

## ON TRANSITIVE PERMUTATION GROUPS

JOHN H. CONWAY, ALEXANDER HULPKE AND JOHN MCKAY

*Abstract*

We assign names and new generators to the transitive groups of degree up to 15, reflecting their structure.

1. *Introduction*

The classification of transitive permutation groups has been pursued for over a century since the 1860 Grand Prix of the Académie des Sciences (announced in 1857 [1]). An account of early work is given in [3] and [12]; a very readable historical outline can be found in [16, Appendix A].

This work led to a classification of the groups up to degree 15 [10], [11], [9]. Having achieved these results, development stopped for some time and was taken up again with the arrival of symbolic computation. The last twenty years have seen extensive work in this area [2] [14], [4] noting errors in earlier tables. Recent work by one of the authors [7] confirms these results, and extends the tables to higher degrees.

Previous workers have given arbitrary generators and a few properties of the groups. For practical work it is desirable to give inherently meaningful names to these groups, as well as generators reflecting more properties.

With this aim we have devised a naming scheme for transitive permutation groups, and apply it to the groups of degree up to 15. Based on the names, we try to find new, “better” generators for the groups, simultaneously confirming the correctness of the names.

Finally, the process of finding names is, to some extent, an actual construction process without tests for conjugacy. So the naming process might be regarded as another test for completeness of the lists.

As usual we speak of “the transitive groups”, meaning “the equivalence classes up to permutation isomorphism”, namely “a set of representatives for the conjugacy classes of transitive groups in the symmetric group”.

2. *Taxonomy*

In this section we present a scheme for assigning names to transitive permutation groups, based on their permutational structure. Whereas the goal of assigning a unique name to each individual transitive permutation group cannot be achieved for all degrees, the scheme presented here is powerful enough for individual naming of all groups of degree up to 15. Conversely, we do not attempt to give names so explicit that one can deduce a generating set for every group based solely on its name. It should be possible, however, to identify

---

The first-named author was supported in part by NSF funding.

The second-named author was supported by DFG, NSERC and FCAR funding.

The third-named author was supported in part by NSERC and FCAR funding.

Received 1st August 1996, revised 8th December 1997; *published 1st June 1998.*

1991 Mathematics Subject Classification 20B35

© 1998, John H. Conway, Alexander Hulpke and John McKay

the group belonging to a name in a list of representatives of the transitive groups without having to determine the correspondence of the whole list to the catalogue printed here.

As we need to distinguish between *permutation isomorphism types* and *names*, we denote names or parts of names used by enclosing them thus:  $\langle\langle G \rangle\rangle$ .

### 2.1. Modifications to the ATLAS notation

As a basis we use the notation of the ATLAS [5], to which we refer also for the names and definitions of the simple groups. The name of a group reflects its subnormal structure, written from left to right in ascending order. The subnormal series is chosen to be compatible with permutational structures, namely kernels of block operations.

Direct products are denoted by “ $\times$ ”, split extensions by “ $\cdot$ ” and nonsplit extensions by “ $\rtimes$ ”. A dot itself “ $\cdot$ ” is used only to separate a normal subgroup and its factor without giving further information about the extension structure.

To such a name, additional information is added in brackets to denote permutation specific information. A group name followed by a number  $n$  in round brackets ‘ $(n)$ ’ denotes that the group operates transitively on  $n$  points, or respectively that a point stabilizer has index  $n$  in the group. Square brackets “[, ]” denote normal structures corresponding to permutational concepts. Curly brackets “{, }” give further information (“hints”) towards the construction. For example, several nonisomorphic transitive representations of one group might be distinguished by a hint towards the point stabilizer of the form  $\langle\langle X(n\{\text{stab}\}) \rangle\rangle$ . We explain the hints given after a description of the basic names (Section 2.5).

### 2.2. Natural names

Some families of groups containing one member for each degree are given natural names. A name of the form  $\langle\langle X(n) \rangle\rangle$  denotes the  $n$ -th member of this family as a permutation group on  $n$  points. The same group is denoted by  $\langle\langle X_n \rangle\rangle$  if it occurs as an abstract group but not necessarily with this action. Exceptions are dihedral and Frobenius groups, for which traditionally the *size* is indicated by an index. Thus  $\langle\langle D(4) \rangle\rangle = \langle\langle D_8(4) \rangle\rangle$  is the dihedral group of size 8. We sum up the names used in the following list:

$A$	Alternating	$F$	Frobenius	$E$	Elementary
$S$	Symmetric	$AL$	Affine linear	$C$	Cyclic
$M$	Mathieu	$D$	Dihedral		

In addition, we use  $\langle\langle L(n) \rangle\rangle$  to denote groups derived from linear groups as defined in Table 1.

### 2.3. Group products

If  $G$  acts transitively on  $\Omega$ , and  $H$  on  $\Delta$ , the direct product has a transitive representation on  $\Omega \times \Delta$ . This is denoted by  $\langle\langle G[\times]H \rangle\rangle$ .

A subdirect product (see [13]) corresponding to two epimorphisms  $\alpha: G \rightarrow F$  and  $\beta: H \rightarrow F$  with  $|F| = m$  is denoted by  $\langle\langle G[\frac{1}{m}]H \rangle\rangle$ . If several subdirect products exist, further information is given in hints towards the epimorphisms:  $\langle\langle G\{\alpha\}[\frac{1}{m}]\{\beta\}H \rangle\rangle$ . If  $F$  is abelian, there is a special subdirect product of  $n$  copies of  $G$ , which is the “augmentation ideal” construction

$$\langle\langle \frac{1}{m}(G^n) \rangle\rangle = \{(g_1, \dots, g_n) \mid g_1^{\alpha_1} \cdots g_n^{\alpha_n} = 1_F\}.$$

Again a hint,  $\langle\langle \frac{1}{m}\{\alpha\}G^n \rangle\rangle$ , can be given to the defining homomorphism(s).

Table 1: The permutation groups  $L(n)$

Name	Size	Type
$L(6)$	60	$PSL(2, 5) = A_5(6)$
$L(7)$	168	$PSL(3, 2)$
$L(8)$	168	$PSL(2, 7)$
$L(9)$	504	$PSL(2, 8)$
$L(10)$	360	$PSL(2, 9)$
$L(11)$	660	$PSL(2, 11)(11)$
$L(12)$	660	$PSL(2, 11)$
$L(13)$	5616	$PSL(3, 3)$
$L(14)$	1092	$PSL(2, 13)$
$L(15)$	20160	$PSL(4, 2) = A_8(15)$

We need to describe intransitive actions of (iterated) (sub)direct products, as an intransitive permutation group  $G \times H$  — and therefore all subdirect products of  $G$  with  $H$  — can be represented on the disjoint union  $\Omega \uplus \Delta$ .

We now take a group  $A$  acting on  $\Omega$  and consider the direct product  $A^m = A_1 \times \cdots \times A_m$  acting on  $\Omega_1 \uplus \cdots \uplus \Omega_m$ . If  $U$  is a subgroup of  $A$  then  $\langle\langle U^m \rangle\rangle$  is the direct product, acting with each component  $U_i$  in the same way on  $\Omega_i$ . For  $k < m$  the group  $\langle\langle U^k \rangle\rangle$  also acts on all orbits in the same way. If  $u \in U^k$  acts as  $u_i$  on  $\Omega_i$  (and thus  $u = \prod u_i$ ), then  $u_i = u_j^{\alpha_{i,j}}$  where  $\alpha_{i,j}$  is a permutation isomorphism (depending only on  $U^k$  and not on  $u$ ) mapping  $U_j$  to  $U_i$ . So, as an intransitive group, the augmentation ideal is denoted by  $\langle\langle A^{m-1} \rangle\rangle$ .

Analogous rules apply to groups of the form  $\langle\langle U^j.V^k \rangle\rangle$  when  $U.V$  is a subgroup of  $A$ .

#### 2.4. Imprimitive constructions

By the embedding theorem [8] imprimitive groups can be embedded into suitable wreath products. We will use these wreath products to describe imprimitive groups: let  $C$  be a transitive group of degree  $l$  and  $H$  a permutation group of degree  $m$ ; then the wreath product  $C \wr H = W$  is a semidirect product  $C^m \rtimes H$  with  $H$  acting on  $C^m$  by permuting the  $m$  components according to the permutation action. We denote the complement to  $C^m$  in  $W$  by  $\hat{H}$ . It is an intransitive group, acting on  $l$  orbits with  $H$  acting simultaneously on the points. When embedding an imprimitive group into  $W$ , the kernel  $K$  of the action on the blocks embeds into  $C^m$  as an intransitive group acting on every orbit like a normal subgroup  $A$  of  $C$ .

For an intransitive subgroup,  $\langle\langle K \rangle\rangle$  of  $C^m$ , as defined in the last section  $\langle\langle [K]H \rangle\rangle$  is the split extension  $\langle\langle K, \hat{H} \rangle\rangle$ ; so the permutational wreath product  $A \wr H$  is denoted by  $\langle\langle [A^m]H \rangle\rangle$ .

When there are epimorphisms  $\beta: K \twoheadrightarrow F$  and  $\gamma: H \twoheadrightarrow F$  and  $|F| = m$ , then  $\langle\langle \frac{1}{m}[K]H \rangle\rangle$  is the subgroup of  $[K]H$  consisting of those elements  $kh$  for which  $k^\beta = h^\gamma$ . Again hints can be placed before the groups to give information about  $\beta$  and  $\gamma$ , leading to names of the form  $\langle\langle \frac{1}{m}\{\beta\}[K]\{\gamma\}H \rangle\rangle$ .

Other groups with the same action  $H$  on the blocks may differ in the part of  $H$  for which a complement in  $\hat{H}$  exists. This complementable part is called the “bodily part” of  $H$ . A group of this type will be called  $\langle\langle [K]H\{\text{bodily}\} \rangle\rangle$ .

Similarly, the kernel of the block operation may partially intersect with the  $K$  given in the name (the reason being that the proper kernel is not readily described). This leads to the

indication of a bodily part of  $K$ , and names of the form  $\langle\langle [K\{\text{bodily}\}]H\{\text{bodily}\} \rangle\rangle$ .

When the index of the bodily part suffices to distinguish groups, it is given as an index to the group names, for example  $\langle\langle [K_i]H_j \rangle\rangle$ . Instead of writing a number, a division sign ‘ $\div$ ’ can be used as an index to denote “fractional part” if this suffices to distinguish the groups. The bodily part of  $H$  is maximized if several possible embeddings exist.

The groups 17-20 of degree 10 may serve as examples: we take subdirect products of the Frobenius group  $F(5)$  of order 20 and degree 5 with itself, in which we “glue” together the factor groups of order 4. We arrange the points 0-9 in the following scheme

$$\begin{array}{cccccc} 0 & 2 & 4 & 6 & 8 \\ 5 & 7 & 9 & 1 & 3 \end{array}$$

with both factors of the subdirect product acting on one row to get orbits (which will become block systems of a transitive group later) via congruences. According to this scheme, the standard subdirect product is

$$5^2 : 4 = \langle(0, 2, 4, 6, 8), (5, 7, 9, 1, 3), (2, 4, 8, 6)(7, 9, 3, 1)\rangle.$$

If we apply the outer automorphism of the factor group, we get another subdirect product. Its intersection with  $5^2 : 4$  has size 50. In other words, the bodily part has index 2. Thus the group is

$$5^2 : 4_2 = \langle(0, 2, 4, 6, 8), (5, 7, 9, 1, 3), (2, 4, 8, 6)(7, 1, 3, 9)\rangle.$$

We extend these two intransitive groups by a factor group of order 2 so that the extension becomes transitive. The standard element of order 2, permuting the blocks, is the complement of the wreath product:

$$a = (0, 5)(2, 7)(4, 9)(6, 1)(8, 3).$$

Extending both subdirect products by this element gives the groups  $[5^2 : 4]2$  and  $[5^2 : 4_2]2$ .

For both subdirect products we take an element  $x$  of the direct product not in the subdirect product, such that  $(xa)^2$  is contained in the subdirect product. Then, extending the subdirect products by  $xa$ , we get a group that is transitive while its order has doubled; therefore, the subdirect product is the base group of this new group. The factor group 2 is not bodily, as otherwise  $x$  would be in the base group. Taking  $x = (2, 8)(4, 6)(7, 9, 3, 1)$ , we get the third group  $[5^2 : 4]2_2$ ; for the other subdirect product  $x = (7, 3)(1, 9)$  yields the fourth group  $[5^2 : 4_2]2_2$ . (Instead of writing  $[5^2 : 4_2]2_2$  we could have written  $[5^2 : 4_2]2_{\div}$ , but there is no advantage in doing so.)

### 2.5. Hints

Hints are given only if they are necessary to distinguish between different groups arising from the same general construction. A hint usually relates to the kernel of an homomorphism, the point stabilizer, or a bodily part. If the index of this subgroup suffices, it is given as an index. If there are two epimorphisms, one which is associated with the identity mapping of the image and one associated with a unique non-identity automorphism of the image, they are distinguished by indices “+” and “-”. (An omitted index always reads as “+”.)

We use single (non-capital) letter abbreviations for other frequent hints referring to subgroups. When standing alone these are written without surrounding hint brackets.

$c$	central or cyclic	$d$	odd or dihedral
$e$	even or elementary		
$i$	intransitive	$t$	transitive

The first three letters are reminiscent of the proper normal subgroups of the dihedral group,  $D_8(4)$ , of order 8, that can be denoted by  $4c = \langle(1, 2, 3, 4)\rangle$ ,  $4d = \langle(1, 3), (2, 4)\rangle$ ,  $4e = \langle(1, 2)(3, 4), (1, 3)(2, 4)\rangle$  and  $2c = \langle(1, 3)(2, 4)\rangle$ .

A hint of the form  $\{n(ind)\}$  after the group name indicates that the group has index  $\langle ind \rangle$  in its normalizer in the full symmetric group.

### 3. Lists

#### 3.1. Description of the tables

The points are numbered from 0 to  $deg - 1$ . (When groups may not act on 0, one should replace 0 by  $deg$ .) This permits us to arrange the numbers in such a way as to identify one block system per group, with congruence classes modulo the number of blocks. For two block systems with coprime block size we can even arrange the numbers to identify both block systems with congruence classes. The example in Section 2.4 typifies these arrangements.

If 0 is not available (for example on a computer), the numbers should not be shifted by 1, but 0 should be replaced by the appropriate degree of the permutation group to keep the congruence information.

We list the groups according to degree in the order in which they were published [2], [14] (as used in MAGMA[6]) and [4]. The same names and arrangements are used in GAP [15].

For each group we try to recreate a new set of generators that reflects the structure indicated by its name. We give these generators, and ensure that the new generators are correct by testing properties of the groups generated.

The groups and their properties are listed in Appendix A, in two sets of tables. The first set lists the groups and their properties. For each group, we give an index number which is in italic if the group is minimally transitive, namely if all its proper subgroups are intransitive. For each group we also give its name, size, parity (whether it is subgroup of the alternating group), the identification number of the normalizer in  $S_n$  as a transitive permutation group in this list, and the identification number of the 2-closure (the largest subgroup of  $S_n$  which has the same orbits on pairs of points, acting by  $(x, y)^g := (x^g, y^g)$ ). The column S gives information about the orbits of the point stabilizer: a fraction  $\frac{a}{b}$  denotes an orbit of size  $a$  for which the action on this orbit is of type  $b$  (as a transitive group of degree  $a$ ). Fixed points are omitted. Multiplicities are indicated by exponents. Finally, we give the generators and — if applicable — representatives for all block systems. To save space we give multiple-use blocks and generators at the beginning of each degree.

For example, let  $G$  be the 21st group of degree 8. It is generated by

$$h = (1, 5)(3, 7), \quad oe = (1, 4, 5, 8)(2, 3)(6, 7), \quad c = (0, 2)(1, 3)(4, 6)(5, 7).$$

It has four block systems, namely

$$\begin{aligned} 2 &= \{\{0, 4\}, \{1, 5\}, \{2, 6\}, \{3, 7\}\}, & x &= \{\{0, 2, 4, 6\}, \{1, 3, 5, 7\}\}, \\ x &= \{\{0, 3, 4, 7\}, \{1, 2, 5, 6\}\}, & x &= \{\{0, 1, 4, 5\}, \{2, 3, 6, 7\}\} \end{aligned}$$

which are determined by their blocks containing 0. These are abbreviated as 2, 4a, 4d and 4b respectively. The blocks of size 2 lead to the name  $\frac{1}{2}[2^4]E(4)$ : Arrange the points 0 to 3 in the first row and 4-7 in the second row of a  $2 \times 4$  array. The columns correspond to the blocks. The action on the blocks is equivalent to that of  $E(4)$ , so we can embed  $G$  into  $2 \wr E(4)$ . The base group  $2^3$  of  $G$  is generated by  $h$  and its conjugate images. Together with

$x = (1, 5)$  it generates the whole  $2^4$ . The standard base complement in  $2 \wr E(4)$  is generated by  $b = (0, 1)(2, 3)(4, 5)(6, 7)$  and  $c$ . However, in  $G$  a factor 2 of  $2^4$  is “glued” with a factor of the  $E(4)$ . So we get, instead of  $x$  and  $b$ , the product  $xb = oe$  as generator in addition to  $h$  and  $c$ .

All block systems with blocks of size 4 have a kernel which is a subdirect product of  $D(4)$  with itself, with a common elementary abelian factor of order 4. As there are different isomorphisms of the factor groups, there are  $|GL(2, 2)| = 6$  possible subdirect products of this type. The products are generated by the normal subgroup kernels  $\langle (0, 2)(1, 3), (4, 6)(5, 7) \rangle$  together with representatives of cosets generating the factor group. In the standard subdirect product these coset representatives form a subset of the diagonal. This leads to a group name  $[\frac{1}{4}D(4)^2]2$  for the 22nd group of degree 8, but it does not appear in the tables because it already has two better names. In fact, this subdirect product is a kernel of  $G$  corresponding to block system 4a; however, in this case, the extension does not split and the factor group is not bodily. So again there is an additional potential name,  $[\frac{1}{4}D(4)^2]2_2$ , which we disregard because there are better ones.

Two of the possible factor isomorphisms yield subdirect products that do not allow a transitive action of the normalizer. The remaining three subdirect products can be identified by the fact that the factor isomorphism identifies only one of the three subgroups of size 4 (denoted by “ $c$ ”, “ $d$ ” and “ $e$ ”) with itself. For example, in the above block arrangement, the product  $\frac{1}{4}dD(4)^2$  is generated by

$$\langle (0, 2)(1, 3), (4, 6)(5, 7), (1, 3)(5, 7), (0, 3)(1, 2)(4, 5, 6, 7) \rangle.$$

This group is permutation isomorphic to the kernel of  $G$  corresponding to the block systems 4b and 4d (which fuse under the action of  $N_{S_8}(G)$ ). This explains the second name  $[\frac{1}{4}dD(4)^2]2$ . (The two remaining products lead to the 15th and 19th groups of degree 8.) Of course, the generators cannot reflect this name as well.

The group  $G$  is of size 32, and contains elements (namely  $oe$ ) which are not contained in the alternating group. The normalizer of  $G$  in  $S_8$  is of type  $2^4D(4)$ , the 35th group; the 2-closure is of type  $2^4E(4)$ , the 31st group of degree 8. The point stabilizer has 3 orbits of size 2 and the action on each orbit is of type  $S_2$ . Every proper subgroup is intransitive.

The second set of tables indicates isomorphism classes within the lists. For each group we give the number of isomorphic groups in the list. To improve clarity, entries in a sequence of the same isomorphism type are denoted by a long dash (—).

#### 4. *Final remarks*

The names and new generators having been defined, all further computations were done with the aid of GAP. The tables were then created in a largely automated way, to reduce the possibility of errors when copying data.

For reference purposes we suggest the name “TPG1” for this scheme.

We finally list in Table 2 the numbers of transitive groups of degrees up to 31, as given in [7]. The increase in the numbers with degree 16 shows that a continuation of our work to higher degrees would be substantially harder. We thank Heiko Theißen for providing a program to compute the 2-closures for degree 15. The second author would like to thank CICMA at Concordia University, Montréal for the hospitality during his stay in early 1995.

Table 2: Transitive groups of degree up to 31

Degree	2	3	4	5	6	7	8	9	10	11
primitive	1	2	2	5	4	7	7	11	9	8
transitive	1	2	5	5	16	7	50	34	45	8
Total	2	4	11	19	56	96	296	554	1593	
Degree	12	13	14	15	16	17	18	19	20	21
primitive	6	9	4	6	22	10	4	8	4	9
transitive	301	9	63	104	1954	10	983	8	1117	164
Degree	22	23	24	25	26	27	28	29	30	31
primitive	4	7	5	28	7	15	14	8	4	12
transitive	59	7	<i>26813</i>	211	96	<i>2382</i>	<i>1852</i>	8	<i>5712</i>	12

Numbers in italics are preliminary, and not yet confirmed.

### Appendix A. *Classification tables*

The classification tables are provided as a separate file, as a special electronic appendix to this paper. This appendix is available to journal subscribers at:

<http://www.lms.ac.uk/jcm/1/lms96001/appendix-a/>.

### Appendix B. *Program for generating the tables*

A program file, used to produce the tables in [Appendix A](#), is available to journal subscribers at:

<http://www.lms.ac.uk/jcm/1/lms96001/appendix-b/>.

### *References*

1. ACADEMIE DES SCIENCES, ‘Grand prix de mathématiques’, *C. R. Acad. Sci. Paris XLIV* (1857), pp. 793–795. 1
2. Gregory BUTLER and John MCKAY, ‘The transitive groups of degree up to 11’, *Comm. Algebra* 11 (1983) 863–911. 1, 5
3. Heinrich BURCKHARDT, ‘Endliche discrete Gruppen’, *Encyclopädie der mathematischen Wissenschaften I*, erster Teil (eds W. F. Meyer, B. G. Teubner, Leipzig, 1898), pp. 208–226. 1
4. Greg[ory] BUTLER, ‘The transitive groups of degree fourteen and fifteen’, *J. Symb. Comput.* 16 (1993) 413–422. 1, 5
5. J[ohn] H. CONWAY, R[obert] T. CURTIS, S[imon] P. NORTON, R[ichard] A. PARKER and R[obert] A. WILSON. *ATLAS of finite groups* (Oxford University Press, 1985). 2
6. J[ohn] CANNON and C[atherine] PLAYOUST, *An introduction to MAGMA* (School of Mathematics and Statistics, University of Sydney, 1993). 5

7. Alexander HULPKE, *Konstruktion transitiver Permutationsgruppen*, PhD thesis, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, 1996. (Verlag der Augustinus Buchhandlung, Aachen, ISBN 3-86073-427-X). 1, 6
8. Marc KRASNER and Leo [A.] KALOUJNINE, ‘Produit complet des groupes de permutations et problème d’extension de groupes II’, *Acta Sci. Math. (Szeged)* 14 (1951) 39–66. 3
9. Harry W. KUHN, ‘On imprimitive substitution groups’, *Amer. J. Math.* 26 (1904) 45–102. 1
10. George A. MILLER, ‘List of transitive substitution groups of degree twelve’, *Quart. J. Pure Appl. Math.* 28 (1896) 193–231. Errata: *ibid.*, 29 (1898) 249. 1
11. George A. MILLER, ‘On the transitive substitution groups of degree thirteen and fourteen’, *Quart. J. Pure Appl. Math.* 29 (1898) 224–249. 1
12. George A. MILLER, ‘Historical note on the determination of all the permutation groups of low degrees’, *The Collected Works of George Abram Miller* 1 (ed. George A. MILLER, University of Illinois Press, 1935), pp. 1–9. 1
13. Robert REMAK. ‘Über die Darstellung der endlichen Gruppen als Untergruppen direkter Produkte’, *J. Reine Angew. Math.* 163 (1930) 1–44. 2
14. Gordon F. ROYLE, ‘The transitive groups of degree twelve’, *J. Symb. Comput.*, 4 (1987) 255–268. 1, 5
15. Martin SCHÖNERT *et al.*, *GAP 3.4, patchlevel 3*. (Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1995). 5
16. Mark W. SHORT. *The primitive soluble permutation groups of degree less than 256*, Lecture Notes in Mathematics 1519 (Springer, Heidelberg, 1992). 1

John H. Conway [conway@math.princeton.edu](mailto:conway@math.princeton.edu)

Mathematics Department  
Princeton University  
Princeton  
New Jersey  
USA

Alexander Hulpke [ahulpke@dcs.st-and.ac.uk](mailto:ahulpke@dcs.st-and.ac.uk)

School of Mathematical and Computational Sciences  
University of St. Andrews  
St. Andrews, Fife KY16 9SS  
Scotland

John McKay [mckay@cs.concordia.ca](mailto:mckay@cs.concordia.ca)

Departments of Computer Science and Mathematics  
Centre Interuniversitaire en Calcul Mathématique Algébrique  
Concordia University  
Montréal  
Canada H3G 1M8