MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 135
JULY 1976, PAGES 632–637

Groups of Square-Free Order, An Algorithm

By J. Alonso

Abstract. An abstract definition of the groups of square-free order is given that leads naturally to a programmable computation of their number. O. Hölder's alternative description of the groups of square-free order is incidentally derived.

Throughout this paper G will be a group of order $h = \Pi_{i=1}^n p_i$, where $p_1 > p_2 > \cdots > p_n$ are given prime numbers. O. Hölder proved in 1895 that the number of groups of order h is

$$\sum_S \left(\prod_{j=1}^r \frac{(p_{S(j)})^{c_{S(j)}} - 1}{p_{S(j)} - 1} \right), \tag{1}$$

where the sum extends to all the subsets $S = \{S(1), S(2), \ldots, S(r)\}$ of the set $\{2, 3, \ldots, n\}$; and $c_{S(j)}$ is the number of differences $p_i - 1$, $i \notin S$, which are divisible by p_j. The number of terms in (1) is very large even for small values of n; and therefore, it seems desirable to have a computer program that for each set of primes $\{p_1, p_2, \ldots, p_n\}$ skips the zero terms in (1).

The present paper makes no use of formula (1); it is an alternative approach to the description of the groups of order h and the determination of their number.

1. If $n = 2$, by the Sylow theorems G has a normal subgroup $\langle a \rangle$ of order $q = p_1$ and a subgroup $\langle b \rangle$ of order $p = p_2$; therefore, $bab^{-1} = a^k$; and since $a = b^p a b^{-p} = a^{k^p}$, k is a solution of the congruence equation

$$x^p = 1 \pmod{q}. \tag{2}$$

If $p | (q - 1)$, (2) has exactly p distinct solutions mod q, say $1, K, K^2, \ldots, K^{p-1}$ forming a cyclic group under multiplication mod q; and G is one of the two metacyclic groups [4, p. 462]

$$(a, b; a^q, b^p, bab^{-1} = a), \tag{3}$$

$$(a, b; a^q, b^p, bab^{-1} = a^K). \tag{4}$$

(3) is a cyclic group generated by ab. Observe that the metacyclic group $(a, b; a^q, b^p, bab^{-1} = a^{K^r})$ with $1 < r < p$ has also presentation (4) if we use the generators a, b^r instead of a, b. If $p \nmid (q - 1)$, then we only have the cyclic group (3).

2. In the general case, $n \geqslant 2$, we will use the following theorems whose proofs can be found in [3, 2.6.7, p. 39, 6.2.11, p. 138, 9.3.11, p. 229 and 9.3.10, p. 228].

THEOREM 1. *If H and A/H are solvable groups, so is A.*

THEOREM 2. *If A is a finite group, p the smallest prime dividing $o(A)$, and a Sylow p-subgroup P of A is cyclic, then P has a normal complement in A.*

Received July 8, 1975; revised November 24, 1975.
AMS (MOS) subject classifications (1970). Primary 20–04; Secondary 20D99.

Definition. A Sylow basis B of a finite group A is a set of Sylow subgroups P_i of A, one for each prime divisor of $o(A)$, such that if $P_1, P_2, \ldots, P_r$ are elements of B then $P_1 P_2 \cdots P_r$ is a subgroup of A of order $\Pi_{i=1}^r o(P_i)$.

THEOREM 3. *If A is a finite solvable group, then A has a Sylow basis.*

THEOREM 4 (HALL). *If A is a finite solvable group of order uv, and* $(u, v) = 1$, *then*: (i) *A has at least one subgroup of order u,* (ii) *all the subgroups of A of order u are conjugate.*

By Theorems 1 and 2 and induction on n, one can easily see that G is solvable; and therefore by Theorem 3, there exist $a_i \in G$, $i = 1, 2, \ldots, n$, such that $o(\langle a_i\rangle) = p_i$; and $\langle a_{S(1)}, a_{S(2)}, \ldots, a_{S(r)}\rangle$ is a subgroup of G of order $\Pi_{i=1}^r p_{S(i)}$ for every subset $S \subseteq \{1, 2, \ldots, n\}$. In particular, for $i < j$, we have, as in Section 1, $a_j a_i a_j^{-1} = a_i^{k(i,j)}$, so that G has a presentation of the form

$$(5) \qquad (\{a_i | 1 \leqslant i \leqslant n\}; \{a_i^{p_i} | 1 \leqslant i \leqslant n\}, \{a_j a_i a_j^{-1} = a_i^{k(i,j)} | 1 \leqslant i < j \leqslant n\})$$

with

$$(6) \qquad (k(i, j))^{p_j} = 1 \pmod{p_i}.$$

For each pair $i < j$ such that $p_j | (p_i - 1)$, we will choose one $\neq 1$ solution $K(i, j)$ of the congruence equation (6); and therefore, $k(i, j)$ is a power of $K(i, j) \pmod{p_i}$.

If $i < j < t$, then $\langle a_i, a_j\rangle$ is normal in $\langle a_i, a_j, a_t\rangle$; and the relation $a_j a_i a_j^{-1} = a_i^{k(i,j)}$ is changed by conjugation by a_t into $a_j^{k(j,t)} a_i^{k(i,t)} a_j^{-k(j,t)} = a_i^{k(i,j)k(i,t)}$, whence $a_i^{k(i,j)^{k(j,t)}k(i,t)} = a_i^{k(i,j)k(i,t)}$; that is: $k(i, j)^{k(j,t)-1} = 1 \pmod{p_i}$ which implies that:

$$(7) \qquad \text{If } i < j < t, \text{ then either } k(i, j) = 1 \text{ or } k(j, t) = 1.$$

Using a convenient power of a_j, $j > 1$, as generator instead of a_j, we may assume as in Section 1 that

$$(8) \qquad k(1, j) \text{ equals either } 1 \text{ or } K(i, j).$$

More generally, we may assume without loss of generality that:

$$(9) \qquad \text{If } 1 = k(1, j) = k(2, j) = \cdots = k(i - 1, j), \text{ then } k(i, j) \text{ is either } 1 \text{ or } K(i, j).$$

PROPOSITION 1. *There exists a group G with any given presentation of type* (5) *with exponents satisfying conditions* (6)–(9).

Proof. For each j, $\langle a_1, a_2, \ldots, a_j, a_{j+1}\rangle$ is the relative holomorph

$$\mathrm{Hol}(\langle a_1, a_2, \ldots, a_j\rangle, \langle f\rangle)$$

with $f(a_i) = a_i^{k(i,j+1)}$, $1 \leqslant i \leqslant j$ [3, 9.2.2, p. 214].

PROPOSITION 2. *Two presentations of type* (5) *with exponents satisfying conditions* (6)–(9) *that differ in one of the exponents $k(i, j)$ present morphically different groups. We postpone the proof of this proposition.*

3. In the case of three factors we will call $r = p_1$, $q = p_2$ and $p = p_3$. By the previous section, G has one of the following presentations:

(10) $(a, b, c; a^r, b^q, c^p, bab^{-1} = a, cac^{-1} = a, cbc^{-1} = b)$,

(11) $(a, b, c; a^r, b^q, c^p, bab^{-1} = a, cac^{-1} = a, cbc^{-1} = b^{K(2,3)})$,

(12) $(a, b, c; a^r, b^q, c^p, bab^{-1} = a, cac^{-1} = a^{K(1,3)}, cbc^{-1} = b)$,

(13) $(a, b, c; a^r, b^q, c^p, bab^{-1} = a, cac^{-1} = a^{K(1,3)}, cbc^{-1} = b^{k(2,3)})$ with $k(2, 3) = K(2, 3)^r, \quad r = 1, 2, \ldots, p - 1$,

(14) $(a, b, c; a^r, b^q, c^p, bab^{-1} = a^{K(1,2)}, cac^{-1} = a, cbc^{-1} = b)$,

(15) $(a, b, c; a^r, b^q, c^p, bab^{-1} = a^{K(1,2)}, cac^{-1} = a^{K(1,3)}, cbc^{-1} = b)$.

In order to show that they present morphically different groups observe:

(i) The groups with presentations (10)–(15) have the following characteristics:

	Abelian	$\langle a\rangle$ central	$\langle b, c\rangle$ Abelian	$\langle b\rangle$ central	$\langle c\rangle$ central
(10)	Yes				
(11)	No	Yes			
(12)	No	No	Yes	Yes	
(13)	No	No	No		
(14)	No	No	Yes	No	Yes
(15)	No	No	Yes	No	No

(ii) If G has two presentations of type (13), say, one with $k(2, 3) = K(2, 3)^s$ and the other with $k(2, 3) = K(2, 3)^t$, then G has elements a, b, c satisfying the relations of the first presentation, and elements a', b', c' satisfying the relations of the second presentation; since $\langle a\rangle$ and $\langle b\rangle$ are normal in G, we have (Theorem 4) $a' = a^x$, $b' = b^y$ and $c' = a^u b^v c^w$. The relation $c'b'c'^{-1} = a'^{K(1,3)}$ implies $a^{xK(1,3)^w} = a^{xK(1,3)}$, whence $w = 1$; and the relation $c'b'c'^{-1} = b'^{K(2,3)^t}$ implies $b^{yK(2,3)^s} = b^{yK(2,3)^t}$, whence $t = s \pmod p$; and therefore, the two presentations coincide.

The preceding discussion permits us to determine the number of groups of order rqp as shown in the following table:

TABLE 1

Number of Groups of Order rqp, $r > q > p$

$q\mid(r-1)$	$p\mid(r-1)$	$p\mid(q-1)$	Number of groups
No	No	No	1
No	No	Yes	2
No	Yes	No	2
No	Yes	Yes	$p + 2$
Yes	No	No	2
Yes	No	Yes	3
Yes	Yes	No	4
Yes	Yes	Yes	$p + 4$

4. Proof of Proposition 2. Assume inductively that the proposition is true for $n-1$, and let G and G' be groups with presentations of the type (5) satisfying conditions (6)–(9) and with $k(i, j) \neq k'(i, j)$ for some pair $i < j$. If $j < n$, then by assumption $\langle a_1, a_2, \ldots, a_{n-1}\rangle \not\cong \langle a'_1, a'_2, \ldots, a'_{n-1}\rangle$ and by Theorem 4 $G \not\cong G'$; therefore, we may assume that $k(i, j) = k'(i, j)$ for all $1 \leqslant i < j < n$. If $k(1, n) \neq k'(1, n)$, then by (8) one of the two is 1 and the other is $K(1, n)$, whence $\langle a_1, a_n\rangle \not\cong \langle a'_1, a'_n\rangle$ and $G \not\cong G'$; therefore, we may assume that $k(1, n) = k'(1, n)$. Let j be the smallest subindex such that $k(j, n) \neq k'(j, n)$; we may assume that $k'(j, n) \neq 1$ and by (7) $k(i, j) = k'(i, j) = 1$ for all $i < j$. If $k(i, n) = k'(i, n) = 1$ for all $i < j$, then by (9) $k(j, n) = 1$ and $k'(j, n) = K(j, n)$; and therefore, $\langle a_1, a_j, a_n\rangle$ is of type (10), whereas $\langle a'_1, a'_j, a'_n\rangle$ is of type (11) and by Theorem 4 $G \not\cong G'$. Else, let i be the least subindex such that $k(i, n) = k'(i, n) \neq 1$; by (9) $k(i, n) = k'(i, n) = K(i, n)$; and therefore, $\langle a'_i, a'_j, a'_n\rangle$ is of type (13), whereas $\langle a_i, a_j, a_n\rangle$ is either of type (13) with different exponent or of type (12); again by Theorem 4 $G \not\cong G'$.

5. O. Hölder's Approach. It is easy to see that $\langle a_j\rangle$ is normal in G if and only if $k(i, j) = 1$ for all $i < j$, and $H = \langle\{a_j | \langle a_j\rangle \text{ normal in } G\}\rangle$ is Abelian and therefore cyclic. Furthermore, condition (7) shows that $G^1 \subseteq H$, and therefore, G/H is also cyclic, which implies [4, p. 462] that G is metacyclic with presentation of the form

$$(a, b; a^s, b^t, bab^{-1} = a^k),\ st = h. \tag{16}$$

$k(1,2)$	$k(1,3)$	$k(2,3)$	$k(1,4)$	$k(2,4)$	$k(3,4)$
1	1	1	1	1	1
					K
				K	1
					k
			K	1	1
					k
				k	1
					k
		K	1	1	1
				K	1
			K	1	1
				k	1
	K	1	1	1	1
				K	1
			K	1	1
				k	1
		k	1	1	1
				K	1
			K	1	1
				k	1
K	1	1	1	1	1
					K
			K	1	1
					k
	K	1	1	1	1
			K	1	1

DIAGRAM 1

Definition. i is linked to j if there exist $S(1) = i, S(2), \ldots, S(r) = j$ such that $a_{S(t)}$ does not commute with $a_{S(t+1)}$, $t = 1, 2, \ldots, r-1$. The proof of the following proposition is trivial:

PROPOSITION 3. *For each i, $\langle a_i, \{a_j | i$ is linked to $j\}\rangle$ is the minimal direct summand of G containing a_i.*

6. The number of groups of order h can be determined by means of the tree diagram of the exponents in (5), as we illustrate here for the case of 4 factors. In Diagram 1 above we write K or k for $K(i, j)$ or $k(i, j)$ when it is not equal to 1; the branches with some K or k exist if and only if the corresponding p_j divides $p_i - 1$; a small k indicates that the offshoot originating at fork (i, j) has multiplicity $p_j - 1$.

7. In the case of 4 factors we call $s = p_1, r = p_2, q = p_3$ and $p = p_4$. The number of groups of order $srqp$ is easily determined by determining first the groups of order srq, and pursuing in the tree diagram the number of extensions of each to groups of order $srqp$. We obtain:

TABLE 2

Number of Groups of Order srqp, $s > r > q > p$

	$p \nmid (s-1)$ $p \nmid (r-1)$ $p \nmid (q-1)$	$p \nmid (s-1)$ $p \nmid (r-1)$ $p \mid (q-1)$	$p \nmid (s-1)$ $p \mid (r-1)$ $p \nmid (q-1)$	$p \nmid (s-1)$ $p \mid (r-1)$ $p \mid (q-1)$	$p \mid (s-1)$ $p \nmid (r-1)$ $p \nmid (q-1)$	$p \mid (s-1)$ $p \nmid (r-1)$ $p \mid (q-1)$	$p \mid (s-1)$ $p \mid (r-1)$ $p \nmid (q-1)$	$p \mid (s-1)$ $p \mid (r-1)$ $p \mid (q-1)$
$r \nmid (s-1)$ $q \nmid (s-1)$ $q \nmid (r-1)$	1	2	2	$p+2$	2	$p+2$	$p+2$	p^2+p+2
$r \nmid (s-1)$ $q \nmid (s-1)$ $q \mid (r-1)$	2	3	4	$p+4$	4	$p+4$	$2p+4$	$(p+2)^2$
$r \nmid (s-1)$ $q \mid (s-1)$ $q \nmid (r-1)$	2	3	4	$p+4$	4	$p+4$	$2p+4$	$(p+2)^2$
$r \nmid (s-1)$ $q \mid (s-1)$ $q \mid (r-1)$	$q+2$	$q+3$	$2q+4$	$2q+p+4$	$2q+4$	$2q+p+4$	$(q+2)(p+2)$	$(q+2)(p+2)$ $+p^2$
$r \mid (s-1)$ $q \nmid (s-1)$ $q \nmid (r-1)$	2	4	3	$p+4$	4	$2p+4$	$p+4$	$(p+2)^2$
$r \mid (s-1)$ $q \nmid (s-1)$ $q \mid (r-1)$	3	5	5	$p+6$	6	$2p+6$	$2p+6$	p^2+3p+6
$r \mid (s-1)$ $q \mid (s-1)$ $q \nmid (r-1)$	4	6	6	$p+7$	8	$2p+8$	$2p+8$	p^2+3p+8
$r \mid (s-1)$ $q \mid (s-1)$ $q \mid (r-1)$	$q+4$	$q+6$	$2q+6$	$2q+p+7$	$2q+8$	$2(p+q+4)$	$(q+2)(p+2)$ $+4$	$(q+2)(p+2)$ $+p^2+p+4$

8. A computer program to determine the number of groups of order h can be written using the tree diagram of Section 6:

(a) Set to 0 the number, NUM, of groups of order h.

(b) As we proceed along one branch, each occurrence of k multiplies NU, the number of groups originated by the branch, by $p_j - 1$. k occurs at the fork (i, j) when the following conditions are satisfied simultaneously: (i) $p_j | (p_i - 1)$, (ii) $k(m, i) = 1$ for all $m < i$, and (iii) $k(m, j) \neq 1$ for some $m < i$.

(c) When the end of one branch is reached, NU is accumulated to NUM.

(d) The next branch is picked up at the last fork (i, j) where $p_j | (p_i - 1)$ and the $k(i, j) \neq 1$ has not been used.

Note. The FORTRAN program implementing the algorithm appears in the microfiche section.

Department of Mathematics
Bennett College
Greensboro, North Carolina 27420

1. O. HÖLDER, "Die Gruppen der Ordnung p^3, pq^2, pqr, p^4," *Math. Ann.*, v. 43, 1893, pp. 300–412.

2. O. HÖLDER, "Die gruppen mit quadratfreier Ordnungzahl", *Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Math.-Phys. Kl.*, v. 1895, pp. 211–229.

3. W. R. SCOTT, *Group Theory*, Prentice-Hall, Englewood Cliffs, N. J., 1964. MR 29 #4785.

4. S. MAC LANE & G. BIRKHOFF, *Algebra*, Macmillan, New York, 1967. MR 35 #5266.

GROUPS OF SQUARE FREE ORDER, AN ALGORITHM

by J. Alonso

```
C          A FORTRAN PROGRAM FOR THE COMPUTATION OF THE NUMBER OF GROUPS OF
C          A GIVEN SQUARE - FREE ORDER H.
C
      DIMENSION NP(10),K(10,10),NB(10,10),KV(10,10)
C
C          NP ARE THE PRIME FACTORS OF H IN DECREASING ORDER.
C          AT FORK (I,J):
C            1) NB IS THE MAX. NUMBER OF OFFSHOOTS (NOT COUNTING MULTIPLICITY).
C            2) K IS THE ORDINAL NUMBER OF THE OFFSHOOT.
C            3) KV IS THE CUMULATIVE MULTIPLICITY OF THE BRANCH.
C
      WRITE(3,5)
5     FORMAT('1',2X,'ORDER'S PRIME FACTORS',13X,'NUMBER OF GROUPS',/)
C
C          GETTING THE INFORMATION AND INITIALIZING.
C
20    READ(2,22)N,(NP(I),I=1,N)
22    FORMAT(11I3)
      IF(N)30,1000,30
30    NUM=0
      NM1=N-1
      DO 50 J=2,N
      JM1=J-1
      Do 50 I=1,JM1
      IF((NP(I)-1)-((NP(I)-1)/(NP(J))*NP(J))35,38,35
35    NB(I,J)=1
      GO TO 40
38    NB(I,J)=2
40    K(I,J)=1
50    KV(I,J)=1
      I1=1
      J1=2
C
C          FOLLOWING ONE BRANCH THROUGH.
C
55    NU=KV(I1,J1)
      DO 500 J=J1,N
      IF(J-J1)70,80,70
70    I2=1
      GO TO 90
80    I2=I1
90    JM1=J-1
      DO 500 I=I2,JM1
      KV(I,J)=NU
      IF(K(I,J)-1)100,500,100
100   IF(I-1)120,200,120
120   IM1=I-1
      DO 180 L=1,IM1
      IF(K(L,J)-1)150,180,150
150   NU=NU*(NP(J)-1)
      GO TO 200
180   CONTINUE
200   IF(J-N)250,500,250
250   JP1=P+1
```

```
      DO 280 L=JP1,N
280   NB(J,L)=1
500   CONTINUE
      NUM=NUM+NU
C
C         PREPARING FOR THE NEXT BRANCH: 2 ITEMS TO BE CONSIDERED
C              ITEM 1: TO DETERMINE AT WHICH FORKIS THE NEW BRANCH TO BE PICKED UP.
C
      DO 700 JA=1,NM1
      J=N+1-JA
      JM1=J-1
      DO 700 IA=1,JM1
      I=J-IA
      IF(K(I,J)-NB(I,J))600,700,600
600   K(I,J)=K(I,J)+1
      I1=I
      J1=J
C
C              ITEM 2: TO RESTORE THE INITIAL VALUES FOLLOWING FORK (I1,J1).
C
      IF(J-I-1)640,610,640
610   IF(J-N)620,55,55
620   JB=J+1
      GO TO 650
640   JB=J
650   DO 670 M=JB,N
      MM1=M-1
      IF(M-J)652,654,652
652   IB=1
      GO TO 656
654   IB=I+1
656   DO 670 L=IB,MM1
      K(L,M)=1
      KV(L,M)=1
      IF(L-1)658,670,658
658   IF((NP(L)-1)-((NP(L)-1)/NP(M))*NP(M))670,659,670
659   LM1=L-1
      DO 665 L1=1,LM1
      IF(K(L1,L)-1)660,665,660
660   NB(L,M)=1
      GO TO 670
665   NB(L,M)=2
670   CONTINUE
      GO TO 55
700   CONTINUE
C
C         OUTPUT
C
      WRITE(3,720)(NP(I),I=1,N)
720   FORMAT(1X,10I3)
      WRITE(3,820)NUM
820   FORMAT('+',40X,I12)
      GO TO 20
1000  STOP
      END
```