80], demonstrating that those groups admit embeddings with quadrilateral faces. The situation becomes more complicated when $\mathbb{Z}_3$ factors are present and triangular faces may arise.

Contractions tend to simplify the topological characteristics of a graph. Significantly, they can be related to group actions.

PROPOSITION 3.59. (THE "CONTRACTION LEMMA") *If the group G acts semiregularly on the connected graph X then X has a contraction to some Cayley graph of G. In particular, if $G \leq H$ then every Cayley graph of H has a contraction to some Cayley graph of G* ([Bab73],[Ser77]).

(Semiregular action means that the stabilizer of every vertex is the identity.) An immediate consequence is the Nielsen-Schreier Theorem that subgroups of free groups are free.

The *Hadwiger number* of a (not necessarily finite) graph X is the supremum of those values k such that some component of X has a contraction onto K_k. The Hadwiger number of graphs embeddable on a fixed surface is bounded (e. g. for the torus, this bound is 7). The converse does not hold. Nonetheless, one can give an asymptotic classification of all finite vertex-transitive graphs with bounded Hadwiger numbers.

THEOREM 3.60. ([BAB]) *There exists a function f such that every finite connected vertex-transitive graph X of Hadwiger number $\leq k$ is either* (a) *toroidal, admitting an automorphic embedding on the torus, or* (b) *ring-like in the following sense: $V(X)$ has a partition $(V_0, \ldots, V_{m-1})$ into blocks of imprimitivity such that* (b1) $|V_i| < f(k)$; (b2) *if there is an edge between V_i and V_j then $|i-j| < f(k)$ or $m - |i-j| < f(k)$;* (b3) *the action of* $\mathrm{Aut}X$ *on the set of blocks is either cyclic or dihedral.*

The proof requires the study of the *local structure* of the graphs via an infinite vertex-transitive "limit graph" (cf. [Bab91c]) and distinguishes cases according to the number of *ends* of the limit graph, using Prop. 3.31. The case of infinitely many ends is disposed of using a sphere packing argument ([Bab91c]) motivated by Thomassen's proof that graphs of degree ≥ 3 and large girth have large Hadwiger number ([Tho83])

The case of two ends yields ring-like graphs, using Dunwoody's Theorem 3.37. The hard case is when the limit has a single end. The analysis requires the following result.

THEOREM 3.61. ([THO92]) *Let X be an infinite locally finite connected vertex-transitive graph with a single end. If X has finite Hadwiger number then X is planar.*

Such an infinite graph, then, can be shown to have a natural associated geometry (along the lines of Thm. 3.49, cf. [Bab]):

THEOREM 3.62. *Let X be an infinite locally finite connected vertex-transitive planar graph with a single end. Then X has an automorphic embedding as a tiling of the Euclidean or hyperbolic plane.*

Returning to the sketch of the proof of Theorem 3.60, we observe that Euclidean tilings give rise to toroidal graphs. Hyperbolic tilings lead to finite graphs of large Hadwiger number, via another sphere packing argument, using the elements of hyperbolic geometry.

3.11 Combinatorial group theory

Combinatorial group theory investigates presentations of groups defined in terms of generators and relations. Typical constructions in this field are the free product with amalgams, and HNN-extensions (cf. Section 3.7). One of the classical results is the Nielsen-Schreier theorem that *every subgroup of a free group is free.* This, incidentally, follows immediately from the Contraction Lemma (Prop. 3.59). Indeed, among the groups with no elements of order 2, precisely the free groups have trees for Cayley graphs; and a contraction of a tree is a tree again.

There is no way we could do justice to this vast area in a tiny amount of space like this; the reader is referred to the monographs by Coxeter-Moser [CM72], Magnus-Karrass-Solitar [MKS66], Lyndon-Schupp [LS77], Serre [Ser80], Dicks-Dunwoody [DD89]. The elementary graph theoretic approach to classical subgroup theorems is emphasized in Imrich's friendly notes [Imr77]. When proving subgroup theorems such as Kurosh's theorem stated at the end of this section, the basic geometric object to consider is the factor of a Cayley diagram of the group G by the action of the subgroup H (Schreier coset diagram). An example of an interesting result in this area proved by an elementary graph theoretic argument is *Howson's theorem:* the intersection of two finitely generated subgroups of a free group is finitely generated [Imr77], [DD89, I.8], [Tar92].

Some of the results mentioned earlier in this chapter belong to Combinatorial Group Theory (e.g. Proposition 3.53 or Dunwoody's Theorem 3.36).

A relatively recent highlight is the *Bass-Serre theory*, the basic technique of which is group actions on trees. They introduce a construction called a *graph of groups* in which a group $G(v)$ is assigned to each vertex v of a directed graph and a subgroup $G(v,w) \leq G(v)$ to every directed edge (v,w), along with an injective homomorphism $t_{v,w} : G(v,w) \to G(w)$. The *fundamental group* of a graph of groups is defined as a group generated by the disjoint union of the $G(v)$ along with one symbol $t_{v,w}$ for every edge (v,w), subject to the relations defining $G(v)$ for each v, and the relations $t_{v,w}^{-1} g t_{v,w} = g^{t_{v,w}}$ for each edge (v,w) and element $g \in G(v,w)$. (Note that therefore $g \in G(v)$ and $g^{t_{v,w}} \in G(w)$.) Moreover, we select an arbitrary maximal subtree of the graph, and set $t_{v,w} = 1$ for every edge (v,w) in the tree.

Observe that if the graph consists of a single directed edge (v,w) then the fundamental group will be the free product of $G(v)$ and $G(w)$, with the subgroup $G(v,w)$ amalgamated. If the graph has a single vertex v with a loop (v,v) then the fundamental group is the HNN extension $(G(v), G(v,v), t_{v,v})$. This is a restatement of Theorems 3.34 and 3.35.

Let now G be a group acting on a tree T without inverting edges. Then the *Bass-Serre structure theorem* asserts that G is isomorphic to the fundamental group of a graph of groups, where the graph is the factor graph of T by the action of G [Ser80, Sec. I.5.4], [DD89, Sec. I.4].

Among the immediate consequences is Kurosh's classical subgroup theorem, asserting that a subgroup of a free product of the groups G_i is a free product of a free group and conjugates of subgroups of the G_i.

3.12 Eigenvalues

Let $\alpha : G \to \mathbb{C}$ be a function, and consider the $n \times n$ matrix $A = (a_{g,h})$, whose rows as well as columns are labeled by the elements of G (in the same order, $n = |G|$), and

$$a_{g,h} = \alpha(gh^{-1}).$$

We can think of α as a "color assignment" to the elements of G; thus A is the adjacency matrix of a Cayley color diagram. We call A a G-circulant, since in the case $G = \mathbb{Z}_n$ we obtain precisely the circulant matrices.

In the circulant case, $\det A$ has a well known expansion into linear factors. Let ω denote a primitive n^{th} root of unity; then the vectors $w_i = (1, \omega^i, \omega^{2i}, \ldots, \omega^{(n-1)i})$ form a system of orthogonal eigenvectors of A, with corresponding eigenvalues

$$\lambda_i = \sum_k \alpha(k)\omega^{ik}. \tag{8}$$

The determinant of A is $\prod_i \lambda_i$.

Examining the expansion of $\det A$ for the dihedral groups, Dedekind noticed that (viewing each value $\alpha(g)$ as an independent variable), most irreducible factors were no longer linear but quadratic, and called on Frobenius in a letter to investigate the general case. Frobenius soon found a wealth of structure; his paper "Über die Primfactoren der Gruppendeterminante", presented to the Prussian Academy of Sciences in 1896, laid the foundations of character theory for nonabelian groups.

A consequence of this theory is, that, denoting the dimensions of the irreducible characters of G by $n_1, \ldots, n_h$ (h is the number of conjugacy classes in G; and $\sum n_i^2 = n$), the eigenvalues of any G-circulant can be assigned to irreducible characters in the following way: n_i^2 eigenvalues correspond to character χ_i; these fall into n_i equal groups, and all the n_i eigenvalues within a group are equal. Moreover, the sum of the potentially different n_i eigenvalues (one from each group of n_i) belonging to χ_i is

$$\lambda_{i,1} + \ldots + \lambda_{i,n_i} = \sum_{g \in G} \alpha(g)\chi_i(g). \tag{9}$$

(See [Bab79d].) In particular, if G is abelian, then each $n_i = 1$, and the expression simplifies to

$$\lambda_i = \sum_{g \in G} \alpha(g)\chi_i(g), \tag{10}$$

a direct generalization of the circulant case (eqn. (8)).

As an example, let $X = X(n, k)$ denote the distance-k graph of the n-dimensional cube. Let A be an n-set and let us represent the elements of the n-cube by subsets of A. With the operation of symmetric difference, this set is the elementary abelian group $\mathbb{Z}_2^n$ and $X = \Gamma(\mathbb{Z}_2^n, S_k)$ where S_k is the set of all k-subsets of A. Characters $\chi_T : \mathbb{Z}_2^n \to \{\pm 1\}$ are associated with subsets $T \subseteq A$ via the rule $\chi_T(B) = (-1)^{|T \cap B|}$. The corresponding eigenvalue of X is $\lambda_T = \sum_{|B|=k} (-1)^{|T \cap B|} = K_k(|T|)$, where

$$K_k(x) = \sum_{i=0}^{k} (-1)^i \binom{x}{i} \binom{n-x}{k-i} \tag{11}$$

is the Krawtchouk polynomial (cf. [BI84, Sec.3.2]).

A more general class of G-circulants, admitting an explicit expression of their eigenvalues, are obtained when α is a *class function*, i.e. α is constant on conjugacy classes. (In other words, $\alpha(gh) = \alpha(hg)$ for every $g, h \in G$.) In this case all the n_i^2 eigenvalues belonging to χ_i are equal, and hence their common value is $\lambda_i = (1/n_i) \sum_{g \in G} \alpha(g)\chi_i(g)$ and the matrix A is diagonalizable (via a unitary transformation).

It follows from the above that if the set S of generators is closed under conjugation then the adjacency matrix of the Cayley digraph $\vec{\Gamma}(G, S)$ is diagonalizable. This is not true for general S; Godsil [God82] has shown that the minimal polynomial of any integral matrix divides the minimal polynomial of some Cayley digraph.

Cayley graphs of cyclic groups of prime order are determined up to isomorphism by their characteristic polynomials (Elspas, Turner [ET70]). This is not true for general groups; families of isospectral Cayley graphs of the dihedral groups of all odd prime degrees are exhibited in [Bab79d].

The results discussed above belong to the *harmonic analysis* over G. For an exposition and a variety of applications (especially to random walks) of the formulas given, see Diaconis [Dia88, Ch. 3], [Dia89]; Chillag [Chi88].

For the extensive literature on the harmonic analysis over locally finite infinite graphs we refer to the survey [MW89].

4 The representation problem

The material of this section is covered in greater detail in the survey paper [Bab81b] where additional references and in many cases complete proofs can be found.

4.1 Abstract representation; prescribed properties

In this section we consider the following type of problem: given a group G find a graph X (or a block design, a lattice, a ring, etc.) such that the automorphism group $\mathrm{Aut}(X)$ is *isomorphic* to G. Such an object X will be said to *represent* the group G. A class $\mathcal{C}$ of objects is said to represent a class $\mathcal{G}$ of groups if, given $G \in \mathcal{G}$ there exists $X \in \mathcal{C}$ such that $\mathrm{Aut}(X) \cong G$. We call $\mathcal{C}$ *universal*, if every group is represented by $\mathcal{C}$. We say that $\mathcal{C}$ is *finitely universal* if every finite group occurs among the groups represented by *finite* members of $\mathcal{C}$.

The natural question, which groups are represented by graphs, was stated by König [Kön36, p.5], and soon answered by Frucht:

THEOREM 4.1. ([FRU38]) *Given a finite group G there exists a finite graph X such that $\mathrm{Aut}(X) \cong G$. In other words, graphs are finitely universal.*

Frucht's proof has been reproduced in several texts [Ore62], [Har69], [Lov79a], [Bol79]. The idea is (i) to observe that the automorphism group of the (colored, directed) Cayley diagram of G with respect to any set of generators is isomorphic to G; (ii) to get rid of colors and orientation by replacing colored arrows by appropriate small asymmetric (automorphism free) gadgets.

The next problem was to find subclasses of graphs and classes of other (combinatorial, algebraic, topological) objects that are universal. This direction was initiated by Frucht and Birkhoff. Frucht proved that *trivalent graphs are finitely universal* [Fru49]. It is immediate from Theorem 4.1 that posets are finitely universal. Since posets are strongly reconstructible from their lattice of ideals (as the poset of join-irreducible elements), it follows that *distributive lattices are finitely universal* (as well as universal, Birkhoff [Bir45]). (Cf. [Bab81b] for proofs and further references.)

These results already foreshadow the lopsidedness of later developments. Take almost any "reasonably broad" class of combinatorial or algebraic structures; the class will be universal. (Groups, planar graphs are notable exceptions.) This "universality phenomenon" was first indicated by Sabidussi [Sab57]; he proved that Hamiltonicity, k-regularity, k-connectedness are all compatible with any prescribed automorphism group. Universality results in topology and algebra were inspired by de Groot's papers [Gro58], [Gro59], where topological spaces and commutative rings were shown to be universal. A surprisingly strong version of the latter result was given by E. Fried and J. Kollár:

THEOREM 4.2. (FRIED, KOLLÁR [FK78],[FK81]) *Every group is the automorphism group of a field. Every finite group is the automorphism group of an algebraic number field.*

(Algebraic number fields are finite extensions of $\mathbb{Q}$.) The proof takes a graph X with the given automorphism group and encodes it into a field (not without ingenuity). This is the basic scheme of most universality proofs.

The extensions constructed by Fried and Kollár are not normal. Therefore their result does not bear on the inverse problem of Galois theory (represent a given group as a Galois group over a given field; notably, over $\mathbb{Q}$). We note in passing that the inverse problem has had its renaissance in the past decade, inspired by J. G. Thompson's new approach [Tho84] (cf. Feit [Fei89], Matzat [Mat87], several articles in [A$^+$85]). One of Thompson's corollaries states that the Monster, the largest sporadic simple group, is a Galois group over $\mathbb{Q}$.

Of the numerous combinatorial universality results, let me quote two of the more surprising ones.

THEOREM 4.3. (E. MENDELSOHN [MEN78B], [MEN78A]) *Every finite group is the automorphism group of* (a) *a Steiner triple system and a Steiner quadruple system;* (b) *a strongly regular graph.*

Universality proofs usually require *reconstruction arguments*. To illustrate this point, we deduce Mendelsohn's result (b) from (a). Let X be a Steiner triple system with the prescribed automorphism group G. Take its line graph $L(X)$. $L(X)$ is strongly regular, and, according to Theorem 1.12, X is strongly reconstructible from $L(X)$, assuming X has > 15 vertices. In particular, $\mathrm{Aut}(X) \cong \mathrm{Aut}(L(X))$ (Cor. 1.13(a)). □

The automorphism group is very sensitive to slight changes in the graph. It is known, for instance, that for any pair of groups G and H there exists a graph X and an edge $e \in E(X)$ such that $\mathrm{Aut}(X) \cong G$ and $\mathrm{Aut}(X \setminus e) \cong H$ (Babai, see [Lov79a, Ex.12.11]).

It is typical for universality proofs that the group structure plays little role. The extent to which group structure can be ignored is demonstrated by generalizations to prescribability of semigroups of *endomorphisms* and even categories, pioneered by the Prague category theory school, especially Pultr and Hedrlín. A *homomorphism* of the graph X to the graph Y is an adjacency preserving map $V(X) \to V(Y)$. Note that non-adjacent vertices may have the same image. *Endomorphisms* of a graph X are homomorphisms $X \to X$. They form the monoid $\mathrm{End}(X)$. (Monoid = semigroup with identity.) The basic result is that *every monoid is the endomorphism monoid of some graph* (finite graphs for finite monoids) (Hedrlín, Pultr, Vopeňka). By encoding graphs, many classes of algebraic and topological structures have been shown to have the same property (see the monograph by Pultr and Trnková [PT80]). A nice introduction to the subject is [HL69].

Universality-type results are known for some classes of structures that are clearly not universal.

THEOREM 4.4. (a) *The automorphism groups of (finite) tournaments have odd order; and every finite group of odd order is represented by a tournament* ([Moo64]).

(b) *G is the automorphism group of a switching class of tournaments if and only if its Sylow 2-subgroups are cyclic or dihedral* ([BCa]). (Two tournaments T_1, T_2 on the common vertex set V are switching equivalent if V can be partitioned into two classes such that one obtains T_2 from T_1 by reversing all edges between the two classes. This equivalence relation divides the set of tournaments on V into switching classes.)

(c) *Denote by Γ_d the class of groups G with a subgroup chain $G = G_0 \geq G_1 \geq \ldots \geq G_m = 1$ such that $|G_{i-1} : G_i| \leq d$ for every i. If X is a connected regular graph of degree $d+1$ then the stabilizer of an edge in X belongs to Γ_d; and every group in Γ_d can be represented this way* ([BL73a]).

It is an open problem to show that the *finite projective planes are not finitely universal*, i.e., not every group is isomorphic to the automorphism group of a finite projective plane. Indeed it seems plausible that most finite groups cannot act on a finite projective plane (as a subgroup of the automorphism group), but no group has been ruled out so far. C. Hering [Her67] proved that for $n \equiv 3 \pmod 4$, any 2-group acting on a projective plane of order n must be cyclic, a (generalized) quaternion group, a dihedral group, or a quasidihedral group.

4.2 Topological properties

Topological properties of a graph (embeddability on a surface, excluded minors) do restrict the abstract group of automorphisms and thus offer a welcome source of connections between the structure of groups and the graphs representing them. The following general non-universality result says that prescribed automorphism groups force arbitrary minors to occur.

THEOREM 4.5. (BABAI [BAB74A]) *Given a finite graph Y there exists a finite group G such that every graph X with $\mathrm{Aut}(X) \cong G$ has Y as a minor.*

Let $\mathcal{C}(Y)$ be the class of finite graphs without Y as a minor. It is expected that the finite groups represented by $\mathcal{C}(Y)$ have a very restricted structure. In particular, it is conjectured that the list of nonabelian finite simple groups represented by $\mathcal{C}(Y)$ is finite (cf. [Bab81b]).

Excluding a *topological subgraph* is, in general, less restrictive than excluding a minor; indeed even the exclusion of vertices of degree ≥ 4 does not restrict the abstract automorphism group. However, prescribed endomorphism monoids do force arbitrary topological subgraphs: another strong non-universality result.

THEOREM 4.6. (BABAI, PULTR [BP80]) *Given a finite graph Y there exists a finite monoid M such that for every graph X, if $\mathrm{End}(X) \cong M$ then X contains a subdivision of Y.*

4.3 Small graphs with given group

The number of orbits is a measure of symmetry. It is natural to ask, how symmetrical the graphs representing a given group can be. When talking about the *orbits of a graph*, we mean the orbits of its automorphism group on the vertex set. Edge-orbits are orbits on the edge set.

With three exceptions, every finite group can be represented by a graph with ≤ 2 orbits ([Bab74b]). (The exceptions are the cyclic groups of orders 3, 4, and 5.)

Most groups even admit a *representation by a vertex-transitive graph.* Nowitz [Now68] and Watkins [Wat71] described an infinite family of groups without a vertex-transitive representation (abelian groups of exponent greater than 2, and generalized dicyclic groups). Hetzel [Het76] and Godsil [God81a] proved that apart from these, there is only a finite number of additional exceptions, each of order ≤ 32. Godsil extended this result to finitely generated infinite groups [God79].

A *graphical regular representation* (GRR) of a group G is a graph X such that $\mathrm{Aut}(G)$ is regular and isomorphic to G. In other words, X is a Cayley graph of G without "extra" automorphisms (all automorphisms correspond to right translations, cf. Sec. 3.1).

The graphs Hetzel and Godsil construct are actually GRR's and the result stated contitutes the full solution of the GRR problem: the characterization of all finite groups which admit a GRR. For certain classes of groups G, including all nonabelian nilpotent groups of odd order, one can actually show that *almost all Cayley graphs of G are GRR's* ([BG82]). (To obtain a random Cayley graph $\Gamma(G, S)$, one chooses a symmetrical set $S = S^{-1} \subseteq G$ at random.)

The analogous problem for digraphs is easier: with 5 exceptions, all groups (finite or infinite) have a *digraphical regular representation* [Bab80a], [Bab78c]. (The exceptions are the elementary abelian groups of orders 4, 8, 9, 16, and the quaternion group of order 8. For infinite groups, the proof employs infinite Ramsey theory, cf. Chap. 42.) A consequence is that every infinite group can be represented by a graph X with 3 orbits.

The situation is quite different when we wish to minimize the number of *edge-orbits*. First of all, if X is a graph representing the group G with a *semiregular* automorphism group (as has been the case so far in this section as well as in most constructions related to Sec. 4.1) then the number of edges of X is at least $nd/2$, where $n = |G|$ and d is the

minimum size of a symmetrical set of generators. (This is a consequence of the Contraction Lemma 3.59.)

Let $e(G)$ denote the *minimum number of edges* and $m_e(G)$ the *minimum number of edge orbits* of the graphs representing G. Clearly $e(G)/|G| \leq m_e(G)$ and it is easy to see that $m_e(G) < C \log |G|$. Two natural questions arise: (a) is $m_e(G)$ bounded? (b) Is $e(G)/|G|$ bounded? – We now have a fairly complete answer to both questions.

THEOREM 4.7. (a)[BG91] *For all finite groups,* $e(G)/|G| < 500$. (b)[BGL91] *If a finite group is generated by* k *abelian subgroups then* $m_e(G) \leq Ck$ *for some absolute constant* C. *(Note that e.g. any direct product of finite simple groups is generated by* $k = 2$ *abelian subgroups.)* (c)(GOODMAN [Goo93]) *There is a constant* $c > 0$ *such that for infinitely many finite groups* G, $m_e(G) > c\sqrt{\log |G|}$. (d)(S. THOMAS [Tho87]) *Assuming the Generalized Continuum Hypothesis, for every successor cardinal* κ *there exists a group* G *of order* κ *such that* $m_e(G) = \kappa$.

The proof of (b) is related to a generalization of a result of Gel'fand and Ponomarev [GP70] that the *subspace lattice* of a vector space of finite dimension ≥ 3 over a prime field *is generated by 4 subspaces*. The proof of (c) has a curious nonconstructive element: certain p-groups of class two, demonstrating the lower bound, are shown to exist by a probabilistic (counting) argument. No explicit family of finite groups with unbounded $m_e(G)$ is known. The groups required for the proof of (d) are *Jónsson groups*, i.e. groups having no proper subgroups of their own cardinality. Shelah proved the existence of such groups for successor cardinals under G.C.H. [She80]. Without G.C.H., no proof is known of the conjecture that $m_e(G)$ can be an arbitrarily large cardinal. □

Some classes of groups are represented by drastically smaller graphs. This is clear for the symmetric groups (graphs of order k represent the group of order $n = k!$), but less evident for the alternating groups (graphs of order $< 2^{k+1}$ represent the alternating group of order $k!/2$). M. Liebeck determines the *exact* minimum order of graphs representing the alternating group A_k for sufficiently large k [Lie83] (e.g. for $k \equiv 0, 1 \pmod 4$ he finds this minimum to be $2^k - k - 2$). (For small k, there are surprises, e.g. $A_8 \cong PSL(4, 2)$ is the automorphism group of a 30-vertex graph: the incidence graph of the projective geometry $PG(3, 2)$.) Liebeck also gives strong lower bounds for the minimum order of graphs representing 3 types of classical simple groups (linear, orthogonal, unitary).

We mention related *open problems.* Let G be a group of order n. It follows from part (a) of the above theorem that G can be represented by a lattice of size $O(n)$. Can G be represented (i) by a *lattice with a bounded number of orbits?* Can G be represented by a *polynomial size* ($n^{O(1)}$) (ii) Steiner triple system, (iii) strongly regular graph, (iv) modular lattice ? We conjecture the negative answer to (iv) but positive answers to (i), (ii), (iii).

4.4 The concrete representation problem, 2-closure

Let $G \leq \mathrm{Sym}(V)$ be a permutation group, acting on the set V. The set of graphs $X = (V, E)$ admitting G as a subgroup of $\mathrm{Aut}(X)$ is easily described; their number is 2^k where k is the number of orbits of the induced action of G on the set of $\binom{|V|}{2}$ pairs.

The *concrete representation problem* asks if $G = \mathrm{Aut}X$ for some graph (digraph, etc.) with vertex set V. This problem is very difficult in general, as the case of regular permutation groups (the GRR problem, Sec. 4.3) has demonstrated. But there is a simple necessary condition.

Let us consider the colored complete directed graph W with vertex set V obtained from G as follows. Two pairs of vertices receive the same color if and only if they belong to the same orbit of the induced action of G on $V \times V$. Vertex v receives the color of the pair (v, v). This is the *coherent configuration* corresponding to the group G. We define W^* to be the undirected version of W: unordered pairs receive colors.

We call $\mathrm{Aut}(W)$ the *2-closure* of G, and $\mathrm{Aut}(W^*)$ the 2^**-closure.* In other words, the 2-closure of G is the largest subgroup of $\mathrm{Sym}(V)$ with the same orbits on $V \times V$; and the 2^**-closure* the largest subgroup with the same orbits on points and unordered pairs.

The group G is *2-closed* if G is equal to its 2-closure; 2^*-closed groups are defined analogously. A group is 2-closed if and only if it is the automorphism group of a colored directed graph; and 2^*-closedness corresponds to colored undirected graphs. These are thus necessary (but not sufficient) conditions for the group to be the automorphism group of a digraph (graph).

All regular permutation groups are 2-closed. Not all of them are 2^*-closed; the exceptions are precisely the abelian groups of exponent greater than two and the generalized dicyclic groups ([Bab77b]).

For transitive permutation groups G, Godsil [God81b] gives further necessary conditions which for some class of nilpotent groups turn out also to be sufficient.

It is an interesting question, *how far the 2-closure* $\mathrm{cl}_2(G)$ *is from a group* G. Liebeck, Praeger, and Saxl [LPS88a] investigate this for the case when G is primitive and almost simple, i. e. $L \lhd G \leq \mathrm{Aut}(L)$ for some simple group L. If G is 2-transitive then $\mathrm{cl}_2(G) = \mathrm{Sym}(V)$; but the gap is much smaller in all other cases. Indeed [LPS88a] find that $\mathrm{cl}_2(G)$ *normalizes* G, with the exception of six sporadic cases (the largest degree occurring in a representation of degree 276 of the Mathieu group M_{24}) plus two surprising infinite families of unbounded ranks with socles $L = G_2(q)$ and $\Omega_7(q)$, resp.

The notion of 2-closure as a tool in the study of permutation groups was introduced by I. Schur, see H. Wielandt [Wie69].

A maximal, not doubly transitive subgroup of S_n is necessarily 2-closed. This observation was used by L. A.Kaluzhnin and M. H. Klin (1972) (cf. [KMF91]) to give elementary proofs of the maximality of several classes of primitive groups, including the induced action of S_m on k-tuples ($n = \binom{m}{k}$), with some restrictions on (m, k). (For a complete study of this question via the classification of finite simple groups, see [LPS87a].)

It is natural to ask which permutation groups arise as the automorphism groups of a hypergraph. If the sizes of the edges are not restricted, we have a nearly complete answer for primitive groups. Obviously, $A_n \neq \mathrm{Aut}(X)$ for any hypergraph X on n vertices. Apart from the alternating groups and an (unknown) finite family of other exceptions, *all primitive groups* G *occur as* $\mathrm{Aut}(X)$ *for some edge-transitive hypergraph* [BCb]. Exceptions include all set-transitive groups: the Frobenius group of order 20 ($n = 5$), $PGL(2, 5)$ ($n = 6$), $PGL(2, 8)$, $P\Gamma L(2, 8)$ ($n = 9$). Another exception is the Frobenius group of order 21 ($n = 7$).

5 High symmetry

As in the Introduction, we shall use the abbreviation CFSG to indicate the Classification of Finite Simple Groups. CFSG has played a decisive role in the recent development of some of the subjects to be discussed below; we shall try to indicate where this is the case.

5.1 Locally s-arc-transitive graphs

All graphs in this section will be assumed finite and *connected*.

Let $s \geq 1$. An *s-arc* starting at a vertex v_0 in a graph X is a sequence $(v_0, \ldots, v_s)$ of vertices such that v_{i-1} $(1 \leq i \leq s)$ and v_i are adjacent and $v_{i-1} \neq v_{i+1}$ $(1 \leq i \leq s-1)$. A group $G \leq \mathrm{Aut}(X)$ is *locally s-arc-transitive* on X if for every vertex v_0, the stabilizer of v_0 in G acts transitively on the s-arcs starting at v_0. If in addition G is vertex-transitive then G is *s-arc-transitive*. Otherwise X is clearly bipartite and G acts transitively on each color-class. For $s = 1$, s-arc-transitivity is the same as flag-transitivity.

X is called (locally) s-arc-transitive if the action of $\mathrm{Aut}(X)$ is (locally) s-arc-transitive. We shall always assume that X is not a cycle (which is s-arc-transitive for every s).

Having excluded the cycles, local s-arc-transitivity implies large girth: the girth must be $\geq 2s-2$. Hence in a locally s-arc-transitive graph, all s-arcs are paths.

For trivalent s-arc-transitive graphs, Tutte [Tut47] proved the astonishing result that s must be bounded: $s \leq 5$ (cf. [Big74, Ch. 18]). He showed that $s = 5$ is attained by a graph C_8 called an "8-cage", a trivalent graph of girth 8 with 1440 vertices; $\mathrm{Aut}(C_8) \cong \mathrm{Aut}(S_6)$ where S_6 is the symmetric group of degree 6 (cf. [Big74, p.125]). By the covering construction of Theorem 1.6 we infer that there are infinitely many trivalent 5-arc-transitive graphs.

Tutte's result was generalized to *locally* s-arc-transitive graphs in a remarkable self-contained 4-page paper by R. M. Weiss [Wei76b].

THEOREM 5.1. (R.M. WEISS) *Let G be a locally s-arc-transitive but not $(s+1)$-arc-transitive group acting on a trivalent graph. Then $s \leq 7$ and $s \neq 6$.*

The bound 7 is attained by the *12-cage* (Tits [Tit59, Appendix], cf. Benson, Gleason [Ben66]).

A group G is (locally) s-regular if G is (locally) s-arc-transitive and the stabilizer of each s-arc is the identity. This is a somewhat artificial concept except for degree 3 when it occurs naturally: a trivalent edge-transitive graph is locally s-regular for some s. Let G be a locally s-regular group on a trivalent graph, and G_v a vertex-stabilizer; then $|G_v| = 3 \cdot 2^s$, the number of s-arcs starting at v. Weiss's bound $s \leq 7$ thus implies that there is only a finite number of possibilities for the vertex stabilizer in a trivalent edge-transitive graph. These possibilities were classified by Tutte for the flag-transitive (and therefore s-regular) case.

For the edge-transitive (and therefore *locally* s-arc-transitive) case the object to be classified is the pair of vertex-stabilizers of an adjacent pair of vertices together with their intersection, $(G_u, G_v, G_u \cap G_v)$. D. M. Goldschmidt [Gol80] classified all these triples and found that there were precisely 15 of them. Goldschmidt's 30-page work is motivated

by the examples afforded by the (bipartite) incidence graphs of "buildings" associated with rank-2 BN pairs over $GF(2)$, occurring in the study of certain classes of groups of Lie type. Goldschmidt's "amalgam method" was the starting point of an important new theory [DGS85], used among others for some aspects of "revisionism", the study of finite simple groups without the use of CFSG.

Tutte's 1947 theorem was extended a third of a century later to s-arc-transitive graphs of arbitrary degree: R. M. Weiss showed, using heavy guns, that $s \leq 7$ *holds for s-arc-transitive graphs of arbitrary degree* [Wei81]. Noting that the stabilizer G_v of a vertex v in a locally 2-arc-transitive group G acts doubly transitively on the neighbors of v, he was able to invoke the *classification of the doubly transitive permutation groups*, available as a consequence of CFSG (cf. Chap. 12). Weiss proves that if $s \geq 4$ then the action of G_v on the set $X(v)$ of neighbors is either affine (has an elementary abelian normal subgroup; in particular the degree is a prime power), or it includes the linear fractional group $PSL(2, p^\alpha)$ as a normal subgroup in its action on the projective line of $|X(v)| = p^\alpha + 1$ points. Here either $s = 4$, or $p \leq 3$ and $s \leq 2p + 1$.

One of the key ingredients in much of the work on arc-transitive graphs was the following theorem, magically singling out a prime number, characteristic for the graph. The result is due to J. G. Thompson and H. Wielandt and was adapted by A. Gardiner [Gar73] in this context (cf. [BCN89, ch. 7.2]). For a subset $S \subseteq V(X)$, let $X^d(S)$ denote the set of vertices within distance d from S (so e.g. $X^0(S) = S$). We use $G_d(S)$ to denote the pointwise stabilizer of $X^d(S)$ in $G \leq \mathrm{Aut}(X)$.

THEOREM 5.2. *Let $G \leq \mathrm{Aut}(X)$ act vertex-transitively on the connected graph X which is not a cycle. Assume that the stabilizer G_v of each vertex v acts as a primitive group on the set of neighbors of v. Then there exists a prime p such that $G_1(e)$ is a p-group (possibly the identity) for every edge e of X.*

R. M. Weiss eliminated the condition of vertex-transitivity and proved that under this weaker assumption (which is implied by *local* 2-arc-transitivity) $G_2(v)$ is a p-group for some vertex v [Wei79].

No analog of Weiss's $s \leq 7$ bound is known for *locally* s-arc-transitive graphs of arbitrary degree. The significance of such an extension would be in its wider applicability which would include incidence graphs of geometries of high symmetry. Such an application of the following partial result of R. M. Weiss will be indicated in Theorem 5.5. We should stress that Weiss's proof is *elementary*.

THEOREM 5.3. *Let $G \leq \mathrm{Aut}(X)$ be a locally s-arc-transitive group acting on the connected graph X of girth g. Assume $s \geq 8$ and $g \leq 2s + 11$. Then $G_5(S) = 1$ for every arc S of length 14.*

5.2 Distance-transitive graphs

This is one of the deepest and most extensively studied areas. We refer to Biggs [Big74] for an introduction and to the recent monographs by Brouwer, Cohen, Neumaier [BCN89] and Bannai, Ito [BI84] for technical discussions. The techniques are partly combinatorial and

algebraic (adjacency algebras) and apply in greater generality to distance *regular* graphs (cf. Chap. 15, Sec. 4); partly group theoretic (both elementary and CFSG-dependent).

First we mention that the *infinite* distance-transitive graphs of finite degree have very simple structure. For $r, s \geq 2$, an *r-tree of s-cliques* is an infinite connected graph all of whose 2-connected blocks are s-cliques and each vertex belongs to exactly r of these cliques.

THEOREM 5.4. (MACPHERSON [MAC82]) *Every infinite distance-transitive graph of finite degree is an r-tree of s-cliques for some $r, s \geq 2$.*

Macpherson's proof is based on Dunwoody's theorem on cuts of graphs with more than one end (Theorem 3.37). (Cf. Ivanov's theorem below.) In constrast, a great variety of infinite distance-transitive graphs of infinite degree follows by Fraïssé's theorem (Theorem 5.8) (Cameron, cf. [BCN89, p.233]). Henceforth in this section we assume that our graphs are finite. (Exception: Theorem 5.6.)

Recently, a project aiming at the complete classification of all distance-transitive graphs was drawn up (see the survey by Praeger [Pra90]). There are two phases to this project: to classify vertex-primitive distance-transitive graphs; and to reduce the general case to these. The program of the first phase was layed out by Praeger, Saxl, Yokoyama [PSY87] who reduced the problem to cases when the automorphism group is either almost simple or affine (has an elementary abelian normal subgroup). As a result of combined efforts of Ivanov, van Bon, Cohen, Inglis, Liebeck, Praeger, Saxl and others, most of the resulting cases have been settled and this phase now approaches completion (cf. [Pra90] for references).

The second phase has not advanced nearly as far but its basic idea is classical.

A graph X of finite diameter d is *antipodal* if being at distance d is an equivalence relation among the vertices of X. Antipodal graphs X of diameter $d \geq 2$ are not vertex-primitive since $X^{(d)}$ is disconnected. (In $X^{(k)}$, two points are adjacent if they are at distance k in X.)

The study of distance transitive graphs can, in a sense, be reduced to the vertex-primitive case, by a result of D. H. Smith and N. J. Martinov which asserts that *a distance-transitive graph of degree ≥ 3 is either primitive, or bipartite, or antipodal.* (Cf. [BCN89, Ch. 4.2].) It follows that starting from a distance-transitive graph, two simple operations will eventually lead to a vertex-primitive one. If X is antipodal, we identify antipodes and obtain a distance-transitive graph *covered* by X. If X is bipartite then $X^{(2)}$ has two isomorphic components, both are distance-transitive (X is a *bipartite doubling* of these components). Bipartite doublings have been studied in a number of recent papers (see e.g. Hemmeter and Woldar [HW90]). Gardiner's 1974 paper [Gar74] initiated the study of antipodal covers. He showed in particular that the size of the antipodal equivalence class is not greater than the degree. Antipodal coverings of some classes were classified recently (see Liebler [Lie91], van Bon and Brouwer [BB87]).

One of the most remarkable general results in this area, predating the classification project indicated, is a classification of distance-transitive graphs by their degree. In 1974, Biggs and Smith [BS71] determined all distance-transitive trivalent distance-transitive

graphs (there are 12 of them). D. H. Smith went on to determining all tetravalent distance-transitive graphs [Smi74]. Mostly by work of A. A. Ivanov, A. V. Ivanov, and I. Faradjev [FII86, II88], all distance-transitive graphs of valency ≤ 13 are now known.

THEOREM 5.5. ([CPSS83], [CAM82]) *There are finitely many distance-transitive graphs of any given degree $d \geq 3$.*

For the primitive case, this is immediate from Sims's conjecture (Theorem 1.1, depending on CFSG). Cameron [Cam82] points out that the general case rapidly follows, observing that from a distance-transitive graph of degree $k \geq 3$ the two operations mentioned above (halving, antipodal quotients) lead to a primitive distance-transitive graph of valency $3 \leq k' \leq k(k-1)$ in at most two steps.

Remarkably, R. M. Weiss [Wei85b] found a proof of Theorem 5.5 avoiding the CFSG reference, based on one of his result on s-arc-transitive graphs (Theorem 5.3), combined with the following powerful elementary result of A. A. Ivanov.

A graph $X = (V, E)$ is *distance-regular* if parameters a_i, b_i, c_i exist such that for each vertex $v \in V$, every vertex at distance i from v has c_i, a_i, and b_i neighbors at distance $i-1, i$, and $i+1$ from v, resp. Distance-transitive graphs are clearly distance-regular. We consider the parameter $t = \sup\{i : (a_i, b_i, c_i) = (a_1, b_1, c_1)\}$. (It is clear that $g \leq 2t+3$ where g is the girth. If $g \geq 4$ then $(a_1, b_1, c_1) = (0, k-1, 1)$ and $2t+2 \leq g \leq 2t+3$.)

THEOREM 5.6. (IVANOV [IVA83]) *If a distance-regular graph has degree k then its diameter is $d \leq t \cdot 4^k$.*

This result is valid for infinite graphs as well, implying that in that case $t = \infty$, hence the graph is an r-tree of s-cliques for some $r, s \geq 2$, thus extending Macpherson's theorem to *distance-regular* graphs.

Returning to finite graphs, it is shown in [BCN89, p. 220] via Weiss's proof, that the diameter of a distance-transitive graph of degree k is $d \leq (k^6)!4^k$. In reality, $d \leq 8$ for $k = 3$, and $d \leq 2k-1$ in all known cases for $k \geq 4$.

We mention two more parameter bounds. Godsil [God88] proves that *if a distance-regular graph X has an eigenvalue of multiplicity $f \geq 3$ then either X is complete multipartite or X has diameter $d \leq 3f-4$ and degree $k \leq (f-1)(f+2)/2$.* The dodecahedron attains the diameter bound; the icosahedron attains the valency bound.

Using CFSG through the list of doubly transitive groups, Weiss [Wei85a] classifies the s-arc-transitive graphs of girth $g \leq 2s+2$ ($s \geq 4$). (Note that $g \geq 2s-2$ always; and $g \leq 2s+2$ holds for all distance-transitive graphs.) As a corollary, he finds *all distance-transitive graphs of degree $k \geq 3$ and girth $g \geq 9$.* In addition to the two largest trivalent distance-transitive graphs (the Biggs–Smith graph on 102 vertices ($g = 9$) and the Foster graph on 90 vertices ($g = 10$), he finds an infinite sequence of graphs with $g = 12$, the incidence graphs of the generalized hexagons of associated with the Chevalley groups $G_2(q)$, q a power of 3.

5.3 Homogeneity

In this section we consider a very strong symmetry constraint, the study of which has led to powerful applications of group theory to model theory. A deeper survey is Lachlan [Lac86]; [KLM89] is accessible to the reader less versed in model theory.

We shall consider finite and countably infinite graphs, digraphs, and other structures.

A graph X is *homogeneous* if every isomorphism between finite induced subgraphs extends to an automorphism of X. Homogeneous digraphs, hypergraphs, etc. are defined analogously. Clearly, the complement of a homogeneous graph is again homogeneous.

Gardiner [Gar76] showed that *the only finite homogeneous graphs are* $m \cdot K_n$ (the disjoint union of cliques of equal size), *their complements,* $L(K_{3,3})$*, and the pentagon.* The finite homogeneous tournaments are just the single point and $\vec{C}_3$ (the directed 3-cycle) (Woodrow [Woo79]). The list of finite homogeneous oriented graphs (digraphs with no 2-cycles) is the following: the single point, $\vec{C}_3$, $\vec{C}_3[\overline{K}_m]$ (lexicographic product, Sec. 2), $m \cdot \vec{C}_3$ (m copies of $\vec{C}_3$), $\vec{C}_4$, and finally the Cayley digraph of the quaternion group Q_8 with respect to the generating set $\{i, j, k\}$ in the usual notation (Lachlan).

Cameron [Cam80a] (cf. [CGS78]) and Gol'fand (unpublished) strengthened Gardiner's result considerably by relaxing the homogeneity condition. We call the graph X *k-homogeneous* if isomorphisms of subgraphs of $\leq k$ vertices extend to automorphisms.

THEOREM 5.7. (CAMERON, GOL'FAND) *If X is a 5-homogeneous finite graph then X appears on Gardiner's list; and therefore X is homogeneous.*

Actually, the result of Cameron and Gol'fand is even more general in that they replace the symmetry condition by a *regularity* condition: X is *k-regular* if any two isomorphic induced subgraphs of $\leq k$ vertices have the same number of common neighbors. Observe that "1-regularity" means X is regular; and "2-regularity" means X is strongly regular. These conditions do not imply the presense of any automorphisms and allow a great variety of examples. This fact is in a remarkable contrast with the situation for $k \geq 5$: *If the finite graph X is 5-regular then it appears on Gardiner's list* (Cameron, Gol'fand).

The following generalization allows us to bring graphs of diameter greater than 2 into the picture. Let us call a graph X *metrically k-transitive* if any distance preserving map between ordered k-tuples of vertices of X extends to an automorphism of X. Note that for $k = 1$ this is vertex-transitivity, and for $k = 2$ it is distance-transitivity. We also note that the neighborhood of a vertex in a metrically k-transitive graph is $(k-1)$-homogeneous. Building on this fact and on Theorem 5.7, Cameron *classifies all finite metrically 6-transitive graphs.* The connected ones are the complement of $m \cdot K_n$, $K_{n,n}$ with a perfect matching deleted, the cycles, $L(K_{3,3})$, the icosahedron, and the graph $J(6, 3)$ on 20 vertices identified with the set of 3-subsets of a 6-set; two vertices are adjacent if the corresponding 3-sets share two elements. It follows that these graphs are automatically metrically k-transitive for every k.

Now we turn to the *countably infinite* (countable for short) case. The best known example is the *Rado graph*, or "generic countable graph", characterized by the following property: given any two disjoint finite subsets A and B of the vertex set, there exists a vertex adjacent to all vertices in A but none in B. This property determines a unique

countable graph. The Rado graph contains all finite graphs as induced subgraphs. A countable random graph (each pair is adjacent with probability 1/2 independently) has probability 1 to be isomorphic to the Rado graph (Erdős–Rényi [ER63]).

In addition, for every m there exists a unique "generic countable graph without K_m subgraphs", $\mathcal{G}_m$. In this classification, the Rado graph is $\mathcal{G}_\infty$. Lachlan and Woodrow [LW80] show that the $\mathcal{G}_m$ $(3 \leq m \leq \infty)$ and their complements exhaust all nontrivial examples of countable homogeneous graphs; the trivial ones are disjoint unions of cliques of equal size and their complements.

The Rado graph has an obvious tournament analogue, the "generic tournament". Lachlan showed that there are only two other countable homogeneous tournaments: the dense linear order (the order-type of the rationals), and the dense circular order. The latter is defined by a countable dense set on the unit circle with no pairs of antipodal points; edges correspond to clockwise walks along the shorter of the two arcs joining a pair of points.

Homogeneous partial orders were classified by J. Schmerl [Sch79]; a countable number of them was found. In contrast to these results, Henson [Hen72] found continuum many nonisomorphic countable homogeneous oriented graphs. Notwithstanding, Cherlin [Che87] classified all the homogeneous oriented graphs.

Model theorist's interest in homogeneous structures dates back to a 1954 paper of Fraïssé [Fra54] linking homogeneity, categoricity, and quantifier elimination.

Let us consider a locally finite "language", i.e. a set L of relation symbols, each associated with a positive integer called the arity such that each arity occurs a finite number of times. An L-structure $\mathcal{M}$ is a set M endowed with a relation of appropriate arity for each symbol in L. (A k-ary relation is a subset of M^k. We allow the case $M = \emptyset$.) Graphs, digraphs correspond to the language of a single binary relation. Every subset of M induces a substructure. (We use the term "substructure" to mean induced substructure.) $\mathcal{M}$ is *homogeneous* if all isomorphisms of finite substructures extend to automorphisms of $\mathcal{M}$. The theory $\mathrm{Th}(\mathcal{M})$ consists of all first order sentences which are true in $\mathcal{M}$. The theories of homogeneous L-structures are precisely those which permit quantifier elimination (first order statements of the form $\varphi(u_1, \ldots, u_k)$ depend only on the substructure induced by $u_1, \ldots, u_k$).

Let $\mathcal{F}(\mathcal{M})$ be the class of structures isomorphic to finite substructures of $\mathcal{M}$. A class $\mathcal{C}$ of L-structures is *hereditary* if it is closed under taking substructures. $\mathcal{C}$ has the *amalgamation property* if, whenever $\mathcal{F}_0, \mathcal{F}_1, \mathcal{F}_2 \in \mathcal{C}$ and $g_i : F_0 \to F_i$ are embeddings (isomorphisms onto substructures) $(i = 1, 2)$, there exist $\mathcal{F}_3 \in \mathcal{C}$ and embeddings $f_i : F_i \to F_3$ $(i = 1, 2)$ such that $g_1 f_1 = g_2 f_2$. (Note especially that we allowed the case $F_0 = \emptyset$, thus taking care of what logicians call the "joint embedding property".) An isomorphism-closed class $\mathcal{C}$ of finite L-structures is called an *amalgamation class* if it is hereditary and has the amalgamation property.

THEOREM 5.8. (FRAÏSSÉ) *If $\mathcal{M}$ is a countable homogeneous L-structure, then $\mathcal{F}(\mathcal{M})$ is an amalgamation class. Conversely, every amalgamation class of finite L-structures is $\mathcal{F}(\mathcal{M})$ for a countable homogeneous L-structure $\mathcal{M}$, unique up to isomorphism.*

The construction of $\mathcal{M}$ in the second statement is a direct limit argument. Since the class of finite graphs without K_m is clearly an amalgamation class, the generic graphs $\mathcal{G}_m$ of the Lachlan–Woodrow theorem are uniquely determined.

A countable structure $\mathcal{M}$ is $\aleph_0$-*categorical* if (up to isomorphism) is the only countable model of its theory. *Every countable homogeneous structure is* $\aleph_0$-*categorical.* (The converse is false.) $\aleph_0$-categoricity depends solely on $\mathrm{Aut}\mathcal{M}$. The *k-types* of a structure $\mathcal{M}$ are the orbits of $\mathrm{Aut}(\mathcal{M})$ on M^k.

THEOREM 5.9. (RYLL-NARDZEWSKI, ENGELER, SVENONIUS) *A countable structure* $\mathcal{M}$ *is* $\aleph_0$*-categorical if and only if it has a finite number of* k*-types for every finite* k*.*

This result, in a sense, reduces the study of $\aleph_0$-categorical structures to the study of *oligomorphic permutation groups* (groups which have a finite number of orbits on k-sets for every k; see Chap. 12, Sec. 9.5, cf. [Cam90]). Oligomorphic groups are precisely the dense subgroups (w. r. to pointwise convergence) in the automorphism groups of $\aleph_0$-categorical structures over locally finite languages.

$\mathcal{N}$ is a *smooth substructure* of $\mathcal{M}$ if $\mathcal{N}$ is a substructure if (i) all automorphisms of $\mathcal{N}$ extend to $\mathcal{M}$; and (ii) for each k, two k-tuples $u, v \in N^k$ belong to the same k-type of $\mathcal{N}$ if and only if they belong to the same k-type of $\mathcal{M}$.

An $\aleph_0$-categorical L-structure is *smoothly approximable* if it is the union of a chain of finite smooth substructures. The "trivial examples" in the Lachlan–Woodrow theorem, i.e. the disjoint unions of complete graphs and their complements, are smoothly approximable. By Theorem 5.9, the approximating finite structures must have a bounded number of k-types for every fixed k.

In one of the most exciting developments in model theory recently, combined work of Cherlin, Lachlan, Harrington, Kantor, Liebeck, Macpherson, and Hrushovski [CL86, CHL85, KLM89, CH], heavily relying on CFSG, has led to the *classification of all finite L-structures with a bounded number of 5-types.* (The same magic number 5 as in Theorem 5.7.)

Let $\mathcal{C}(L, k)$ denote the class of L-structures with at most k 5-types. The final result is that $\mathcal{C}(L, k)$ can be decomposed into finitely many classes and each class has a simple dimension theory: a finite number of dimensions is identified, and each first order statement is equivalent to a Boolean combination of finiteness and exact value statements of each dimension. The dimensions can be varied essentially independently. Dimensions correspond to classes of Lie geometries; the classical examples of the latter are linear and projective spaces over finite fields, possibly with forms (symplectic, orthogonal, unitary), and Grassmannians over disjoint unions of these. Pure sets occur as degenerate examples. The ℓ^{th} Grassmannian over the geometry $\mathcal{G}$ is the orbit of an ℓ-dimensional subgeometry of $\mathcal{G}$ under $\mathrm{Aut}(\mathcal{G})$. (When $\mathcal{G}$ is the disjoint union of t pure sets each of size m, the ℓ^{th} Grassmannian is the association scheme defined by the natural action of $S_m \wr S_t$ on a set of size $n = \binom{m}{\ell}^t$.)

The proof uses full force of CFSG through the structure theory of primitive permutation groups (O'Nan–Scott Theorem, cf. Chap. 12), including recent work of Aschbacher and Liebeck on maximal subgroups of classical groups.

A corollary of this theory is that for every finite language L and every k, *membership in* $\mathcal{C}(L, k)$ *can be tested in polynomial time.*

Another curious corollary is the following. Let us say that the graph X has the m-*extension property* if for any two disjoint subsets A, B of the vertex set there exists a vertex

adjacent to all vertices in A but none in B, assuming $|A|+|B| \leq m$. (The Rado graph has this property for all m. Almost all graphs on n vertices have the m-extension property for $m = (1-\epsilon)\log_2 n$; and the Paley graph $P(q,2)$ (Sec. 1.1) for $m = (1/2-\epsilon)\log_2 q$ [Bol85, Ch. 13.2].)

COROLLARY 5.10. ([CH]) *If for every m, X_m is a finite graph with the m-extension property then the number of orbits of* $\mathrm{Aut}(X_m)$ *on 5-tuples of vertices is unbounded (as $m \to \infty$).*

It would be desirable to see a proof of this result which does not require CFSG.

A final note on higher cardinals: Kierstead and Nyikos [KN89] characterize those n-uniform hypergraphs of cardinality κ which have a finite number of isomorphism types of induced subhypergraphs of cardinality λ for some infinite $\lambda < \kappa$.

6 Graph isomorphism

Deciding whether or not two explicitly given finite algebraic or combinatorial structures are isomorphic is a long-standing unsolved question in the theory of computing. Since all such structures can be canonically encoded by polynomial-time computable graphs ([HP66], [Mil79]), it would suffice to solve it for graphs.

From a practical point of view, backtrack algorithms perform quite well. The leader in the trade is B. McKay's program "Nauty" [McK87]. However, in spite of considerable effort, the theoretical complexity status of graph isomorphism is still unresolved.

6.1 Complexity theoretic remarks

For basic concepts of computational complexity theory we refer to Chapter 29; see also [GJ79].

While "graph isomorphism" (the set of pairs of isomorphic graphs) clearly belongs to *NP*, it is not known to belong to *coNP*. In other words, it is not known whether or not for all pairs of nonisomorphic graphs, a short (polynomial length) proof of nonisomorphism exists. It is known, however, that nonisomorphism has bounded round interactive proofs [GMW86], a fact that puts "nonisomorphism" in the class *AM*, a randomized extension of *NP*. This is considered strong theoretical evidence against *NP*-completeness of "graph isomorphism"; if it were *NP*-complete, the "polynomial time hierarchy", a hierarchy of complexity classes between *P* and *PSPACE*, would collapse. For further references, see [BM88] (cf. Chapter 29).

6.2 Algorithmic results: summary of worst case bounds

The best current worst-case bound for a general graph isomorphism algorithm is $\exp\sqrt{cn\log n}$ for n-vertex graphs (Luks and Zemlyachenko, cf. [BL83]). For some special classes of graphs, substantially better results are available. For groups given by their multiplication tables, and for Steiner triple systems, $n^{O(\log n)}$ isomorphism tests easily follow from the

observation that these structures have generating sets of size $\leq \log n$. For *planar* graphs, ingenious use of stacks has resulted in a *linear time* isomorphism test (Hopcroft, Tarjan, Wong [HT72], [HW74]). Combinatorial methods in similar spirit yielded polynomial time isomorphism tests for graphs of bounded genus ($n^{O(g)}$ time for genus $g \geq 1$) [FM80]. Group theoretic methods led to polynomial time algorithms for graphs with colored vertices and bounded color-classes (isomorphisms preserve colors by definition) [Bab79c], for graphs with bounded multiplicity of eigenvalues [BGM82], and, with considerably deeper use of group theory, for graphs of bounded degree (Luks [Luk82]) ($n^{O(d)}$ time for graphs of degree $\leq d$ [BL83]; $O(n^3 \log n)$ time for trivalent graphs [GHL$^+$87]). As a consequence of Luks's methods, isomorphism of block designs (BIBD's) with bounded k and λ can be tested in time $n^{O(\log n)}$ [BL83] (k is the block size and there are λ blocks common to each pair of vertices); isomorphism of tournaments can be tested in time $n^{O(\log n)}$ [BL83]; and isomorphism of λ-planes (symmetric designs) with bounded λ in $n^{O(\log \log n)}$ time [BL83]. A common generalization of the polynomial time results for bounded degree and bounded genus was obtained by Miller [Mil83b], [Mil83a].

Luks's beautiful paper [Luk82] is the single most fundamental reading in the area. It introduces the profound links to group theory to be discussed in Section 6.6

6.3 Canonical forms

An algorithmic problem closely related to graph isomorphism is the problem of *complete invariants* and in particular of *canonical forms* of graphs. Let $\mathcal{K}$ denote a class of objects with an equivalence relation to be called "isomorphism". An *invariant* on $\mathcal{K}$ is a mapping f from $\mathcal{K}$ to some class $\mathcal{L}$ of objects such that whenever $X, Y \in \mathcal{K}$ are isomorphic, $f(X) = f(Y)$. We call f a *complete* invariant, if the converse also holds: $f(X) = f(Y)$ implies $X \cong Y$. If, in addition, $\mathcal{L} = \mathcal{K}$ and $f(X) \cong X$ for every $X \in \mathcal{K}$ then the complete invariant f is called a *canonical form* over $\mathcal{K}$; and $f(X)$ the canonical form of X. For graphs, a canonical form f assigns a labeling to the vertices, and this assignment is uniquely defined by f up to automorphisms of X. We call such a labeling canonical, although strictly speaking it is the coset of the automorphism group consisting of all the labelings corresponding to f which is canonical.

Clearly, if a canonical form for a class of objects is available, then isomorphism testing is accomplished by simply comparing the canonical forms. The converse is not known to be true, but in all classes listed above, canonical forms can be obtained within the same time bound as guaranteed for isomorphism testing (cf. [BL83]).

An important invariant of graphs is the characteristic polynomial of their adjacency matrix. This invariant fails to be complete (quite badly, cf. Cor. 1.14), as do all other known polynomial time computable invariants.

An example of a canonical form of a graph is the one which produces the lexicographically first adjacency matrix. While this is clearly a complete invariant, unfortunately it is NP-hard to compute (reduction from maximum clique).

6.4 Combinatorial heuristics: success and failure

Testing graph isomorphism is easily seen to be equivalent to determining the orbits of the automorphism group of a graph. It is therefore natural to try to find invariant colorings of the vertex set $V(X)$ (i.e. each color class should be a union of orbits of $\mathrm{Aut}(X)$), and refine the color partition in the hope that eventually we obtain the orbit partition. An ordered partition $(C_1, \ldots, C_m)$ of $V(X)$ into invariant color classes C_i can be refined in a simple way: with each vertex $v \in C_i$, we associate the list $(i, \beta_1, \ldots, \beta_m)$, where β_j denotes the number of neighbors of v in C_j. Now order these lists lexicographically; vertices with the same list receive the same color in the new coloring. (The first round colors the vertices by their degree.) Eventually the process stops at a *stable coloring*, characterized by the fact that for every i, j all vertices in C_i have the same number of neighbors in C_j.

Let $\mathcal{T}$ denote the class of graphs which are partitioned by this process into singletons. Clearly, these graph have no automorphisms other than the identity, and the refinement process results in a unique canonical labeling of the graphs belonging to $\mathcal{T}$.

This naive method is highly successful on average: all but an exponentially small fraction of the graphs on n vertices are partitioned into singletons *in the third round* (and thus in linear time) [BK79]. This is a constructive version of the Erdős-Rényi theorem that all but an exponentially small fraction of the graphs are asymmetric (Sec. 1.6).

Perhaps even more surprising is the result of Kučera [Kuč87] that a modified procedure yields a unique *canonical labeling of almost all trivalent graphs* (and of graphs of bounded degree) *in linear time.* One of the difficulties in handling regular graphs in linear time is how to achieve an initial coloring at all. Kučera achieves this by considering the shortest cycles.

If we allow more time, a simpler way would be to *individualize* a vertex, i.e. to assign a unique color to it, thereby creating a nontrivial initial coloring. Even if subsequent refinements lead to complete partitioning into singletons, we still have to repeat the procedure for every vertex, thereby losing a factor of n in time. One can also individualize a set of k vertices at once (giving each of them distinct colors), thereby increasing the running time by a factor of n^k.

This combination is shown in [Bab80b] and [Bab81c] to succeed for strongly regular graphs as well as for primitive coherent configurations with $k < 4\sqrt{n}\log n$ (see Chap. 41, Sec. 4).

A stronger refinement procedure was proposed in 1968 by Weisfeiler and Leman [Wei76a]: they suggested to color the set of ordered pairs of vertices. Given an ordered partition $V \times V = C_1 \times \cdots \times C_m$, into color classes C_i, we associate with each pair (u, v) of vertices the list $(i, \beta_{jk} : 1 \leq j, k \leq m)$, where $(u, v) \in C_i$ and β_{jk} counts those vertices w with $(u, w) \in C_j$ and $(w, v) \in C_k$. Now again order these lists lexicographically to obtain a refined coloring of $V \times V$. The initial coloring of $V \times V$ uses 3 colors: edges, non-edges, and the diagonal.

The class of graphs for which no refinement is obtained is the *strongly regular graphs.* In general, the stable partitions for the Weisfeiler-Leman procedure are precisely the *coherent configurations* (Chap. 15, Sec. 3).

One can generalize the Weisfeiler-Leman procedure to partitioning the set V^d of ordered d-tuples in an analogous way. The stable configuration obtained is canonical and the

question is, for what d is the resulting partition of the diagonal necessarily the orbit partition of the vertex set. Such a d would yield a canonical form computable in $O(n^{d+1})$ time.

The Cameron-Gol'fand theorem (Thm. 5.7) implies that for $d \geq 5$, at least one non-trivial partition occurs in all cases except for the unions of complete graphs of equal size and the complements thereof. The result of [Bab80b] mentioned above implies that $d = O(\sqrt{n} \log n)$ completely succeeds for strongly regular graphs.

Yet a surprising negative result of Cai, Fürer, Immermann [CFI92] dashed the hopes for a purely combinatorial isomorphism test in moderately exponential ($\exp(n^{1-c})$) time. They construct a *pair of nonisomorphic graphs which force $d = \Omega(n)$ in order for the Weisfeiler-Leman procedure for d-tuples to distinguish them.*

Their counterexample still leaves ample room for a combination of combinatorial and group theoretic methods to work. Their graphs are partitioned into vertex classes of size 4, and, as mentioned before, the simplest group theoretic method, based on [Bab79c], yields canonical forms for graphs with bounded color classes in polynomial time.

We should mention that the current best timing for isomorphism testing and canonical forms for general graphs, $\exp(O(\sqrt{n \log n}))$, is obtained by combining Luks's group theoretic method with a combinatorial trick of Zemlyachenko [ZKT85] (cf. [Bab81a]). Since Zemlyachenko's method does not apply for instance to 3-uniform hypergraphs, the best bound for isomorphism testing within this class is C^n (Luks, cf. [BL83]).

6.5 Reductions, isomorphism complete problems, Luks equivalence class

The graph isomorphism problem (ISO for short) is polynomial time equivalent to the isomorphism problem for directed, vertex and edge-colored graphs (isomorphisms preserve colors by definition), and more generally to explicit structures with a set of relations of arbitrary arities. This can be proven by the method of encoding colors into gadgets as in Frucht's theorem, cf. [HP66], [Mil79]. A number of restricted classes $\mathcal{C}$ are known to be *isomorphism complete*, i.e. ISO can be reduced to isomorphism within $\mathcal{C}$. These include commutative semigroups, k-connected regular bipartite graphs with or without Hamilton cycles, graphs with large girth and chromatic number, etc. Exceptions are those classes which are known to have subexponential ($\exp(n^{o(1)})$) isomorphism tests (groups, Latin squares, tournaments, polynomial time testable classes), as well as strongly regular graphs.

The following problems are also known to be equivalent to ISO (see Mathon [Mat79]). Given a graph, determine (i) the orbits of $\mathrm{Aut}(X)$; (ii) generators of $\mathrm{Aut}(X)$; (iii) (Babai-Mathon) the order of $\mathrm{Aut}(X)$.

Observe that (ii), if applied to the union of a pair of isomorphic connected graphs, yields an isomorphism.

E. M. Luks found another, related *equivalence class of group theoretic problems.* Let $G, H \leq \mathrm{Sym}(\Omega)$ be permutation groups given by a list of generators. The following problems are polynomial time equivalent: (a) find (generators for) $G \cap H$ *(group intersection);* (b) given an element $\sigma \in \mathrm{Sym}(\Omega)$, decide whether or not $G \cap H\sigma = \emptyset$ *(coset intersec-*

tion); (c) given a subset $A \subset \Omega$, find the *set-stabilizer* of A in G; (d) given $A \subset \Omega$ and $\sigma \in \mathrm{Sym}(\Omega)$, decide whether the set-stabilizer of A intersects the coset $G\sigma$; (e) given $\sigma, \tau \in \mathrm{Sym}(\Omega)$, decide whether or not σ belongs to the double coset $G\tau H$; (f) given $\tau \in G$, find the centralizer of τ in G; (g) given $\sigma, \tau \in G$, decide whether or not the centralizer of τ in $\mathrm{Sym}(\Omega)$ intersects $G\sigma$.

(Note that if "set-stabilizer" is replaced by "pointwise set stabilizer" in problems (c) and (d), they become polynomial time solvable.)

PROPOSITION 6.1. (LUKS) *ISO reduces to coset intersection in polynomial time.*

For simplicity we prove instead, how to reduce the determination of $\mathrm{Aut}(X)$ to group intersection. Let $X = (V, E)$ be a graph and let Ω be the set of unordered pairs from V. Let $G \leq \mathrm{Sym}(\Omega)$ denote the induced action of $\mathrm{Sym}(V)$ on pairs; and let $H = \mathrm{Sym}(E) \times \mathrm{Sym}(\Omega \setminus E) \leq \mathrm{Sym}(\Omega)$ be the set stabilizer of E in $\mathrm{Sym}(\Omega)$. Then obviously, the induced action of $\mathrm{Aut}(X)$ on Ω is $G \cap H$. $\square$

It is significant that there is strong theoretical evidence suggesting that the decision problems in the Luks equivalence class ((b), (d), (e), (g)) are *not NP*-complete ([GMW86], [BM88]). If any of these problems (and therefore each of them) were *NP*-complete, this would imply the collapse of the "polynomial time hierarchy" in complexity theory, just as *NP*-completeness of ISO would (cf. Sec. 6.1).

Even more significantly, subcases of ISO can be reduced to polynomial time solvable subcases of *coset intersection*, and thereby they become polynomial time solvable themselves. This is one of the fundamental observations in Luks's seminal paper [Luk82].

6.6 Groups with restricted composition factors

In this section, we sketch the proof of the main result of [Luk82].

THEOREM 6.2. (LUKS) *Isomorphism of graphs of bounded degree can be tested in polynomial time.*

Recall that we used Γ_d to denote the class of groups with a chain of subgroups $G = G_0 \geq \ldots \geq G_m = 1$ such that $|G_{i-1} : G_i| \leq d$. This is the class of groups which occurs as edge-stabilizers in connected graphs of degree $\leq (d+1)$ (Theorem 4.4 (c)).

Using the trivial direction of this characterization, Luks reduced isomorphism of graphs of degree $\leq (d+1)$ to set stabilizers within a coset $G\sigma$ ($G \leq \mathrm{Sym}(\Omega)$, $\sigma \in \mathrm{Sym}(\Omega)$), where $G \in \Gamma_d$ and G is given by a list of generators. Next, he solved the latter problem in polynomial time, inventing a permutation group version of the classical algorithmic technique of "divide and conquer". The idea is to solve the problem one orbit at a time, reducing to a sub-coset in each round. For transitive G, we break G into blocks of imprimitivity; let N be the stabilizer of a system of maximal blocks. Now G/N acts as a primitive group on the blocks. $G\sigma$ is the union of $|G/N|$ cosets of N, and we solve the problem separately inside each coset. Formally, fix $A \subseteq \Omega$, and for any G-invariant set $B \subseteq \Omega$ let $\mathcal{C}(B, G\sigma) = \{\pi \in G\sigma : (A \cap B)^\pi = A \cap B\}$. This set is either empty or a coset of a subgroup of G. The identity $\mathcal{C}(B_1 \cup B_2, G\sigma) = \mathcal{C}(B_1, \mathcal{C}(B_2, G\sigma))$ is used to reduce to

the transitive case. For $H \leq G$ we have $G = \bigcup_i H\tau_i$ and thus $\mathcal{C}(B, G\sigma) = \bigcup \mathcal{C}(B, H\tau_i\sigma)$; this can be used to reduce the imprimitive case ($H = N$).

The algorithm runs in polynomial time because of the following result. It is easy to see that Γ_d can be characterized as the class of groups of which each composition factor is a subgroup of the symmetric group S_d.

THEOREM 6.3. (BABAI, CAMERON, PÁLFY [BCP82]) *Let $G \leq S_n$ be a primitive group of degree n and assume $G \in \Gamma_d$. Then $|G| \leq n^{cd}$ where c is an absolute constant. More generally, if all alternating composition factors of G have bounded orders and all classical groups among the composition factors of G have bounded dimensions then $|G| \leq n^C$ for some constant C depending only on the bounds in the condition.*

Note that in particular, *primitive solvable groups* have order $\leq n^c$, where $c = 3.24399...$ (Pálfy [Pál82], Wolf [Wol82]).

Turning back to Luks's algorithm, Theorem 6.3 guarantees that $|G/N|$ is polynomially bounded, allowing a recurrence in timing with polynomially bounded solution, completing the proof of Theorem 6.2. (We note that Theorem 6.3 was not available to Luks at the time; instead, in the difficult affine case, he used the second reduction step above with H a Sylow p-subgroup which he showed had polynomially bounded index.) □

Isomorphism of tournaments can be decided in $n^{O(\log n)}$ time [BL83]. This algorithm uses the Pálfy-Wolf bound on primitive solvable groups (above) (and the Feit–Thompson theorem through the solvability of the automorphism groups of tournaments).

6.7 Basic permutation group algorithms

We assume in this section that a permutation group $G \leq \mathrm{Sym}(\Omega)$ is given by a set S of s generators; $|\Omega| = n$. Some of the basic algorithmic problems to solve are testing *membership* in G of a given $\sigma \in \mathrm{Sym}(\Omega)$; determining the *order* of G; constructing the *normal closure* of a subgroup (also given by a list of generators). Once these are solved, solvability and nilpotence of G are easily decided. In his pioneering work in computational group theory, C. C. Sims [Sim70], [Sim78], [Sim71] constructed algorithms for these problems wich ran fast in practice and were later asymptotically analysed to run in polynomial time in the worst case (see below).

Theory and practice diverge in the areas of more advanced problems, including determining the *center*, the *composition factors*, the *Sylow subgroups*. All these problems are now solvable in polynomial time. The elegant construction of a composition chain and the composition factors (Luks [Luk87]) uses the O'Nan–Scott Theorem (Chap. 12) and requires CFSG (the Classification of Finite Simple Groups) through Schreier's Hypothesis (the outer automorphism group of a simple group is solvable). Beals has recently found an elementary algorithm for composition factors [Bea93b]. Kantor's construction of the Sylow subgroups [Kan85b], [Kan85a] starts with finding a composition chain via [Luk87] and rests on detailed knowledge of CFSG and a case-by-case study of the classical groups. Luks's algorithm to find the center is elementary [Luk87].

Many other important problems are *not* known to be solvable in polynomial time, and in fact often they are at least as hard in general as *graph isomorphism* (centralizers,

intersections, cf. Sec. 6.5). Particularly efficient backtrack procedures have recently been found and implemented by J. Leon [Leo91], using partitioning heuristics (cf. Sec. 6.4). Such procedures are often used even for problems solvable in polynomial time (e.g. finding the center by repeated application of a backtrack routine for centralizers), showing a discrepancy between theoretical and practical measures of efficiency.

For the rest of this section we return to the complexity analysis of the basic problems. Given a chain $G = G_0 \geq G_1 \geq \ldots \geq G_m = 1$ of subgroups, a *strong generating set* (SGS) with respect to this chain is a set $T \subseteq G$ such that $\langle T \cap G_i \rangle = G_i$ for every i. This concept was introduced by C. C. Sims [Sim70] (with respect to the stabilizer chain) as the fundamental data structure for permutation group algorithms. (Recent algorithms often operate on different chains of subgroups; however, it is possible to switch efficiently from any SGS to one in Sims's sense [CFS90].) Given an SGS, the problems of membership and order can be solved easily, a presentation (in terms of generators and relations) can be deduced, and slight variations of the SGS methods yield normal closures as well. Variants of Sims's method have been shown to run in polynomial time ($O(n^6 + sn^2)$ [FHL80] and $O(n^5 + sn^2)$ [Knu91], [Jer86]). These elementary algorithms require $\Omega(n^5)$ even on *average* on large classes of examples [Knu91].

Better asymptotic bounds have been obtained using heavy guns. For two function f, g let us write $f(n) = O^{\sim}(g(n))$ if for sufficiently large n, $f(n) \leq g(n) \log^c n$ for some constant c. With this notation, the best current deterministic asymptotic worst case bound is $O^{\sim}(sn^3)$ [BLS93]. This bound depends on CFSG primarily through estimates of the orders of primitive permutation groups (Chap. 12, Theorem 5.8, cf. [Cam81]). With randomization we can do considerably better and have an entirely elementary $O^{\sim}(n^3 + sn)$ Monte Carlo algorithm to construct an SGS [BCF$^+$91]. (Being Monte Carlo, the algorithm does not guarantee to construct an SGS but it does so with arbitrarily large probability.) The algorithm includes a particularly efficient *normal closure* routine, running in $O^{\sim}(n^2 + sn)$. The basic technique of the algorithm generalizes the following observation: *Let $g_1, \ldots, g_k \in G$ generate G and let H be a proper subgroup of G. Then the probability that $h \notin H$ for a* random subproduct $h = g_1^{\epsilon_1} \cdots g_k^{\epsilon_k}$ *is* $\geq 1/2$. (The $\epsilon_i \in \{0, 1\}$ are selected by independent unbiased coin-flips.)

A *base* of G is a set $B \subseteq \Omega$ such that the pointwise stabilizer of B in G is the identity. Let $\mu(G)$ be the minimum size of a base. The case of small $\mu(G)$ is of particular interest. For instance, if G is simple non-alternating then $\mu(G) = O(\log n)$. It is easy to see that $2^{\mu(G)} \leq |G| \leq n^{\mu(G)}$. Let us say that a class $\mathcal{G}$ of groups has *small bases* if $\mu(G) = (\log n)^{O(1)}$ for $G \in \mathcal{G}$. Sims style algorithms run in $O^{\sim}(sn^2)$ on groups with a small base. Using new combinatorial techniques, elementary Monte Carlo algorithms have been found which construct an SGS in *nearly linear*, $O^{\sim}(sn)$ time for small base groups [BCFS91]. The speedup relies on methods capable of handling chains of certain *subsets* of G which are not subgroups; the subgroup structure of small base groups tends to be too coarse to allow nearly linear time. The key new ingredients are an efficient implementation of Sims's *Schreier vector data structure* to store coset representatives in a *shallow tree* (depth guaranteed to be $\leq \log |G|$) via an algorithmic version of the Reachability Theorem (Theorem 6.4); and the use of the Local Expansion property (Theorem 3.41) to rapidly locate new elements if the current partial SGS misses a substantial portion of G.

Finding *domains of imprimitivity* seems indispensable when delving deeper into the group structure. Atkinson's algorithm finds them in quadratic time [Atk75]. For small base groups, Beals improved this to nearly linear time [Bea93a], and in a *tour de force,* used this with Seress to find a composition series in nearly linear time [BS92b].

A final note on *parallelization.* An *NC algorithm* uses $n^{O(1)}$ parallel processors and extremely short, $(\log n)^{O(1)}$ time, where n is the length of the input. (So none of the processors has time to read any substantial portion of the input; cf. Chap. 29.) Radical departure from the classical methods has allowed the design of an *NC algorithm to construct an SGS* and solve some of the basic problems in NC, including membership, order, normal closures, solvability, center, composition factors [BLS87]. Again, the algorithm uses CFSG mainly through Theorem 5.8 of Chap. 12, and also requires Luks's composition factors algorithm. The algorithm digs deeply into the normal structure of G. Even the rudimentary task of membership testing requires determining the composition series first.

6.8 Complexity of related problems

Problems related to *graph isomorphism* ("ISO" for short) and *permutation group membership* fall into a variety of complexity classes. Groups, semigroups will be given by a list of generators, unless otherwise stated.

A surprising result of Anna Lubiw [Lub81] asserts that the following problem is NP-complete: *Does a given permutation group have a fixed-point-free element ?* Even the case when G is an elementary abelian 2-group is NP-complete. F. Lalonde [Lal81] used this to show the following problem NP-complete: *Does a given a bipartite graph have an automorphism of order 2 interchanging the two color classes?* In contrast, if we omit the "order 2" restriction, the problem becomes *isomorphism complete* (equivalent to ISO). The original (equivalent) statement of Lalonde's theorem is this: *The star system problem is NP-complete.* The "star system problem" has a family $\mathcal{F}$ of n subsets of an n-set V for input and asks if there exists a graph $X = (V, E)$ such that $\mathcal{F} = \{X(v) : v \in V\}$ is the family of vertex neighborhoods in X.

Isomorphism of groups of order n, given by their Cayley tables, can be decided in time $n^{\log_2 n + O(1)}$ because the groups are generated by $\leq \log_2 n$ elements and any mapping of the generators can be extended to a homomorphism in at most one way. This argument generalizes to quasigroups which in turn include Steiner triple systems.

To decide *isomorphism of permutation groups* is at least as hard as hard as ISO [BKL]. On the other hand this problem is in NP for the following simple reason: Let $G = \langle S \rangle \leq \mathrm{Sym}(A)$ and $H = \langle T \rangle \leq \mathrm{Sym}(B)$ be permutation groups and $f : S \to \mathrm{Sym}(B)$ a map. Then f extends to an isomorphism of G onto H if and only if the following two polynomial time testable conditions hold: (i) H is generated by the f-image of S; (ii) the orders of G, H, and the group $\langle (s, f(s)) : s \in S \rangle$ agree. – On the other hand, isomorphism of permutation group also belongs to the class *coAM* [BKL] (cf. Sec. 6.1) and is therefore unlikely to be NP-complete.

If $G, H, K \leq \mathrm{Sym}(A)$ and $\sigma \in \mathrm{Sym}(A)$ then the *double coset membership* problem "$\sigma \in GH$?" belongs to the Luks equivalence class (is equivalent to coset intersection)

(Sec. 6.5). On the other hand, the question "$\sigma \in GHK$?" is NP-complete (Luks).

The membership problem for *semigroups of transformations* of a finite set is $PSPACE$-complete (Kozen [Koz77]).

The membership problem for $d \times d$ *integral matrices* is *undecidable* already for $d = 4$. This is immediate from the following result of Mihailova [Mih58]: The membership problem is undecidable for subgroups of $F_2 \times F_2$, where F_2 is the free group of rank 2. However, finiteness of an integral matrix group (or a matrix group over an algebraic number field) can be decided in polynomial time [BBR93], and if the group is finite, the usual basic questions (order, center, composition chain, Sylow subgroups) can be answered in Las Vegas polynomial time [BB93]. (A Las Vegas algorithm uses randomization but never outputs a wrong answer.)

For finite groups, the membership problem is in NP under quite general conditions. A *black box group* is, informally, a group whose elements are encoded by (0,1)-strings of uniform length, and the group operations are performed by a "black box". (As all our groups, a black box group is given by a list of generators.) Then membership is in NP, relative to the black box. In particular, membership in matrix groups over finite fields is in NP. This is immediate from the following combinatorial result. A *straight line program* reaching a group element $g \in G$ from a set S of generators of G is a sequence $g_1, \ldots, g_m$ of elements of G such that $g_m = g$, and for each i, either $g_i \in S$, or $g_i = g_j^{-1}$, or $g_i = g_j g_k$ for some $j, k < i$. The *cost* of such a program is the number of inversions and multiplications (the calls to S are free). The *straight line cost* of $g \in G$ (relative to S) is the minimum cost of straight line programs reaching g from S.

THEOREM 6.4. (REACHABILITY THEOREM [BS84]) *Given any set S of generators of a group G of order n, the straight line cost of any $g \in G$ is less than $(1 + \log_2 n)^2$.*

We conjecture that membership in matrix groups also belongs to *coNP*. The proof of this statement and the stronger statement that the *order* of a matrix group over a finite field belongs to NP (i.e. the correct order has polynomial time verifiable certificates) depends, in essence, on the following conjecture.

Short presentation conjecture. Every group of order n has a presentation (in terms of generators and relations) of length $(\log n)^{O(1)}$.

(The *length* of a presentation is the total number of characters required to write down the presentation.) It follows from Theorem 6.4 that it suffices to prove this conjecture for simple groups. All cases have been confirmed with the exception of the rank 1 simple groups of twisted Lie type (unitary, Suzuki, Ree) [BGK$^+$].

None of the problems mentioned in this section, with the possible exception of isomorphism of groups given by a Cayley table, is expected to have polynomial time solution. In particular, the membership problem for 1×1 matrix groups is a close relative of the *discrete logarithm* problem (given $a, b \in GF(q)$, find an integer x such that $a^x = b$ or decide that no such x exists) which is not expected to be solvable in polynomial time (cf. [AD93]).

Modulo this obstacle, however, a great deal of stucture can be found in matrix groups and even in black box groups [BB93].

7 The reconstruction problem

All graphs in this section are finite unless otherwise stated.

In the Introduction to this chapter we gave a general definition of reconstructibility; and discuused a number of instances. Examples include Whitney's theorems on the reconstructibility of graphs from their line graphs (with known exceptions) (Sec. 1.2), of 3-connected graphs from their cycle matroids (cf. Chap. 11, Sec. 7), and from many other functions of graphs (the area of graph equations comes under this heading, see [CS79]). The unsettled status of the Graph Isomorphism problem is related to the non-reconstructibility from any of the known polynomial time computable invariants.

While reconstruction problems (solved and unsolved) seem to pop up in nearly every topic considered, the term "The Reconstruction Problem" has been reserved for the single most notorious member of this species in graph theory: the Kelly–Ulam Reconstruction Conjecture. It is this problem to which this brief last section is devoted. For more information and references we refer to the surveys mentioned in the preface to this chapter.

7.1 Vertex reconstruction

With every a graph $X = (V, E)$ we associate the multiset $D^v(X)$ of isomorphism types of its one-vertex-deleted subgraphs, i.e. the isomorphism type of $X \setminus v$ for each $v \in V$. We call $D^v(X)$ the *deck of 1-vertex-deleted subgraphs*. Analogously one can define the multiset $D^e(X)$, the deck of 1-edge-deleted subgraphs, and more generally, $D^v_k(X)$ and $D^e_k(X)$, the decks of k-vertex-deleted (k-edge-deleted, resp.) subgraphs.

The graph X is *vertex reconstructible* (or simply reconstructible) if it is determined (up to isomorphism) by $D^v(X)$. Edge-reconstructibility is defined analogously. More generally we say that the graph invariant $f(X)$ (cf. Section 6.3) is vertex-reconstructible if $f(X)$ is determined by $D^v(X)$. The *Reconstruction Conjecture* says that *all finite graphs with* ≥ 3 *vertices are reconstructible* (P. J. Kelly, S. M. Ulam, 1942).

The answer to the analogous question for directed graphs is negative: an infinite family of pairs of non-isomorphic tournaments with identical decks has been found by P. K. Stockmeyer [Sto77].

It is known that *almost every graph is vertex-reconstructible* (Erdős). Indeed, this is an immediate consequence of the fact that almost every graph X has the following property: no pair of two-vertex-deleted subgraphs of X are isomorphic. – This argument generalizes to smaller subgraphs: almost all graphs are reconstructible from their k-vertex-deleted subgraphs for all $k < c \log n$ for some constant $c > 0$.

Some concrete classes of graphs are also known to be reconstructible. These include disconnected graphs, trees (Kelly, 1957), and some families of tree-like graphs. In particular, all graphs with $\leq n$ edges are reconstructible. On the other hand, if $m(n)$ is a function such that $m(n) - n$ is unbounded, then it is not known whether or not all graphs with $m(n)$ edges are reconstructible.

Among the reconstructible invariants, one should mention the degree sequence and a refinement of this: the sequence of degree sequences of the neighborhoods of the vertices [NW78]. Applying powerful counting techniques to reconstruction theory, Tutte [Tut79]

has shown important polynomials associated with graphs to be reconstructible: the characteristic polynomial, the chromatic polynomial, and generalizations of these.

The Reconstruction Conjecture is false for infinite graphs (even for forests) but no counterexamples are known to the following variant, *Halin's Conjecture:* If two (finite or infinite) graphs with at least 3 vertices have the same deck of vertex-deleted subgraphs, then each is isomorphic to a subgraph of the other.

7.2 Edge reconstruction

It is known that a vertex-reconstructible graph with at least 4 edges is also edge-reconstructible (Greenwell [Gre71]). In addition, however, large classes of graphs are known to be edge-reconstructible for which vertex-reconstructibility is open. The first result in this direction was Lovász's [Lov72b] who proved that if a graph has more edges than its complement then it is edge-reconstructible. Lovász's proof used a clever inclusion-exclusion argument which was the basis of rapid further improvements. V. Müller [Mül77] showed that graphs with m edges and n vertices are edge-reconstructible unless $2^{m-1} \leq n!$, which means $m \leq n \cdot \log_2 n$. Nash-Williams [NW78] modified Müller's proof and obtained the following lemma, from which Müller's bound is immediate.

LEMMA 7.1. (NASH-WILLIAMS) *Suppose that the graph $X = (V, E)$ is not edge-reconstructible. Then for every subset $A \subseteq E$ such that $|A \setminus E|$ is even, there exists a permutation $\sigma \in \mathrm{Sym}(V)$ such that $E \cap E^\sigma = A$.*

Lovász observed that this lemma has the following immediate consequence:

COROLLARY 7.2. *If $X = (V, E)$ is not edge-reconstructible then for every $T \subseteq E$,*

$$|\sigma \in \mathrm{Sym}(V) : T^\sigma \subseteq E| \geq 2^{|E|-|T|-1}.$$

L. Pyber [Pyb90] used this to derive that *all Hamiltonian graphs are edge-reconstructible*, with possibly a finite set of exceptions. Indeed, by Cor. 7.2, a nonreconstructible Hamiltonian graph with n vertices and m edges would have at least $2^{m-n-2}/n$ Hamilton cycles. But this is too much: Pyber proves that no graph has more than c^{m-n} Hamilton cycles, where $c = 1.977$. □

The arguments used in the proofs of Lovász, Müller, Nash-Williams lend themselves to a much more general treatment. The following framework was introduced by V. Mnukhin [Mnu87].

Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group acting on the set Ω. We say that two subsets Δ_1, $\Delta_2 \subseteq \Omega$ are G-isomorphic if $\Delta_1^\sigma = \Delta_2$ for some $\sigma \in G$. For any subset $\Gamma \subseteq \Omega$ let Γ^G be the G-orbit of Γ, i.e. the set of subsets of Ω, G-isomorphic to Γ.

For $\Delta \subseteq \Omega$ let the k-deleted deck $D_k(\Delta)$ be the multiset of G-isomorphism classes of the $(|\Delta| - k)$-element subsets of Δ. The set Δ is k-reconstructible if it is determined (up to G-isomorphism) by its k-deleted deck $D_k(\Delta)$.

In particular, taking Ω to be the set of $\binom{n}{2}$ pairs of elements of V and $G \cong \mathrm{Sym}(V)$ be the induced action of $\mathrm{Sym}(V)$ on Ω, the concept of G-isomorphism of subsets of Ω

becomes the ordinary isomorphism of graphs on the vertex set V; and k-reconstructibility turns into the concept of reconstructibility from the deck of *k-edge-deleted* subgraphs.

Generalizing Müller's theorem Mnukhin proves that if $\Delta \subset \Omega$ is not 1-reconstructible then $2^{|\Delta|-1} \leq |G|$.

Below we indicate a *linear algebra* approach introduced by Godsil, Krasikov, and Roditty [GKR87] to extend Müller's result to k-reconstructibility for $k \geq 2$. Their technique is easily adapted to Mnukhin's situation.

Recall that a hypergraph $\mathcal{F} \subseteq 2^\Omega$ is m-uniform if $|E| = m$ for each $E \in \mathcal{F}$.

DEFINITION 7.3. The *Vapnik–Chervonenkis dimension* or VC dimension of a hypergraph $\mathcal{F} \subseteq 2^\Omega$ is the greatest integer t for which there exists a subset $A \subseteq \Omega$ with $|A| = t$ such that every subset $B \subseteq A$ occurs as $B = A \cap E$ for some $E \in \mathcal{F}$.

For $0 \leq s \leq n$ the s-inclusion matrix $I(\mathcal{F}, s)$ of a hypergraph $\mathcal{F} \subseteq 2^\Omega$ has rows indexed by the members $F \in \mathcal{F}$, columns indexed by subsets $A \subseteq \Omega$ with $|A| = s$, and entry 1 if $A \subseteq F$ and 0 otherwise. The s^*-inclusion matrix $I^*(\mathcal{F}, s)$ has all the columns of the t-inclusion matrices for $t = 0, 1, 2, \ldots, s$.

We say that $\mathcal{F}$ is *s-independent* if the rows of the s-inclusion matrix are linearly independent (i.e. $I(\mathcal{F}, s)$ has full row-rank), and it is s^*-independent if the rows of $I^*(\mathcal{F}, s)$ are linearly independent. Clearly s-independence implies s^*-independence, and for uniform hypergraphs, the converse also holds [FW81].

THEOREM 7.4. (FRANKL–PACH [FP83]) *If $\mathcal{F}$ is s^*-dependent, then its VC dimension is at least $s + 1$.*

The proof follows from the proof of Cor. 4.2 in Chap. 31. For a theory of the inclusion matrices, including this result, see [BF92].

The main lemma of [GKR87] follows.

LEMMA 7.5. *If Δ_1 and Δ_2 have the same k-deleted deck $D_k(\Delta_i)$ but are not G-isomorphic, then the m-uniform set-system $\mathcal{F} = \Delta_1^G \cup \Delta_2^G$ is $(m-k)$-dependent (where $m = |\Delta_i|$).*

PROOF: We prove the dependence of the rows of $I(\mathcal{F}, m-k)$ by explicitly giving coefficients $c(E)$ $(E \in \mathcal{F})$ for a linear relation among them. For $i = 1, 2$ let $\alpha_i = |G_{\{\Delta_i\}}|$ (the size of the set-stabilizer of Δ_i). If $E \in \Delta_1^G$ let $c(E) = \alpha_1$, and if $E \in \Delta_2^G$ let $c(E) = -\alpha_2$. To check that this linear combination of the rows is a zero row, consider a column indexed by a set $T \subseteq \Omega$ with $|T| = m - k$. The column has zeros except where $T \subseteq E$. So the entry for this column in the indicated linear combination of the rows will be α_1 times the number of $E \in \Delta_1^G$ with $T \subseteq E$, minus α_2 times the number of $E \in \Delta_2^G$ with $T \subseteq E$. This is the number of $\sigma \in G$ for which $T \subseteq \Delta_1^\sigma$ minus the number of $\sigma \in G$ for which $T \subseteq \Delta_2^\sigma$ But this difference is zero because for every set T of size $m - k$, the number of $\sigma \in G$ for which $T^\sigma \subseteq \Delta_i$ is independent of i. □

Using this lemma and Theorem 7.4 we infer the following generalization of Müller's inequality.

THEOREM 7.6. ([GKR87]) *If $\Delta \subseteq \Omega$ is not k-reconstructible, then $2^{|\Delta|-k} \leq |G|$.*

PROOF: Combining the foregoing results we obtain that for $\mathcal{F}$ as before, the VC-dimension of $\mathcal{F}$ is $\geq m - k + 1$. Hence $|\mathcal{F}| \geq 2^{m-k+1}$, while clearly $|\mathcal{F}| \leq 2|G|$. $\square$

In particular we obtain that if a graph with n vertices and m edges is not k-reconstructible then $2^{m-k} \leq n!$, or $m \leq k + n \log_2 n$.

For $k = 1$ we also recover Lovász's corollary to the Nash-Williams Lemma (slightly improved).

THEOREM 7.7. *If $\Delta \subseteq \Omega$ is not 1-reconstructible, then for every $\Gamma \subseteq \Delta$,*

$$|\{\sigma \in G : \Gamma^\sigma \subseteq \Delta\}| \geq 2^{|\Delta|-|\Gamma|} - 1.$$

PROOF: Let $\mathcal{F}$ be as before (now $k = 1$). Since its VC dimension is $\geq m - k + 1 = m$, there is a set $A \subseteq \Omega$ with $|A| = m$ of which every subset is its intersection with some $E \in \mathcal{F}$. In particular, $A \in \mathcal{F}$. Now take any proper subset Γ of Δ. Since Δ and Δ_2 have the same 1-deleted deck, we also have $\Gamma^\sigma \subseteq \Delta_2$ for some $\sigma \in G$, hence we have $\Gamma^\tau \subseteq A$ for some $\tau \in G$ (since $A \in \mathcal{F} = \Delta^G \cup \Delta_2^G$). And $|\{\sigma \in G : \Gamma^\sigma \subseteq \Delta\}| = |\{\sigma \in G : \Gamma^\tau \subseteq \Delta^\sigma\}|$. But this latter is at least the number of proper subsets of A which contain Γ^τ, because each of those is $A \cap E$ for some $E \in \mathcal{F}$ (hence for some $E = \Delta^\sigma$ since the proper subsets are in the 1-deleted deck which Δ and Δ_2 share). The latter number is $2^{m-|\Gamma|} - 1$. $\square$

References

[A+85] M. Aschbacher et al., editors. *Proceedings of the Rutgers Group Theory Year, 1983-1984*. Cambridge University Press, 1985.

[AB89] F. Annexstein and M. Baumslag. Limitations on constructing expanders with Cayley graphs. manuscript, 1989.

[Abb72] H.L. Abbott. A note on Ramsey's theorem. *Canad. Math. Bull.*, 15:9–10, 1972.

[AD87] D. Aldous and P. Diaconis. Strong uniform times and finite random walks. *Adv. Appl. Math.*, 8:69–97, 1987.

[AD93] L.M. Adleman and J. Demarrais. A subexponential algorithm for discrete logarithms over all finite fields. *Mathematics of Computation*, 61:1–15, 1993.

[AHI92] F. Aurenhammer, J. Hagauer, and W. Imrich. Cartesian graph factorization at logarithmic cost per edge. *Comput. Complexity*, 2:331 – 349, 1992.

[Ald83] D. Aldous. Random walks on finite groups and rapidly mixing Markov chains. In *Séminaire de Probabilités XVII*, pages 243–297. Springer-Verlag, 1983. Lecture Notes in Mathematics, 986.

[Ald87] D. Aldous. On the Markov chain simulation method for uniform combinatorial distributions and simulated annealing. *Probability in Engineering and Inf. Sci.*, 1:33–46, 1987.

[Ale74] V. E. Alekseiev. On the number of Steiner triple systems. *Math. Notes*, 15:461–464, 1974.

[Alo86] N. Alon. Eigenvalues and expanders. *Combinatorica*, 6:83–96, 1986.

[Als79] B. Alspach. Hamiltonian cycles in vertex-transitive graphs of order $2p$. In *Proc. Tenth S.E. Conf., Boca Raton*, volume XXIII of *Congr. Numerantium*, pages 131–139. Utilitas Math., 1979.

[Asc76] M. Aschbacher. A homomorphism theorem for finite graphs. *Proceedings of the AMS*, 54:468–471, 1976.

[Asc80] M. Aschbacher. *The Finite Simple Groups and Their Classification*, volume 7 of *Yale Mathematical Monographs*. Yale Univ. Press, New Haven and London, 1980.

[Atk75] M. D. Atkinson. An algorithm for finding the blocks. *Math. Comp.*, 29:911–913, 1975.

[Bab] L. Babai. Vertex-transitive graphs, excluded minors, and hyperbolic geometry. in preparation.

[Bab73] L. Babai. Groups of graphs on given surfaces. *Acta Math. Acad. Sci. Hung.*, 24:215–221, 1973.

[Bab74a] L. Babai. Automorphism groups of graphs and edge-contraction. *Discrete Math.*, 8:13–20, 1974.

[Bab74b] L. Babai. On the minimum order of graphs with given group. *Canad. Math. Bull.*, 17:467–470, 1974. MR 53♯10641.

[Bab75] L. Babai. Automorphism groups of planar graphs II. In A. Hajnal et al., editors, *Infinite and finite sets (Proc. Conf. Keszthely, Hungary, 1973)*. Bolyai - North-Holland, 1975.

[Bab77a] L. Babai. Some applications of graph contractions. *J. Graph Theory*, 1:125–130, 1977.

[Bab77b] L. Babai. Symmetry groups of vertex transitive polytopes. *Geometriae Dedicate*, 6:331–338, 1977.

[Bab78a] L. Babai. Chromatic number and subgraphs of Cayley graphs. In *Theory and Applications of Graphs*, volume 642 of *Lecture Notes in Math*, pages 10–22. Springer-Verlag, Berlin-Heidelberg-New York, 1978.

[Bab78b] L. Babai. Embedding graphs in Cayley graphs. In J-C. Bermond et al., editor, *Combinatories et theorie des graphes (Proc. Conf. Paris-Orsay,1976)*, pages 13–15. Centre National de Rech. Sci., 1978.

[Bab78c] L. Babai. Infinite digraphs with given regular automorphism groups. *J. Combinatorial Theory (B)*, 25:26–46, 1978. MR 58♯16380.

[Bab79a] L. Babai. Almost all Steiner triple systems are asymmetric. In C.C. Lindner and A. Rosa, editors, *Topics in Steiner Systems*, volume 7 of *Ann. Discrete Math*, pages 37–39. North-Holland,Amsterdam, 1979.

[Bab79b] L. Babai. Long cycles in vertex-transitive graphs. *J. Graph Theory*, 3:301–304, 1979. MR 80m:05059.

[Bab79c] L. Babai. Monte Carlo algorithms in graph isomorphism testing. Tech. Rep. 79–10, Dép. Math. et Stat., Univ. de Montréal, 1979.

[Bab79d] L. Babai. Spectra of Cayley graphs. *J. Combinatorial Theory (B)*, 29:180–189, 1979.

[Bab80a] L. Babai. Finite digraphs with given regular automorphism groups. *Periodica Math. Hung.*, 11:257–270, 1980.

[Bab80b] L. Babai. On the complexity of canonical labelling of strongly regular graphs. *SIAM J. on Computing*, 9:212–216, 1980.

[Bab81a] L. Babai. Moderately exponential bound for graph isomorphism. In *Fundamentals of Computation Theory*, volume 117 of *Lecture Notes in Math.*, pages 34–50. Springer-Verlag, Berlin-Heidelberg-New York, 1981.

[Bab81b] L. Babai. On the abstract group of automorphisms. In *Combinatorics*, volume 52 of *London Math. Soc. Lecture Notes*, pages 1–40. Cambridge Univ. Press, London, 1981.

[Bab81c] L. Babai. On the order of uniprimitive permutation groups. *Annals of Mathematics*, 113:553–568, 1981.

[Bab85] L. Babai. Arc transitive covering digraphs and their eigenvalues. *J. Graph Theory*, 8:363–370, 1985.

[Bab89] L. Babai. The probability of generating the symmetric group. *J. Comb. Theory (A)*, 52:148–153, 1989.

[Bab91a] L. Babai. Computational complexity in finite groups. In *Proc. Internat. Congress of Mathematicians, Kyoto 1990*, pages 1479–1489. Springer, Tokyo, 1991.

[Bab91b] L Babai. Local expansion of vertex-transitive graphs and random generation in finite groups. In *Proc. 23rd ACM Symposium on Theory of Computing*, pages 164–174, 1991.

[Bab91c] L. Babai. Vertex-transitive graphs and vertex-transitive maps. *J. Graph Theory*, 15:587–627, 1991.

[Bae47] R. Baer. Direct decompositions. *Trans. Amer. Math. Soc.*, 62:62–98, 1947.

[Bas72] H. Bass. The degree of polynomial growth of finitely generated nilpotent groups.

Proc. London Math. Soc., 25:603–614, 1972.

[BB87] J. van Bon and A.E. Brouwer. The distance-regular antipodal covers of classical distance-regular graphs. *Coll. Math. Soc. János Bolyai*, 52:141–166, 1987.

[BB93] R. Beals and L. Babai. Las vegas algorithms for matrix groups. In *Proc. 34th IEEE Symp. Found. Comp. Sci.*, pages 427–436, 1993.

[BBR93] L. Babai, R. Beals, and D. Rockmore. Deciding finiteness of matrix groups in deterministic polynomial time. In *Proc. ISSAC'93, Kiev*, pages 117–126. ACM Press, 1993.

[BCa] L. Babai and P.J. Cameron. Automorphism groups of switching classes of tournaments. to appear.

[BCb] L. Babai and P.J. Cameron. Most primitive groups are automophism groups of edge-transitive hypergraphs. to appear.

[BC75] M. Brown and R. Connelly. On graphs with a constant link, II. *Discrete Math.*, 11:199–232, 1975.

[BCF+91] L. Babai, G. Cooperman, L. Finkelstein, E.M. Luks, and Á. Seress. Fast Monte Carlo algorithms for permutation groups. In *Proc. 23rd ACM Symposium on Theory of Computing*, pages 90–100, 1991.

[BCFS91] L. Babai, G. Cooperman, L. Finkelstein, and Á. Seress. Nearly linear time algorithms for permutation groups with a small base. In *Proc. ISSAC'91 (Internat. Symp. on Symbolic and Algebraic Computation), Bonn*, pages 200–209, 1991.

[BCK81] E. Bannai, P. J. Cameron, and J. Kahn. Nonexistence of certain distance-transitive digraphs. *J. Combinatorial Theory (B)*, 31:105–110, 1981.

[BCN89] A.E. Brouwer, A.M. Cohen, and A. Neumaier. *Distance-regular graphs*. Springer, 1989.

[BCP82] L. Babai, P.J. Cameron, and P.P. Pálfy. On the orders of primitive groups with restricted nonabelian composition factors. *J. of Algebra*, 79:161–168, 1982.

[BE82] L. Babai and P. Erdős. Representation of group elements as short products. In J. Turgeon A. Rosa, G. Sabidussi, editor, *Theory and Practice of Combinatorics*, number 12 in Ann. Discr. Math., pages 21–26. North-Holland, 1982.

[Bea93a] R. Beals. Computing blocks of imprimitivity for small base groups in nearly linear time. In L. Finkelstein and W. M. Kantor, editors, *Groups and Comptation*, volume 11 of *DIMACS Ser. in Discr. Math. and Theor. Comp. Sci.*, pages 17–26. A.M.S., 1993.

[Bea93b] R. Beals. An elementary algorithm for computing the composition factors of a permutation group. In *Proc. ISSAC'93, Kiev*, pages 127–134. ACM Press, 1993.

[Bed85] A.R. Bednarek. Whitney's theorem for infinite graphs. *Discrete Math.*, 56:83–85, 1985. MR 87b:05065.

[Ben66] C.T. Benson. Minimal regular graphs of girth eight and twelve. *Canad. J. Math.*, 18:1091–1094, 1966.

[Ber72] C. Berge. Une condition pour qu'un hypergraphe soit fortement isomorphe à un hypergraphe complet ou multiparti. *C.R. Acad. Sci., Paris*, 274:1783–1786, 1972.

[BF92] L. Babai and P. Frankl. *Linear Algebra Methods in Combinatorics*. The University of Chicago, 1992. Preliminary version 2.

[BG82] L. Babai and C.D. Godsil. On the automorphism groups of almost all Cayley graphs. *Europ. J. Combinatorics*, 3:9–15, 1982.

[BG91] L. Babai and A.J. Goodman. Subdirectly reducible groups and edge-minimal graphs with given automorphism group. *J. London Math. Soc.*, 47:417–432, 1991.

[BG93] L. Babai and A. J. Goodman. On the abstract group of automorphisms. In D. Jungnickel and S. A. Vanstone, editors, *Coding Theory, Design Theory, Group Theory*, pages 121–143. Wiley, 1993. Proc. Marshall Hall Conf.

[BGK+] L. Babai, A. Goodman, W.M. Kantor, E.M. Luks, and P.P. Pálfy. Short presentations for finite groups. in preparation.

[BGL91] L. Babai, A.J. Goodman, and L. Lovász. Graphs with given automorphism group and few edge orbits. *Europ. J. Combin*, 12:185–203, 1991.

[BGM82] L. Babai, D. Yu. Grigoryev, and D. M. Mount. Isomorphism of graphs with bounded eigenvalue multiplicity. In *Proc. 14th ACM Symposium on Theory of Computing*, pages 310–324, 1982.

[BH77] J.A. Bondy and R.L. Hemminger. Graph reconstruction – a survey. *J. Graph Theory*, 1:227–268, 1977.

[BH92] L. Babai and G. Hetyei. On the diameter of random Cayley graphs of the symmetric group. *Combinatorics, Probability, and Computing*, 1:201–208, 1992.

[BHK+90] L. Babai, G. Hetyei, W.M. Kantor, A. Lubotzky, and Á. Seress. On the diameter of finite groups. In *Proc. 31st IEEE Symp. Found. of Computer Science*, pages 857–865, 1990.

[BHM80] A. Blass, F. Harary, and Z. Miller. Which trees are link graphs? *J. Combin. Theory, Ser. B*, 29:277–292, 1980.

[BI84] E. Bannai and T. Ito. *Algebraic Combinatorics, I.* Benjamin/Cummings, Menlo Park, 1984.

[Big72] N. L. Biggs. The symplectic representation of map automorphisms. *Bull. London Math. Soc.*, 4:303–306, 1972.

[Big73] N. L. Biggs. Three remarkable graphs. *Canad. J. Math.*, 25:397–411, 1973.

[Big74] N. L. Biggs. *Algebraic Graph Theory.* Cambridge Univ. Press, 1974.

[Bir45] G. Birkhoff. Sobre los grupos di automorfismos. *Revista Unión Math. Argentina*, 11:155–157, 1945.

[BK79] L. Babai and L. Kučera. Canonical labeling of graphs in linear average time. In *Proc. 20th IEEE Symp. on Foundations of Comp. Sci.*, pages 39–46, 1979.

[BKL] L. Babai, S. Kannan, and E. M. Luks. Bounded round interactive proofs for nonisomorphism of permutation groups. in preparation.

[BKL89] L. Babai, W.M. Kantor, and A. Lubotzky. Small diameter Cayley graphs for finite simple groups. *Europ. J. Comb.*, pages 507–522, 1989.

[BL73a] L. Babai and L. Lovász. Permutation groups and almost regular graphs. *Studia Sci. Math. Hung.*, 8:145–150, 1973.

[BL73b] A. Bruen and B. Levinger. A theorem on permutations of a finite field. *Canad. J. Math.*, 25:1060–1065, 1973.

[BL83] L. Babai and E. M. Luks. Canonical labeling of graphs. In *Proc. 15th ACM Symposium on Theory of Computing*, pages 171–183, 1983.

[BLS87] L. Babai, E. M. Luks, and Á. Seress. Permutation groups in NC. In *Proc. 19th*

ACM Symposium on Theory of Computing, pages 409–420, 1987.

[BLS93] L. Babai, E. M. Luks, and Á. Seress. Computing composition series in primitive groups. In L. Finkelstein and W. M. Kantor, editors, *Groups and Comptation*, volume 11 of *DIMACS Ser. in Discr. Math. and Theor. Comp. Sci.*, pages 1–16. A.M.S., 1993.

[BM88] L. Babai and S. Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *J. Comp. Syst. Sci.*, 36:254–276, 1988.

[Bol79] B. Bollobás. *Graph Theory*. Springer, New York, 1979.

[Bol82] B. Bollobás. The asymptotic number of unlabelled regular graphs. *J. London Math. Soc.*, 26:201–206, 1982.

[Bol85] B. Bollobás. *Random Graphs*. Academic Press, London, 1985.

[Bon91] J.A. Bondy. A graph reconstructor's manual. In *Proc. of the Thirteenth British Combinatorial Conference*. Cambridge Univ. Press, 1991. London Math. Soc. Lecture Note Series.

[Bou69] I.Z. Bouwer. Section graphs for finite permutation groups. *J. Combinat. Theory*, 6:378–386, 1969.

[Bou72] I.Z. Bouwer. On edge but not vertex transitive regular graphs. *J. Comb. Theory B*, 12:32–40, 1972.

[BP80] L. Babai and A. Pultr. Endomorphism monoids and topological subgraphs of graphs. *J. Combinatorial Theory (B)*, 38:278–283, 1980. MR 82c:05052.

[BS71] N. L. Biggs and D.H. Smith. On trivalent graphs. *Bull. London Math. Soc.*, 3:155–158, 1971.

[BS80] J.A. Bondy and M. Simonovits. Longest cycles in 3-connected cubic graphs. *Canad. J. Math.*, 32:987–992, 1980.

[BS84] L. Babai and E. Szemerédi. On the complexity of matrix group problems. In *Proc. 24th IEEE Symp. Found. of Computer Science*, pages 229–240, 1984.

[BS85] L. Babai and Vera T. Sós. Sidon sets in groups and induced subgraphs of Cayley graphs. *Europ. J. Combin.*, pages 101–114, 1985.

[BS88] L. Babai and Á. Seress. On the diameter of Cayley graphs of the symmetric group. *J. Comb. Theory (A)*, 49:175–179, 1988.

[BS92a] L. Babai and M. Szegedy. Local expansion of symmetrical graphs. *Combinatorics, Probability, and Computing*, 1:1–11, 1992.

[BS92b] R. Beals and Á. Seress. Structure forest and composition factors in nearly linear time. In *Proc. 24th ACM Symp. Theory of Computing*, pages 116–125, 1992.

[Bul72] V.K. Bulitko. On the problem of the finiteness of a graph with given vertex neighborhoods. *General systems theory (Russian), Akad. Nauk Ukrain. SSR Inst. Kibernet.*, pages 76–83, 1972. in Russian.

[Bur11] W. Burnside. *Theory of Groups of Finite Order*. Cambridge Univ. Press, 1911.

[BW80] L. Babai and M. Watkins. Connectivity of infinite graphs having a transitive torsion group action. *Archiv. der Math.*, 34:90–96, 1980.

[Cam] P.J. Cameron. unpublished.

[Cam80a] P. J. Cameron. 6-transitive graphs. *J. Combinatorial Theory (B)*, 28:168–179, 1980.

[Cam80b] P. J. Cameron. On graphs with given automorphism group. *Europ. J. Combi-*

natorics, 1:91–96, 1980.

[Cam81] P.J. Cameron. Finite permutation groups and finite simple groups. *Bull. London Math. Soc.*, 13:1–22, 1981.

[Cam82] P.J. Cameron. There are only finitely many distance transitive graphs of given valency greater than two. *Combinatorica*, 2:9–13, 1982. MR 83k:05050.

[Cam83] P. J. Cameron. Automorphism groups of graphs. In R. J. Wilson L. W. Beineke, editor, *Selected Topics in Graph Theory, 2*, pages 89–127. Acad. Press, 1983. MR 86i:05079.

[Cam90] P.J. Cameron. *Oligomorphic Permutation Groups*. London Math. Soc. Lecture Notes. Cambridge Univ. Press, 1990.

[Car60] L. Carlitz. A theorem on permutations in a finite field. *Proc. Amer. Math. Soc.*, 11:456–459, 1960.

[CDS80] D.M. Cvetković, M. Doob, and H. Sachs. *Spectra of Graphs*. Acad. Press, 1980.

[CFI92] J. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12:389–410, 1992.

[CFS90] G. Cooperman, L. Finkelstein, and N. Sarawagi. A random base change algorithm for permutation groups. In *Proc Int. Symp. Symbolic and Algebraic Comp. (ISSAC'90)*, pages 161–168. ACM, 1990.

[CGS78] P. J. Cameron, J.-M. Goethals, and J. J. Seidel. Strongly regular graphs having strongly regular subconstituents. *J. Algebra*, 55:257–280, 1978.

[CH] G. Cherlin and E. Hrushovski. Finite structures with few types. in preparation.

[Cha61] C. C. Chang. Ordinal factorization of finite relations. *Trans. A.M.S.*, 101:259–293, 1961.

[Che87] G.L. Cherlin. Homogeneous directed graphs. The imprimitive case. In *Logic Colloquium'85*, pages 67–88. Elsevier Sci. Publ., 1987.

[Chi88] D. Chillag. Generalized circulant and class functions of finite groups II. *Lin. Alg. Appl.*, 108:199–212, 1988.

[CHL85] G. Cherlin, L. Harrington, and A.H. Lachlan. $\aleph_0$-categorical, $\aleph_0$-stable structures. *Ann. Pure Appl. Logic*, 28:103–135, 1985.

[CL86] G. Cherlin and A.H. Lachlan. Stable finitely homogeneous structures. *Trans. Amer. Math. Soc.*, 296:815–850, 1986.

[CM72] H. S. M. Coxeter and W. O. J. Moser. *Generators and Relations for Discrete Groups*. Springer Verlag, third edition, 1972.

[Coh72] D. E. Cohen. *Groups of Cohomological Dimension One*, volume 254 of *Springer Lect. Notes in Math.* Springer Verlag, 1972.

[Con80] M. D. E. Conder. Generators of the alternating and symmetric groups. *J. London Math. Soc.*, 2:75–86, 1980.

[Cox61] H. S. M. Coxeter. *Introduction to Geometry*. New York Wiley, 1961.

[CPSS83] P.J. Cameron, C.E. Praeger, J. Saxl, and G.M. Seitz. On the Sims conjecture and distance transitive graphs. *Bull. London Math. Soc.*, 15:499–506, 1983.

[CS79] D.M. Cvetković and S.K. Simić. A bibliography of graph equations. *J. Graph Theory*, 3:311–324, 1979.

[CSW89] J. A. Conway, N. J. A. Sloane, and A. R. Wilks. Gray codes for reflection groups. *Graphs and Combinatorics*, 5:315–325, 1989.

[DD89] W. Dicks and M.J. Dunwoody. *Groups acting on graphs*. Cambridge studies in advanced mathematics 17. Cambridge Univ. Press, 1989.

[Del73] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Repts. Suppl.*, 10, 1973. MR 52♯5187.

[Dez73] M. Deza. Une propriété extrémale des plans projectifs finis dans une classe de codes equidistants. *Discrete Math.*, 6:343–352, 1973.

[DF87] J.R. Driscoll and M.L. Furst. Computing short generator sequences. *Info. and Comput*, 72:117–132, 1987.

[DGS85] A. Delgado, D. Goldschmidt, and B. Stellmacher. *Groups and Graphs, New Results and Methods*. Birkhäuser, 1985.

[Dia88] P. Diaconis. *Group representations in probability and statistics*. Institute of Mathematical Statistics, 1988.

[Dia89] P. Diaconis. Patterned matrices. In *Matrix Theory and Application*, pages 37–58, 1989. Proc. Symp. Appl. Math, Phonix, AZ, 1989.

[Dix69] J. D. Dixon. The probability of generating the symmetric group. *Math. Z.*, 110:199–205, 1969.

[DS84] P.G. Doyle and J.L. Snell. *Random walks and electric networks*. Math. Assoc. of America, 1984.

[Dun82] M. J. Dunwoody. Cutting up graphs. *Combinatorica*, 2:13–25, 1982.

[Dür85] E. Dürnberger. Every connected Cayley graph of a group with prime order commutator group has a Hamilton cycle. In *Cycles in Graphs (Burnaby, B.C. 1982)*, pages 75–80. North-Holland, 1985. vol. 115 of North-Holland Math. Studies, MR 87f:05082.

[EF80] Péter L. Erdős and Z. Füredi. On automorphisms of line-graphs. *Europ. J. Comb.*, 1:341–345, 1980.

[EG81] S. Even and O. Goldreich. The minimum length generator sequence is NP-hard. *J. Algorithms*, 2:311–313, 1981.

[Eil34] S. Eilenberg. Sur les transformations périodiques de la surface de sphére. *Fund. Math.*, 22:28–41, 1934.

[Ell88] M.N. Ellingham. Recent progress in edge-reconstruction. *Congressus Numerantium*, 62:3–20, 1988.

[ER63] P. Erdős and A. Rényi. Assymetric graphs. *Acta Math. Acad. Sci. Hungar.*, 14:295–315, 1963. MR 27♯3538.

[ER65] P. Erdős and A. Rényi. Probabilistic methods in group theory. *J. d'Analyse Math.*, 14:127–138, 1965.

[ET70] B. Elspas and J. Turner. Graphs with circulant adjacency-matrices. *J. Combinatorial Theory*, 9:297–307, 1970. MR 42♯7540.

[Fed92] T. Feder. Product graph representations. *J. Graph Theory*, 16:467–488, 1992.

[Fei89] W. Feit. Some finite groups with nontrivial centers which are Galois groups. In K.N. Cheng and Y.K. Leong, editors, *Group Theory*, pages 87–109. Walter de Gruyter, 1989.

[Fel68] W. Feller. *An Introduction to Probability Theory and Its Applications I.* Wiley, 3rd edition, 1968.

[FHL80] M. L. Furst, J. Hopcroft, and E. M. Luks. Polynomial time algorithms for

permutation groups. In *Proc. 21st IEEE Symp. Found. of Computer Science*, pages 36–41, 1980.

[FII86] I.A. Faradžev, A.A. Ivanov, and A.V. Ivanov. Distance transitive graphs of valency 5, 6, and 7. *Europ. J. Comb.*, 7:303–319, 1986. in Russian: *Zh. Vychisl. Mat. i Mat. Fiz.*, 24:1704–1718, 1984.

[Fis71] B. Fischer. Finite groups generated by 3-transpositions, I. *Invent. Math.*, 13:232–246, 1971.

[FK78] E. Fried and J. Kollár. Automorphism groups of algebraic number fields. *Math. Z.*, 163:121–123, 1978.

[FK81] E. Fried and J. Kollár. Automorphism groups of fields. In B. Csákány, E. Fried, and E.T. Schmidt, editors, *Universal Algebra (Proc. Conf. Esztergom 1977)*, Coll. Math. Soc. J. Bolyai 24. North-Holland, 1981.

[FM80] I. Filotti and J. Mayer. Polynomial-time algorithm for determining the isomorphism of graphs of fixed genus. In *Proc. 12th ACM Symp. on Theory of Comp.*, pages 236–243, 1980.

[FMS+89] A. Fiat, S. Moses, A. Shamir, I. Shimsoni, and G. Tardos. Planning and learning in permutation groups. In *Proc. 30th IEEE Fondations of Computer Science*, pages 274–279, 1989.

[Fol67] J. Folkman. Regular line-symmetric graphs. *J. Comb. Theory*, 3:215–232, 1967.

[Fou74] J.C. Fournier. Une condition pour qu'un hypergraphe, ou son complementaire, soit fortement isomorphe à un hypergraphe complet. In *Hypergraph Seminar*, volume 411 of *Springer Lecture Notes in Math.*, pages 95–98. Springer Verlag, 1974.

[FP83] P. Frankl and J. Pach. On the number of sets in a null t-design. *Europ. J. Combin.*, 4:205–236, 1983.

[Fra54] R. Fraïssé. Sur l'extension aux relations de quelques proprietes des ordres. *Ann. Sci. École Norm. Sup.*, 71:361–388, 1954.

[Fre45] H. Freudenthal. Über die Enden diskreter Räume und Gruppen. *Commentarii Math. Helv.*, 17:1–38, 1945.

[Fru38] R. Frucht. Herstellung von Graphen mit vorgegebener abstrakter Gruppe. *Compositio Math.*, 6:239–250, 1938.

[Fru49] R. Frucht. Graphs of degree 3 with given abstract group. *Canad. J. Math.*, 1:365–378, 1949.

[Fru52] R. Frucht. A one-regular graph of degree three. *Canad. J. Math*, 4:240–247, 1952.

[FS92] J. Feigenbaum and A. A. Schäffer. Finding the prime factors of strong direct product graphs in polynomial time. *Discrete Math.*, 109:77–102, 1992.

[FT65] L. Fejes Tóth. *Reguläre Figuren*. Akadémia Kiadó, Budapest, 1965.

[FW81] P. Frankl and R.M. Wilson. Intersection theorems with geometric consequences. *Combinatorica*, 1:357–368, 1981.

[Gal71] T. Gallai. Transitiv orientierbare Graphen. *Acta Math. Sci. Hung.*, 22:51–63, 1971.

[Gar73] A. Gardiner. Arc-transivity in graphs I. *Quart. J. Math. Oxford (2)*, 24:399–407, 1973. MR 48♯1973.

[Gar74] A. Gardiner. Antipodal covering graphs. *J. Comb. Theory (B)*, 16:255–273, 1974.

[Gar76] A. Gardiner. Homogeneous graphs. *J. Combinatorial Theory (B)*, 20:94–102, 1976. MR 54♯7316.

[GHL+87] Z. Galil, C.M. Hoffmann, E.M. Luks, C.P. Schnorr, and A. Weber. An $O(n^3 \log n)$ deterministic and an $O(n^3)$ Las Vegas isomorphism test for trivalent graphs. *J. ACM*, pages 513–531, 1987.

[GI87] C.D. Godsil and W. Imrich. Embedding graphs in Cayley graphs. *Graphs and Combinatorics*, 3:39–43, 1987.

[GJ79] M.R. Garey and D.S. Johnson. *Computers and Intractibility, A Guide to the Theory of NP-Completeness*. Freeman, San Francisco, 1979.

[GKR87] C.D. Godsil, L. Krasikov, and Y. Roditty. Reconstructing graphs from their k-edge-deleted subgraphs. *J. Combin. Theory, Ser. B*, 43:360–363, 1987.

[GL74] D.L. Greenwell and L. Lovász. Applications of product colouring. *Acta. Math. Acad. Sci. Hung.*, 25:335–340, 1974.

[GMW86] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yields nothing but their validity and a methodology of cryptographic protocol design. In *Proc. 27th IEEE Symp. Found. of Computer Science*, pages 168–195, 1986.

[God78] C. D. Godsil. Graphs, groups and polytopes. In *Combinatorial Mathematics*, volume 686 of *Lecture Notes in Math.*, pages 157–164. Springer-Verlag,Berlin-Heidelberg-New York, 1978. MR 80m:05052.

[God79] C.D. Godsil. *Graphs with Regular Groups*. PhD thesis, 1979.

[God80a] C.D. Godsil. More odd graph theory. *Discrete Math.*, 32:205–207, 1980.

[God80b] C.D. Godsil. Neighborhoods of transitive graphs and GRR's. *J. Comb. Theory B*, 29:116–140, 1980.

[God81a] C.D. Godsil. GRR's for non-solvable groups. In L. Lovász et al., editor, *Algebraic Methods in Graph Theory (Proc. Conf. Szeged, 1978)*, volume 25 of *Coll. Math. Soc. J. Bolyai*, pages 221–239. North-Holland, 1981.

[God81b] C.D. Godsil. On the full automorphism group of a graph. *Combinatorica*, 1:243–256, 1981.

[God82] C. D. Godsil. Eigenvalues of graphs and digraphs. *Lin. Alg. Appl.*, 46:43–50, 1982.

[God88] C.D. Godsil. Bounding the diameter of distance-regular graphs. *Combinatorica*, 8:333–343, 1988.

[Gol80] D.M. Goldschmidt. Automorphisms of trivalent graphs. *Annals of Mathematics*, 111:377–406, 1980.

[Goo93] A.J. Goodman. The edge-orbit conjecture of Babai. *J. Comb. Theory, Ser. B*, 57:26–35, 1993.

[GP70] I.M. Gel'fand and V.A. Ponomarev. Problems of linear algebra and classification of quadruples of subspaces in a finite-dimensional vector space. In *Hilbert Space Operators*, pages 163–237. Coll. Math. Soc. János Bolyai, vol.5., 1970.

[Gre71] D.L. Greenwell. Reconstructing graphs. *Proc. Amer. Math. Soc.*, 30:431–433, 1971.

[Gri83] R.I. Grigorchuk. On Milnor's problem of group growth. *Soviet Math. Dokl.*,

28:23–26, 1983.

[Gro58] J. de Groot. Automorphism groups of rings (Abstract). In *Internat. Congr. Math., Edinburgh*, page 18, 1958.

[Gro59] J. de Groot. Groups represented by homeomorphism groups I. *Math. Annalen*, 138:80–102, 1959.

[Gro81] M. Gromov. Groups of polynomial growth and expanding maps. *Publ. Math. IHES*, 53:53–73, 1981.

[GS81] B. Grünbaum and G.C. Shephard. The geometry of planar graphs. In H. N. V. Temperley, editor, *Combinatorics*, Proc. 8th British Comb. Conf., pages 124–150. Cambridge Univ. Press, 1981.

[GT87] J. L. Gross and T. W. Tucker. *Topological Graph Theory*. Wiley, 1987.

[GW85] R. L. Graham and P. M. Winkler. On isometric embeddings of graphs. *Trans. Amer. Math. Soc.*, 288:527 – 536, 1985.

[Haj85] A. Hajnal. The chromatic number of the product of two $\aleph_1$-chromatic graphs can be countable. *Combinatorica*, 5:137–139, 1985.

[Hal64] R. Halin. Über unendliche Wege in Graphen. *Math. Ann.*, 157:125–137, 1964. MR 30♯578.

[Ham62] M. Hamermesh. *Group Theory and its Application to Physical Problems*. Addison-Wesley, 1962.

[Ham81] Y. O. Hamidoune. An application of connectivity theory in graphs to factorizations of elements in groups. *Europ. J. Comb.*, 2:349–355, 1981.

[Ham90] Y. O. Hamidoune. On some graphic aspects of addition theorems. In R. Bodendiek and R. Henn, editors, *Topics in Combinatorics and Graph Theory*, pages 349–355. Physica Verlag, Heidelberg, 1990.

[Har69] F. Harary. *Graph Theory*. Addison-Wesley, 1969.

[Hel78] P. Hell. Graphs with given neighbourhoods I. In *Proc. Colloque Internat. CNRS (Orsay 1976)*, pages 219–223. CNRS, Paris, 1978.

[Hen72] C.W. Henson. Countable homogeneous relational structures and $\aleph_0$-categorical theories. *J. Symbolic Logic*, 37:494–500, 1972.

[Her67] C. Hering. Eine Bemerkung über Automorphismengruppen von endlichen projektiven Ebenen und Möbiusebenen. *Arch. Math.*, 18:107–110, 1967.

[Het76] D. Hetzel. *Über reguläre graphische Darstellungen von auflösbaren Gruppen*. PhD thesis, Technische Universität Berlin, 1976. Diplomarbeit.

[HL69] Z. Hedrlín and J. Lambek. How comprehensive is the category of semigroups? *J. Algebra*, 11:195–212, 1969.

[Hol81] D. F. Holt. A graph which is edge transitive but not arc transitive. *J. Graph Theory*, 5:201–204, 1981.

[Hop44] H. Hopf. Enden offener Räume und unendliche diskontinuierliche Gruppen. *Comment. Math. Helv.*, 16:81–100, 1944.

[HP65] Z. Hedrlín and A. Pultr. Symmetric relations (undirected graphs) with given semigroups. *Monatsh. Math.*, 69:318–322, 1965.

[HP66] Z. Hedrlín and A. Pultr. On full embeddings of categories of algebras. *Illinois J. Math.*, 10:392–406, 1966.

[Hru92] E. Hrushovski. Extending partial isomorphisms of graphs. *Combinatorica*,

12:411–416, 1992.

[HT72] J. E. Hopcroft and R. E. Tarjan. Isomorphism of planar graphs. In R. M. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 131–152. Plenum Press, 1972.

[HT73] J. E. Hopcroft and R. E. Tarjan. Dividing a graph into triconnected components. *SIAM J. on Computing*, 2:135–158, 1973.

[Hup57] B. Huppert. Zweifach transitive auflösbare Permutationsgruppen. *Math. Z.*, 68:126–150, 1957.

[Hup67] B. Huppert. *Endliche Gruppen I.* Springer Verlag, Berlin, 1967.

[Hur93] A. Hurwitz. Über algebraische Gebilde mit eindeutigen Transformationen in sich. *Math. Ann.*, 41:403–442, 1893.

[HW74] J. E. Hopcroft and J. K. Wong. Linear time algorithm for isomorphism of planar graphs. In *Proc. 6th ACM Symposium on Theory of Computing*, pages 172–184, 1974.

[HW90] J. Hemmeter and A. Woldar. On the maximal cliques of the quadratic forms graph in even characteristic. *European J. Comb.*, 11:119–126, 1990.

[II88] A.A. Ivanov and A.V. Ivanov. Distance-transitive graphs of valency $8 \leq k \leq 13$. In *Algebraic, Extremal and Metric Combinatorics*, pages 112–145. Cambridge Univ. Press, 1988.

[Imr71] W. Imrich. Assoziative produkte von graphen. *Sitzungsb. II, Österr. Akad. Wiss., Math. Naturw. Kl.*, 180:203–239, 1971. MR 47,♯4863.

[Imr77] W. Imrich. Subgroup theorems and graphs. In *Combinatorial Mathematics V*, volume 622 of *Springer Lecture Notes in Math.*, pages 1–27. Springer Verlag, 1977.

[Imr89] W. Imrich. Embedding graphs into cartesian products. In *Proceedings of the First China-USA International Conference on Graph Theory and its Applications*, volume 576 of *Annals New York Acad. Sci.*, pages 266 – 274. 1989.

[Imr93] W. Imrich. Graph products. a survey. unpublished, 1993.

[Iva83] A.A. Ivanov. Bounding the diameter of a distance regular graph. *Soviet Math. Dokl.*, 28:149–152, 1983.

[Jac86] Bill Jackson. Longest cycles in 3-connected cubic graphs. *J. Comb. Theory, Ser. B*, 41:17–26, 1986.

[Jer85] M. Jerrum. The complexity of finding minimum-length generator sequences. *Theor. Comp. Sci.*, 36:265–289, 1985.

[Jer86] M. Jerrum. A compact representation for permutation groups. *J. of Algorithms*, 7:60–78, 1986.

[Joh63] S.M. Johnson. Generation of permutations by adjacent transpositions. *Math. Comput.*, 17:282–285, 1963.

[Jón81] B. Jónsson. Arithmetic of ordered sets. In *Ordered Sets*, NATO ASI Ser. C, pages 3 – 41. Reidel, 1981.

[Jor95] C. Jordan. Nouvelles recherches sur la limite de transitivité des groupes qui ne contiennent pas le groupe alterné. *Journ. de Mathématiques*, 1:35–60, 1895.

[JS78] G.A. Jones and D. Singerman. Theory of maps on orientable surfaces. *Proc. London Math. Soc.*, 37:273–307, 1978.

[JW80] M. Jungerman and A.T. White. On the genus of finite abelian groups. *European J. Comb.*, 1:243–251, 1980.

[Kan69] W. M. Kantor. Automorphism groups of designs. *Math. Z.*, 109:246–252, 1969. MR 43♯71.

[Kan72] W. M. Kantor. k-homogeneous groups. *Math. Z.*, 124:261–265, 1972.

[Kan85a] W. M. Kantor. Polynomial-time algorithms for finding elements of prime order and Sylow subgroups. *J. Algorithms*, 6:478–514, 1985.

[Kan85b] W.M. Kantor. Sylow's theorem in polynomial time. *J.C.S.S.*, 30:359–394, 1985.

[Ker21] B. v. Kerékjártó. Über die periodischen Transformationen der Kreisscheibe und der Kugelfläche. *Math. Ann.*, 80:36–38, 1921.

[Kes59] H. Kesten. Symmetric random walks on groups. *Trans. A.M.S.*, 92:336–354, 1959.

[KL75] V.L. Kompel'macher and V.A. Liskovets. Sequential generation of permutations by means of a basis of transpositions (in russian). *Kibernetika*, pages 17–21, 1975.

[Kli81] M.H. Klin. On edge but not vertex transitive graphs. In *Algebraic Methods in Graph Theory*, pages 405–434. North-Holland, 1981. Colloq. Math. Soc. Bolyai, Szeged, 1978.

[KLM89] W.M. Kantor, M.W. Liebeck, and H.D. Macpherson. $\aleph_0$-categorical structures smoothly approximable by finite substructures. *Proc. LMS*, 59:439–463, 1989.

[KMF91] M.H. Klin, M.E. Muzychuk, and L.A. Faradžev. Cellular rings and groups of automorphisms of graphs. In *Investigations in the Algebraic Theory of Combinatorial Objects*. Kluwer, 1991.

[KN89] H.A. Kierstead and P.J. Nyikos. Hypergraphs with finitely many isomorphism subtypes. *Trans. Amer. Math. Soc.*, 312:699–718, 1989.

[Knu91] D.E. Knuth. Notes on efficient representation of perm groups. *Combinatorica*, 11:57–68, 1991. prelim. version circulated since 1981.

[Knu94] D.E. Knuth. The sandwich theorem. *Electronic J. Combinatorics*, 1, 1994. 48pp.

[Kön36] D. König. *Theorie der endlichen und unendlichen Graphen*. Akad. Verlagges. Geest u. Portig, Leipzig, 1936.

[Koz77] D. Kozen. Lower bounds for natural proof systems. In *Proc. 18th ACM Symposium on Theory of Computing*, pages 254–266, 1977.

[Kuč87] L. Kučera. Canonical labeling of regular graphs in linear average time. In *Proc. 28th Ann. IEEE Symp. on Theory of Computing*, pages 271–279, 1987.

[KW85] K. Keating and D. Witte. On Hamilton cycles in Cayley graphs in groups with cyclic commutator subgroup. In *Cycles in Graphs (Burnaby, B.C. 1982)*. North-Holland, 1985. North-Holland Math. Stud 115, MR 87f:05082.

[Lac86] A.H. Lachlan. Homogeneous structures. In *Proc. of the International Congress of Math.*, pages 314–321, 1986.

[Lal81] F. Lalonde. Le probleme d'etoiles pour graphes est NP-complet. *Discrete Math*, 33:271–280, 1981.

[Lei92] F. T. Leighton. *Introduction to parallel algorithms and architectures: arrays, trees, hypercubes*. Morgan Kaufman, San Mateo, CA, 1992.

[Leo91] J. S. Leon. Permutation group algorithms based on partitions I: Theory and

algorithms. *J. Symb. Comput.*, 12:533–583, 1991.

[LGH75] C. H. C. Little, D. D. Grant, and D. A. Holton. On defect-d matching in graphs. *Discrete Math.*, 13:41–54, 1975. Erratum, *ibid.* 14 (1976), 203.

[Lie83] M.W. Liebeck. On graphs whose full automorphism group is an alternating group or a finite classical group. *Proc. London Math. Soc.*, 47:337–362, 1983.

[Lie91] R.A. Liebler. The classification of distance-transitive graphs of type $q.k_{q,q}$. *European J. Comb.*, 12:125–128, 1991.

[Lov71] L. Lovász. On the cancellation law among finite relational structures. *Periodica Math. Hung.*, 1:145–156, 1971.

[Lov72a] L. Lovász. Direct product in locally finite categories. *Acta Sci. Math. (Szeged)*, 23:319–322, 1972.

[Lov72b] L. Lovász. A note on the line reconstruction problem. *J. Comb. Theory B*, 13:309–310, 1972.

[Lov79a] L. Lovász. *Combinatorial Problems and Exercises*. Akadémiai Kiadó, Budapest and North-Holland, Amsterdam, 1979. 2nd ed., 1993.

[Lov79b] L. Lovász. On the Shannon capacity of a graph. *IEEE Trans. Info. Theory*, 25:1–7, 1979.

[LP86] L. Lovász and M. D. Plummer. *Matching Theory*. North Holland, Akadémiai Kiadó, 1986.

[LPS87a] M.W. Liebeck, C.E. Praeger, and J. Saxl. A classification of the maximal subgroups of the finite alternating and symmetric groups. *J. Algebra*, 111:365–383, 1987.

[LPS87b] M.W. Liebeck, C.E. Praeger, and J. Saxl. Distance transitive graphs with symmetric or alternating automorphism group. *Bull. Austral Math. Soc.*, 35:1–25, 1987.

[LPS88a] M.W. Liebeck, C.E. Praeger, and J. Saxl. On the 2-closures of finite permutation groups. *J. London Math. Soc*, 37:241–252, 1988.

[LPS88b] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8, 1988.

[LS77] R.C. Lyndon and P.E. Schupp. *Combinatorial Group Theory*. Springer Verlag, 1977.

[Lub81] A. Lubiw. Some NP-complete problems similar to graph isomorphism. *SIAM J. Comp.*, 10:11–21, 1981.

[Luk82] E.M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *J. Comp. Sys. Sci.*, 25:42–65, 1982.

[Luk87] E.M. Luks. Computing the composition factors of a permutation group in polynomial time. *Combinatorica*, 7:87–99, 1987.

[LV89] N. Linial and U. Vazirani. Graph products and chromatic numbers. In *Proc. 30th IEEE Symp. Found. of Computer Science*, pages 124–128, 1989.

[LW65] D. Livingstone and A. Wagner. Transitivity of finite permutation groups on unordered sets. *Math. Z.*, 90:393–403, 1965.

[LW80] A. H. Lachlan and R. E. Woodrow. Countable homogeneous undirected graphs. *Trans. Amer. Math. Soc.*, 262:51–49, 1980.

[Mac67] A.M. Macbeath. The classification of non euclidean plane crystallographic

groups. *Canad. J. Math.*, 6:1192–1205, 1967.

[Mac82] H.D. Macpherson. Infinite distance-transitive graphs of finite valency. *Combinatorica*, 2:63–70, 1982.

[Mad71a] W. Mader. Minimale n-fach kantenzusammenhängende Graphen. *Math. Ann.*, 191:21–28, 1971.

[Mad71b] W. Mader. Über den Zusammenhang symmetrischer Graphen. *Arch. Math.*, 22:333–336, 1971.

[Man71] P. Mani. Automorphismen von polyedrischen Graphen. *Math. Ann.*, 192:297–303, 1971.

[Mar85] D. Marušič. Vertex transitive graphs and digraphs of order p^k. In *Cycles in Graphs (Burnaby, B.C. 1982)*, pages 115–128. North-Holland, 1985. North-Holland Math. Stud 115; MR 87b:5067.

[Mar87] D. Marušič. Hamiltonian cycles in vertex symmetric graphs of order $2p^2$. *Discrete Math.*, 66:169–174, 1987.

[Mar88] G.A. Margulis. Explicit group theoretic construction of combinatorial schemes and their application for the construction of expanders and concentrators. *Probl. Info. Transmission*, 24, 1988.

[Mas96] H. Maschke. The representation of finite groups, especially of the rotation groups of the regular bodies of three- and four-dimensional space, by Cayley's color diagrams. *Amer. J. Math.*, 18:156–194, 1896.

[Mat79] R. Mathon. A note on the graph isomorphism counting problem. *Inf. Proc. Letters*, 8:131–132, 1979.

[Mat87] B.H. Matzat. *Konstructive Galoistheorie*. Springer, Berlin-Heidelberg-New York, 1987. Lecture Notes in Math. 1284.

[McC63] R. McConnel. Pseudo-ordered polynomials over a finite field. *Acta Arith.*, 8:127–151, 1963.

[McK71] R. McKenzie. Cardinal multiplication of structures with a reflexive relation. *Fund. Math.*, 75:60–101, 1971.

[McK84] P. McKenzie. Permutations of bounded degree generate groups of polynomial diameter. *Info. Proc. Letters*, 19:253–254, 1984.

[McK87] B. D. McKay. Nauty user's guide, version 1.2. Tech. rep. tr-cs-87-03, Dept. Comp. Sci., Australian National Univ., Canberra, 1987.

[Men78a] E. Mendelsohn. Every (finite) group is the group of automorphisms of a (finite) strongly regular graph. *Ars. Combinatoria*, 6:75–86, 1978. MR 81a:05065.

[Men78b] E. Mendelsohn. On the groups of automorphisms of Steiner triple and quadruple systems. *J. Comb. Theory A*, 25:97–104, 1978. MR 80d:05010.

[MGT] S. Markvorsen, S.Mc. Guinness, and C. Thomassen. Transient random walks on graphs and metric spaces with applications to hyperbolic surfaces. to appear.

[Mih58] K.A. Mihailova. The occurence problem for direct products of groups (in russian). *Dokl. Akad. Nauk SSSR*, 119:1103–1105, 1958. and *Mat. Sb. (N.S.)* 70:241–251, 1966.

[Mil68a] J. Milnor. Growth of finitely generated solvable groups. *J. Differential Geometry*, 2:447–449, 1968.

[Mil68b] J. Milnor. A note on curvature and fundamental groups. *J. Differential Geom-*

etry, 2:1–7, 1968.

[Mil79] G.L. Miller. Graph isomorphism, general remarks. *J. Comp. Syst. Sci.*, 18:128–142, 1979.

[Mil83a] G.L. Miller. Isomorphism of graphs which are pairwise k-separable. *Inf. and Control*, 56:21–33, 1983.

[Mil83b] G.L. Miller. Isomorphism of k-contractible graphs. A generalization of bounded valence and bounded genus. *Inf. and Control*, 56:1–20, 1983.

[MKS66] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial Group Theory*. Interscience, N.Y., 1966.

[Mnu87] V.B. Mnukhin. Reconstruction of k-orbits of a permutation group. *Math. Notes*, 42:975–980, 1987.

[Moo64] J.W. Moon. Tournaments with a given automorphism group. *Canad. J. Math.*, 16:485–489, 1964. MR 29:603.

[MP83] D. Marušič and T.D. Parsons. Hamiltonian paths in vertex-symmetric graphs of order $4p$. *Discrete Math.*, 43:91–96, 1983.

[MR92] G.L. Miller and V. Ramachandran. A new graph triconnectivity algorithm and its parallelization. *Combinatorica*, 12:53–76, 1992.

[Mül77] V. Müller. The edge reconstruction hypothesis is true for graphs with more than $n \log_2 n$ edges. *J. Comb. Theory B*, 22:281–283, 1977.

[MW84] B.D. McKay and N.C. Wormald. Automorphism of random graphs with specified degrees. *Ars Combinatorica*, 19A:15–26, 1984.

[MW89] B. Mohar and W. Woess. A survey on spectra of infinite graphs. *Bull. London Math. Soc.*, 21:209–234, 1989.

[MZ55] D. Montgomery and L. Zippin. *Topological Transformation Groups*. Interscience, N.Y., 1955.

[Now68] L.A. Nowitz. On the non-existence of graphs with transitive generalized dicyclic groups. *J. Comb. Theory*, 4:49–51, 1968.

[NP92] P. M. Neumann and C. E. Praeger. A recognition algorithm for special linear groups. *Proc. London Math. Soc.*, 65:555–603, 1992.

[NW78] C.St.J.A. Nash-Williams. The reconstruction problem. In *Selected Topics in Graph Theory*, pages 205–236. Academic Press, London, 1978.

[Ore62] O. Ore. *Theory of Graphs*, volume 38 of *Colloq. Publ.* A.M.S., Providence, 1962.

[Oxt80] J. C. Oxtoby. *Measure and Category*, volume 2 of *Grad. Texts in Math.* Springer, 1980.

[Pál82] P.P. Pálfy. A polynomial bound on the orders of primitive solvable groups. *J. Algebra*, 77:127–137, 1982.

[Pól37] G. Pólya. Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen. *Acta. Math*, 68:145–254, 1937.

[Pra85] C.E. Praeger. Imprimitive symmetric graphs. *Ars. Combin. A*, 19:149–163, 1985. MR 86k:5058.

[Pra90] C.E. Praeger. Finite vertex transitive graphs and primitive permutation groups. In D. Jungnickel and S.A. Vanstone, editors, *Codes, Designs, Groups, Marshall Hall Conference, Vermont*, pages 51–65. Wiley, 1990.

[Pro77] V.K. Proulx. *Classification of the toroidal groups*. PhD thesis, Columbia Uni-

versity, 1977.

[PSY87] C.E. Praeger, J. Saxl, and K. Yokoyama. Distance transitive graphs and finite simple groups. *Proc. London Math. Soc.*, 55:1–21, 1987.

[PT80] A. Pultr and V. Trnková. *Combinatorial, Algebraic and Topological Representations of Groups, Semigroups and Categories*. Academia Praha, Prague, 1980.

[Pyb90] L. Pyber. The edge reconstruction of hamiltonian graphs. *J. Graph Theory*, 14:173–179, 1990.

[Qui86] J-J. Quisquater. *Structures d'interconnection: construction et applications*. PhD thesis, 1986.

[Rag72] M.S. Raghunathan. *Discrete Subgroups of Lie Groups*. Springer-Verlag, New York - Heidelberg, 1972.

[Ran48] R.A. Rankin. A campanological problem in group theory. *Proc. Cambridge Phil. Soc.*, 44, 1948.

[Rob70] R.W. Robinson. Enumeration of non-separable graphs. *J. Comb. Theory*, 9:327–356, 1970.

[RS59] E. Rapaport-Strasser. Cayley color groups and Hamilton lines. *Scripta Math.*, 24:51–58, 1959.

[RY68] G. Ringel and J.W.T. Youngs. Solution of the Heawood map-coloring problem. *Proc. Nat. Acad. Sci. USA*, 60:438–445, 1968.

[Sab57] G. Sabidussi. Graphs with given automorphism group and given graph theoretical properties. *Canad. J. Math.*, 9:515–525, 1957.

[Sab60] G. Sabidussi. Graph multiplication. *Math. Z*, 72:446–457, 1960.

[Sab64] G. Sabidussi. Vertex-transitive graphs. *Monatsh. Math.*, 68:426–438, 1964.

[Sch65] D.S. Schonland. *Molecular Symmetry*. Van Nostrand, London, 1965.

[Sch73] A.J. Schwenk. Almost all trees are cospectral. In F. Harary, editor, *New directions in the Theory of Graphs*, pages 275–308. Academic Press, New York, 1973.

[Sch79] J. Schmerl. Countable homogenous partially ordered sets. *Algebra Universalis*, 9:317–321, 1979.

[Ser77] J.-P. Serre. *Arbres, amalgames, SL_2*, volume 46 of *Astérisque*. Société Mathématique de France, Paris, 1977.

[Ser80] J-P. Serre. *Trees*. Springer-Verlag, Berlin-Heidelberg-New York, 1980.

[She80] S. Shelah. On a problem of Kurosh, Jónsson groups and applications. In *Word Problems II.*, pages 373–394. North Holland, 1980.

[Sim67] C.C. Sims. Graphs and finite permutation groups. *Math. Z.*, 95:76–86, 1967.

[Sim70] C.C. Sims. Computational methods in the study of permutation groups. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 169–183. Pergamon Press, 1970.

[Sim71] C.C. Sims. Computation with permutation groups. In *Proc. 2nd Symp. Symb. Algeb. Manipulation*, pages 23–28. ACM, 1971.

[Sim78] C.C. Sims. Some group theoretic algorithms. Springer Lect. Notes in Math. 697, pages 108–124. Springer Verlag, 1978.

[Smi74] D.H. Smith. Distance-transitive graphs of valency four. *J. London Math. Soc.*, 8:377–384, 1974.

[Spe83] J. Spencer. What's not inside a Cayley graph? *Combinatorica*, 3:239–241, 1983.

[Sta71] J. Stallings. *Group Theory and Three-Dimensional Manifolds*. Yale Univ. Press, New Haven, 1971.

[Sto77] P.K. Stockmeyer. The falsity of the reconstruction conjecture for tournaments. *J. Graph Theory*, 1:19–25, 1977.

[Tar92] G. Tardos. Intersection of subgroups of a free group. *Inventiones Math.*, 108:29–36, 1992.

[Tho83] C. Thomassen. Girth in graphs. *J. Combinat. Theory, Ser. B*, 35:129–141, 1983.

[Tho84] J.G. Thompson. Some finite groups which appear as $Gal(L/K)$ where $K \subseteq Q(\mu_n)$. *J. Algebra*, 89:437–499, 1984.

[Tho87] Simon Thomas. The infinite case of the edge-orbit conjecture. *Alg. Universalis*, 24:167–168, 1987.

[Tho90] C. Thomassen. Resistances and currents in infinite electrical networks. *J. of Comb. B*, 49:87–102, 1990.

[Tho91] C. Thomassen. Tilings of the torus and the Klein bottle and vertex-transitive graphs on a fixed surface. *Trans. Amer. Math. Soc.*, 323:605–635, 1991.

[Tho92] C. Thomassen. The Hadwiger number of infinite vertex-transitive graphs. *Combinatorica*, 12:481–491, 1992.

[Tit59] J. Tits. Sur la trialité at certains groupes qui s'en déduisent. *Publ. Math. I.H.E.S.*, 2:14–60, 1959.

[Tit70] J. Tits. Sur le groupe des automorphismes d'un arbre. In *Essays on Topology and Related Topics (Mémoires dédiés á Georges de Rham*, pages 188–211. Springer, 1970.

[Tit72] J. Tits. Free subgroups of linear groups. *J. Algebra*, 20:250–270, 1972.

[Tit75] V.K. Titov. On the symmetry of graphs. In *Voprosy Kibernetiki (Proc. of the 2nd All-Union Seminar on Combinatorial Math., Moscow)*, volume 15, pages 76–109, 1975.

[Tro85] V.I. Trofimov. Graphs with polynomial growth. *Math. USSR Sbornik*, 51:405–417, 1985.

[Tro92] V.I. Trofimov. On the action of a group on a graph. *Acta Applicandae Math.*, 29:161–170, 1992.

[Tru92] J.K. Truss. Generic automorphisms of homogeneous structures. *Proc. London Math. Soc.*, 65:121–141, 1992.

[Tuc83] T.W. Tucker. Finite groups acting on surfaces and the genus of a group. *J. Comb. Theory B*, 34:82–98, 1983.

[Tuc84] T.W. Tucker. On Proulx's four exceptional toroidal groups. *J. Graph Theory*, 8:29–33, 1984.

[Tut47] W.T. Tutte. A family of cubical graphs. *Proc. Cambr. Phil. Soc.*, 43:459–474, 1947.

[Tut79] W.T. Tutte. All the king's horses. In J.A. Bondy and U.S.R. Murty, editors, *Graph Theory and Related Topics*, pages 15–33. Academic Press, 1979.

[TW94] C. Thomassen and W. Woess. Vertex-transitive graphs and accessibility. *J. Combinat. Theory - B*, 26:1–60, 1994.

[Var85] N.Th. Varopoulos. Isoperimetric inequalities and Markov chains. *J. of Functional*

Analysis, 63:215–239, 1985.

[Var91] N.Th. Varopoulos. Analysis and geometry on groups. In *Proc. Internat. Congr. Math., Kyoto 1990*, pages 951–957. Springer, Kyoto, 1991.

[VPH65] P. Vopenka, A. Pultr, and Z. Hedrlín. A rigid relation exists on any set. *Comment. Math. Univ. Carolinae*, 6:149–155, 1965.

[Wat70] M.E. Watkins. Connectivity of transitive graphs. *J. Comb. Theory*, 8:23–29, 1970.

[Wat71] M.E. Watkins. On the action of non-abelian groups on graphs. *J. Comb. Theory B*, 1:95–104, 1971.

[Wei76a] R. Weisfeiler, editor. *On Construction and Identification of Graphs*. Lecture Notes in Math. 556. Springer, 1976.

[Wei76b] R.M. Weiss. Über lokal s-reguläre Graphen. *J. Comb. Theory B*, 20:124–127, 1976.

[Wei79] R. M. Weiss. Elations of graphs. *Acta Math. Acad. Sci. Hungary*, 34:101–103, 1979.

[Wei81] R.M. Weiss. The nonexistence of 8-transitive graphs. *Combinatorica*, 1:309–311, 1981. MR 84f:05050.

[Wei85a] R.M. Weiss. Distance-transitive graphs and generalized polygons. *Arch. Math. (Basel)*, 45:186–192, 1985. MR 87a:05081.

[Wei85b] R.M. Weiss. On distance transitive graphs. *Bull. London Math. Soc.*, 17:253–256, 1985.

[WG84] D. Witte and J.A. Gallian. A survey: Hamiltonian cycles in Cayley graphs. *Discrete Math.*, 51:293–304, 1984.

[Whi32] H. Whitney. Congruent graphs and the connectivity of graphs. *Amer. J. Math*, 54:150–168, 1932. Jbuch 58, 609 [see Lovász, Problem 15.1].

[Whi73] A.T. White. *Graphs, Groups, and Surfaces*. North-Holland, 1973.

[Whi85] A.T. White. Ringing the changes II. *Ars Combin. A*, 20:65–75, 1985. MR 87e:05080.

[Wie64] H. Wielandt. *Finite Permutation Groups*. Acad. Press, N.Y., 1964.

[Wie69] H. Wielandt. Permutation groups through invariant relations. Lecture notes, Ohio State University, 1969.

[Wig27] E. Wigner. Einige Folgerungen aus der Schrödingerschen Theorie für die Termstrukturen. *ZS. f. Phys.*, 43:624–652, 1927.

[Wig59] E.P. Wigner. *Group Theory and its Application to the Quantum Mechanics of Atomic Spectra*. Academic Press, New York, 1959.

[Wil66] H. C. Wilkie. On non-euclidean crystallographic groups. *Math. Z.*, 91:87–102, 1966.

[Wil74] R.M. Wilson. Nonisomorphic Steiner triple systems. *Math. Z.*, 135:303–313, 1974.

[Wit86] D. Witte. Cayley digraphs of prime-power order are Hamiltonian. *J. Comb. Theory B*, 40:107–112, 1986.

[Wol68] J.A. Wolf. Growth of finitely generated solvable groups and curvature of Riemannian manifolds. *J. Differential Geometry*, 2:421–446, 1968.

[Wol82] T.R. Wolf. Solvable and nilpotent subgroups of $GL(n, q^m)$. *Can. J. Math.*,

34:1097–1111, 1982.

[Won67] W.J. Wong. Determination of a class of permutation groups. *Math. Z.*, 99:235–246, 1967.

[Woo79] R.E. Woodrow. There are four countable ultrahomogeneous graphs without triangles. *J. Comb. Theory (B)*, 27:168–179, 1979.

[Wor86] N. Wormald. A simpler proof of the asymptotic formula for the number of unlabelled r-regular graphs. *Indian J. Math.*, 28:43–47, 1986.

[Wri71] E.M. Wright. Graphs on unlabelled nodes with a given number of edges. *Acta. Math.*, 126:1–9, 1971.

[ZKT85] V.M. Zemlyachenko, N.M. Kornienko, and R.I. Tyshkevich. Graph isomorphism problem. *J. of Soviet Mathematics*, 29:1426–1481, 1985. Original in Zapiski LOMI Vol. 118, 1982.

[ZVC80] H. Zieschang, E. Vogt, and H-D. Coldewey. *Surfaces and Planar Discontinuous Groups*, volume 835 of *Lect. Notes in Math.* Springer, 1980.