

STANDARD GENERATORS FOR THE SUZUKI GROUPS

JOHN BRAY AND HENRIK BÄÄRNHIELM

ABSTRACT. We present a black box algorithm that finds standard generators for the Suzuki groups $Sz(q)$, where $q = 2^{2m+1}$ for some $m > 0$. The algorithm is Las Vegas, with time complexity $O(q \log(q)^5)$ group operations. It is implemented in the computer algebra system MAGMA.

1. INTRODUCTION

The family of simple groups known as Suzuki groups were introduced in [17, 18, 19], as matrix groups of degree 4. They are usually denoted $Sz(q)$, where \mathbb{F}_q is the defining field, so that $q = 2^{2m+1}$ for some $m > 0$. In [6], standard generators for $Sz(q)$ are given, as well as a short presentation for $Sz(q)$ on these generators. We shall use the notation of [6], so that our standard generators for $Sz(q)$ are

$$x = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \quad (1)$$

$$y = \begin{bmatrix} \omega^{t/2+1} & 0 & 0 & 0 \\ 0 & \omega^{t/2} & 0 & 0 \\ 0 & 0 & \omega^{-t/2} & 0 \\ 0 & 0 & 0 & \omega^{-t/2-1} \end{bmatrix} \quad (2)$$

$$z = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad (3)$$

where $t = 2^{m+1} = \sqrt{2q}$ and ω is a primitive element of \mathbb{F}_q .

In [2], the Suzuki groups are studied from an algorithmic perspective, and a constructive recognition algorithm is presented. Constructive recognition can also be solved by finding standard generators and then solving a module isomorphism problem[11]. The algorithm presented here therefore provides an alternative to [2, Theorem 3.25], useful when q is small. Moreover, [2, Theorem 3.25] depends on a few conjectures, one ([2, Conjecture 3.23]) of which is proved by the algorithm presented here. Hence this paper forms a part of the Matrix Group Recognition Project[12].

In [15, pp. 17], the concept of a *black box group* is defined. In short, it is a group where the elements are encoded as strings of uniform length over a finite alphabet, and equipped with an *oracle* (the “black box”) that can find a string representing the product of two given elements, find a string representing the inverse of a given element, and test if a given element is the identity.

Here we consider the Suzuki groups as black box groups with order oracles. In other words, the black box group has an additional oracle that finds the order of a given element. We shall also assume an oracle for the discrete logarithm problem.

The time complexity measures will be bit operations. We will use the following notation for a black box group G :

- μ The time complexity for the group operation in G , *i.e.* the cost of the black box.
- η The time complexity to find the order of an element of G .
- ξ The time complexity to construct a uniformly random element of G .
- ζ The time complexity for a field operation, *i.e.* a multiplication in \mathbb{F}_q .
- χ The time complexity for solving an instance of the discrete logarithm problem in \mathbb{F}_q .

Note that some of these are redundant. Clearly, $\chi \in O(q\zeta)$, and since q is a power of 2, by [9], $\chi \in O(\exp(c \log(q)^{1/3} \log \log(q)^{2/3}))$ where $c > 0$ is a small constant. By [3], $\xi \in O((\log(|G|))^5 \mu)$. Moreover, in $\text{Sz}(q)$ every element has order $O(q)$, so that $\eta \in O(q\mu)$, and $|\text{Sz}(q)| = q^2(q^2 + 1)(q - 1)$, so that $\log(|G|) \in O(\log(q))$. If elements of \mathbb{F}_q are represented as polynomials over \mathbb{F}_2 (as bit-strings), then by [20, Theorem 8.23], $\zeta \in O(\log(q) \log \log(q) \log \log \log(q))$.

The algorithms we present will be probabilistic, of *Las Vegas* type. Such algorithms are defined in [15, Section 1.3] and [10, Section 3.2.1]. In short, a Las Vegas algorithm either returns **failure**, with probability at most ε , or otherwise returns a correct result. One can enclose such an algorithm in a loop that iterates until the algorithm returns a correct result, thus obtaining a probabilistic time complexity. This is the way we present Las Vegas algorithms, since it is the one that is closest to how the algorithm is used in practise.

When we say that an algorithm is “given a group $\langle X \rangle$ ”, then the generating set X is fixed and known. In other words, the the algorithm is given the generating set X and will operate in $\langle X \rangle$.

Our algorithm will find standard generators expressed as *straight line programs* (abbreviated to SLPs) in the given generating set. An SLP is a data structure for a word, which ensures that during evaluation, subwords occurring multiple times are not computed more often than during construction. An important issue is the length of the SLPs that are computed. We assume that SLPs of random elements have length $O(n)$ where n is the number of random elements that have been selected so far during the execution of the algorithm.

The objective of the paper is to prove the following result.

Theorem 1. *There exists a Las Vegas algorithm that, given a black box group $G = \langle X \rangle \cong \text{Sz}(q)$, where $q = 2^{2m+1}$ for some $m > 0$, finds $\bar{x}, \bar{y}, \bar{z} \in G$ as straight line programs in X , such that the mapping*

$$\bar{x} \mapsto x \tag{4}$$

$$\bar{y} \mapsto y \tag{5}$$

$$\bar{z} \mapsto z \tag{6}$$

is an isomorphism. The algorithm has expected time complexity $O(q(\xi + \mu) + \log \log(q)\eta + q \log(q)\zeta + \chi)$, or equivalently $O(q \log(q)^5 \mu)$. The length of the returned SLPs are $O(q)$.

The algorithm has been implemented in the computer algebra system MAGMA[4].

2. PRELIMINARIES

Recall that the *trace* (over the prime field) of an element $a \in \mathbb{F}_q$, where $q = p^e$ for some prime number p , is $\text{Tr}(a) = \sum_{i=0}^{e-1} a^{p^i} \in \mathbb{F}_p$. Trivially, $\text{Tr}(a)$ can be computed in time $O(ep\zeta)$.

Henceforth assume that $q = 2^{2m+1}$ for some $m > 0$, and ω will denote a fixed primitive element of \mathbb{F}_q . We shall also denote the Euler totient function by ϕ .

We can express any $a \in \mathbb{F}_q$ as $a = \sum_{i=0}^{2m} a_i \omega^i$, where each $a_i \in \mathbb{F}_2$. Then

$$\mathrm{Tr}(a) = \sum_{j=0}^{2m} a^{2^j} = \sum_{j=0}^{2m} \sum_{i=0}^{2m} a_i (\omega^i)^{2^j} = \sum_{i=0}^{2m} a_i \mathrm{Tr}(\omega^i) \quad (7)$$

and hence if $\mathrm{Tr}(\omega^i)$ is pre-computed for $i = 0, \dots, 2m$, then $\mathrm{Tr}(a)$ can be computed in time $O(\log(q))$.

Lemma 2. *There exists $k \in \{1, \dots, q-1\}$ such that*

- (1) $\gcd(k, q-1) = 1$,
- (2) $\mathrm{Tr}(\omega^{-k}) = 1$.

Proof. This is proved in [14]. Also see [8] for an overview. \square

Lemma 3. *Let $g \in \mathrm{Sz}(q)$. Then $|g| = q \pm t + 1$ if and only if $\mathrm{Tr}(\mathrm{Tr}(g)^{t/2-1}) = 1$.*

Proof. TODO \square

We use the notation of [6].

Lemma 4. *Let k be as in Lemma 2, and let $a = \omega^k$. There exists unique $b \in \mathbb{F}_q$ such that $|T(a, b)z| = 4$ and $(T(a, b)^2 z)^{T(a, b)} = (T(a, b)^2 z)^q$.*

Proof. Direct calculations show that $|T(a, b)z| > 2$ unless $a = b = 0$, $\mathrm{Tr}(T(a, b)^2 z) = a^{t+2}$ and $\mathrm{Tr}(T(a, b)z) = a^t + a^{t+2} + ab + b^t$. Hence by Lemma 3, $|T(a, b)^2 z| = q \pm t + 1$. Also, if $|T(a, b)z| = 4$ then [2, Lemma 5.2] implies that $\langle T(a, b), z \rangle$ is a maximal subgroup of $\mathrm{Sz}(q)$ of shape $C_{q \pm t + 1} : C_4$. By [2, Theorem 2.1], the element of order 4 at the top acts on the normal subgroup as powering by $\pm q$.

In $\mathrm{Sz}(q)$, elements of trace 0 have orders 1, 2, 4, and

$$\begin{aligned} a^t + a^{t+2} + ab + b^t &= 0 \Leftrightarrow \\ a^2 + a^{2t+2} + a^t b^t + b^2 &= 0 \Rightarrow \\ b^2 + a^{t+1} b + a^2 + a^{2t} &= 0 \end{aligned} \quad (8)$$

where the third equation is a^t times the first added to the second. The quadratic equation has solutions $b_1 = a^{t+1} \sum_{i=1}^{m+1} a^{-2^i}$ and $b_2 = b_1 + a^{t+1}$, which both give the value $a^{s+2}(1 + \mathrm{Tr}(a^{-1}))$ of $\mathrm{Tr}(T(a, b)z)$. Hence $T(a, b_1)z$ and $T(a, b_2)z$ have order 4. One acts as the power q on $T(a, b)^2 z$ and the other as the power $-q$. \square

Lemma 5. *The element $T(0, a)z$ has order 5 if and only if $a = 1$.*

Proof. Elements in $\mathrm{Sz}(q)$ of order 5 are conjugate (why?!). A direct calculation shows that $|T(0, 1)z| = 5$ and $\mathrm{Tr}(T(0, a)z) = a^t$. Hence by [2, Proposition 2.8], if $a \neq 1$ then it is not conjugate to $T(0, 1)z$, and hence cannot have order 5. \square

Lemma 6. *There exists an absolute constant $c > 0$ such that the product of two random involutions in $\mathrm{Sz}(q)$ has odd order with probability at least c .*

Proof. Given a fixed involution j_1 and a random involution j_2 , their product is odd if j_2 lies in a different maximal parabolic, or if $j_1 = j_2$. Hence the probability is $1 - 1/(q^2 + 1) + 1/((q^2 + 1)(q - 1)) \geq 449/455 = c$ since $m \geq 1$. \square

By [2, Theorem 2.3], a maximal parabolic of $\mathrm{Sz}(q)$ has shape $(\mathbb{F}_q \cdot \mathbb{F}_q) : \mathbb{F}_q^\times$.

Theorem 7. *There exists a Las Vegas algorithm that, given a black box group $G = \langle X \rangle \cong \text{Sz}(q)$, and an element $f \in G$ of order 4, finds $h \in G$ such that $|h| = q-1$ and $\langle f, h \rangle$ is a maximal parabolic in G . The algorithm has time complexity $O((\mu \log(q) + \xi + \eta) \log \log(q))$. If f is given as an SLP in X of length $O(n)$, then h will be found as an SLP in X of length $O(n + \log(q))$.*

Proof. The algorithm proceeds as follows:

- (1) Use the algorithm of [5] to find an element $g \in C_G(f^2) \cong \mathbb{F}_q \cdot \mathbb{F}_q$. If $|g| = 4$ then let $j := g^2$, otherwise $j := g$. Find another g if $j = f^2$. This takes expected time $O(\mu + \xi + \eta)$.
- (2) Find random $c \in G$ such that $j^c \notin C_G(f^2)$ and $|f^2 j^c| = 2k+1$. The number of involutions in $C_G(f^2)$ is $q-1$, and the total number of involutions in G is $(q-1)(q^2+1)$. Hence by Lemma 6, this takes expected time $O(\mu + \xi + \eta)$.
- (3) Let $h = c(j^c f^2)^k$. This takes time $O(\mu \log(q))$. Then $(f^2)^h = j$ and hence $\langle f, h \rangle$ lies in a maximal parabolic (h must fix the point fixed by f^2 and j).
- (4) Since $h \notin C_G(f^2)$, it must have odd order. Check that $|h| = q-1$ (rather than a proper divisor). Return to the first step otherwise.

By [2, Theorem 2.1], the probability that h has the correct order is $\phi(q-1)/(q-1)$. Hence by [13, Section II.8], the number of iterations of the algorithm is $O(\log \log(q))$. \square

3. THE MAIN ALGORITHM

We now describe the algorithm in Theorem 1.

- (1) Find random $f \in G$ of order 4. The total number of such elements in G is $q(q^2+1)(q-1)$, and $|G| = q^2(q^2+1)(q-1)$. Hence this takes time $O(q(\mu + \xi))$.
- (2) Let $s = f^2$. Find random $c \in G$ such that $|ss^c| \notin \{1, 2, 4\}$. Let $\bar{z} = s^c$. Similarly as in the proof of Theorem 7, this takes expected time $O(\mu + \xi)$. Note that we have f, s, \bar{z} as SLPs of length $O(q)$. Moreover, f corresponds to $T(a_1, b_1)$, s corresponds to $T(0, a_1^{t+1})$, for some $a_1, b_1 \in \mathbb{F}_q$.
- (3) Use Theorem 7 with f and hence find h of order $q-1$. Then h corresponds to $T(a_2, b_2)D(\lambda)$, for some $a_2, b_2 \in \mathbb{F}_q$ and $\lambda \in \mathbb{F}_q^\times$.
- (4) Find $j \in \{1, \dots, q-1\}$ such that $|s^{h^j} \bar{z}| = 5$. Replace s and f with s^{h^j} and f^{h^j} . Then by Lemma 5, s corresponds to $T(0, 1)$ and f corresponds to $T(1, b_3)$ for some $b_3 \in \mathbb{F}_q$. This takes time $O(q\mu)$.
- (5) Compute $\text{Tr}(\omega^i)$ for each $i = 0, \dots, 2m$. This takes time $O(\log(q)^2 \zeta)$.
- (6) Find a primitive element $a = \omega^l \in \mathbb{F}_q$ such that $\text{Tr}(a^{-1}) = 1$. By [20, Corollary 11.10, Theorem 8.24] and (7), this takes time $O(q \log(q))$. We next want to replace h so that its diagonal part corresponds to $D(\omega)$.
- (7) For random $j \in \{1, \dots, q-1\}$, perform the following steps:
 - (a) Determine if $\gcd(j, q-1) = 1$, and simultaneously compute $1/j \pmod{q-1}$. Skip to the next j if not. By [20, Corollary 11.10, Theorem 8.24], this takes time

$$O(\log(q) \log \log(q)^2 \log \log \log(q)).$$

- (b) Find the minimal polynomial $g(w) = \sum_{i=0}^{2m+1} d_i w^i$ of ω^j , over \mathbb{F}_2 . If $\lambda = \omega^j$, then by [6], $f^{d_{2m+1} h^{2m+1}} f^{d_{2m} h^{2m}} \dots f^{d_1 h} f^{d_0}$ has order at most 2. Skip to the next j if not, otherwise let $k := 1/j \pmod{q-1}$ and break. By [16], this takes time $O(\log(q)^2 \zeta + \log(q)\mu)$.

We expect to find k in $O(q/\log(q))$ iterations. Hence this step takes expected time $O(q(\log(q)\zeta + \mu + \log \log(q)^2 \log \log \log(q)))$.

- (8) Replace h with h^k . Then h corresponds to $T(a_2, b_2)D(\omega)$. This takes time $O(\log(q)\mu)$.
- (9) Find $j \in \{1, \dots, q-1\}$ such that $\bar{f} := fs^{h^j}$ has order 4 and either $\bar{z}\bar{f}\bar{z}\bar{f}^2\bar{z}\bar{f}^3 = 1$ or $\bar{z}\bar{f}^3\bar{z}\bar{f}^2\bar{z}\bar{f} = 1$. By [6], this implies that \bar{f} corresponds to $T(1, 0)$ or $T(1, 0)^{-1} = T(1, 1)$, respectively. If $\bar{z}\bar{f}\bar{z}\bar{f}^2\bar{z}\bar{f}^3 = 1$, then let $\bar{x} = \bar{f}$, otherwise let $\bar{x} = \bar{f}^{-1}$. This takes time $O(q\mu)$. Note that we then have \bar{x} as an SLP in X of length $O(q)$.
- (10) Let $u = \bar{x}^{h^l}$. Then u corresponds to $T(a, b_4)$ for some $b_4 \in \mathbb{F}_q$. This takes time $O(\log(q)\mu)$.
- (11) Find $j \in \{1, \dots, q-1\}$ such that $\bar{u} := us^{h^j}$ has order 4 and $(\bar{u}^2\bar{z})^{\bar{u}} = (\bar{u}^2z)^q$. By Lemma 4, this j is unique. This takes time $O(q\mu)$.
- (12) Now \bar{u} corresponds to $T(a, b)$ for some specific $b \in \mathbb{F}_q$, and by the proof of Lemma 4, b is either $\alpha = a^{t+1} \sum_{i=0}^{m+1} a^{-2^i}$ or $\alpha + a^{t+1}$. Determine which value is correct by directly calculating the matrices. This takes time $O(\log(q)\zeta)$, using [7] to calculate $(T(a, b)^2z)^q$.
- (13) Find $j \in \{1, \dots, q-1\}$ such that $\omega^j = b^{t-1}$. Let $v = \bar{u}s^{h^j}$. Then v corresponds to $T(a, 0)$. This takes time $O(\chi + \mu)$.
- (14) From [6], it follows that in $Sz(q)$ the following relation holds:

$$zT(a, 0)z = D(a^2)T(a, 0)zT(0, a^{-1-t})$$

Hence $\bar{v} := \bar{z}v\bar{z}s^{h^{-l}}\bar{z}v^{-1}$ corresponds to $D(a^2)$.

- (15) Let $\bar{y} = \bar{v}^{q/(2l)}$. Then \bar{y} corresponds to $D(\omega)$. Clearly we have \bar{y} as an SLP of length $O(q)$.

This proves Theorem 1. Finally, we can also verify that $\bar{x}, \bar{y}, \bar{z}$ are standard generators, using the short presentation given in [6].

APPENDIX A. IMPLEMENTATION DATA

The algorithm has been implemented in MAGMA. To illustrate that the algorithm is very much practical, we display the timings when the algorithm is executed on the representations of $Sz(8)$ and $Sz(32)$ that are available in version 3 of the WEB-ATLAS[1]. The time shown is the average taken over 10 executions.

TABLE 1. Timings on matrix groups for $q = 8$

Degree	Field	ID	Time [s]
64	\mathbb{F}_2		0.019
4	\mathbb{F}_{2^3}		0.006
16	\mathbb{F}_{2^3}		0.010
14	\mathbb{F}_5	a	0.010
14	\mathbb{F}_5	b	0.010
35	\mathbb{F}_5	a	0.020
35	\mathbb{F}_5	b	0.020
35	\mathbb{F}_5	c	0.021
63	\mathbb{F}_5		0.046
195	\mathbb{F}_5		0.482
65	\mathbb{F}_{5^3}	a	0.280
65	\mathbb{F}_{5^3}	b	0.288
65	\mathbb{F}_{5^3}	c	0.274
64	\mathbb{F}_7		0.056
91	\mathbb{F}_7		0.102
105	\mathbb{F}_7		0.147
14	\mathbb{F}_{7^2}		0.019
14	\mathbb{F}_{13}	a	0.021
14	\mathbb{F}_{13}	b	0.020
35	\mathbb{F}_{13}		0.062
65	\mathbb{F}_{13}	a	0.251
65	\mathbb{F}_{13}	b	0.234
65	\mathbb{F}_{13}	c	0.227
91	\mathbb{F}_{13}	c	0.449
14	$\mathbb{Z}[i]$	a	0.301
14	$\mathbb{Z}[i]$	b	0.344
65	\mathbb{C}	a	11.135
65	\mathbb{C}	b	9.958
65	\mathbb{C}	c	10.280
64	\mathbb{Z}		0.274
91	\mathbb{Z}		18.257
105	$\mathbb{Z}[i]$		91.083

TABLE 2. Timings on permutation groups for $q = 8$

Degree	Time [s]
65	0.0004
520	0.004
560	0.004
1456	0.006
2080	0.006

TABLE 3. Timings on matrix groups for $q = 32$

Degree	Field	ID	Time [s]
4	\mathbb{F}_{2^5}		0.022
124	\mathbb{F}_5		0.510
124	\mathbb{F}_{41}		2.923
124	$\mathbb{Z}[i, 1/2]$	a	1329.788
124	$\mathbb{Z}[i, 1/2]$	b	1199.178

TABLE 4. Timings on permutation groups for $q = 32$

Degree	Time [s]
1025	0.015
198400	4.631

REFERENCES

1. R. Abbot, J. Bray, S. Linton, S. Nickerson, S. Norton, R. Parker, S. Rogers, I. Suleiman, J. Tripp, P. Walsh, and R. Wilson, *Atlas of Finite Group Representations*, <http://brauer.maths.qmul.ac.uk/Atlas/>.
2. Henrik Bäärnhielm, *Algorithmic problems in twisted groups of Lie type*, Ph.D. thesis, Queen Mary, University of London, 2007.
3. László Babai, *Local expansion of vertex-transitive graphs and random generation in finite groups*, STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing (New York, NY, USA), ACM Press, 1991, pp. 164–174.
4. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
5. John N. Bray, *An improved method for generating the centralizer of an involution*, Arch. Math. (Basel) **74** (2000), no. 4, 241–245. MR MR1742633 (2001c:20063)
6. ———, *Presentations of the Suzuki groups*, preprint, 2007.
7. Frank Celler and C. R. Leedham-Green, *Calculating the order of an invertible matrix*, Groups and computation, II (New Brunswick, NJ, 1995), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 28, Amer. Math. Soc., Providence, RI, 1997, pp. 55–60. MR MR1444130 (98g:20001)
8. Mustafa Coban, *Primitive elements in finite fields with arbitrary trace*, Master's thesis, Sabanci University, <http://digital.sabanciuniv.edu/tezler/tezler/mdbf/master/cobanm/ana.pdf>, 2003.
9. Don Coppersmith, *Fast evaluation of logarithms in fields of characteristic two*, IEEE Trans. Inform. Theory **30** (1984), no. 4, 587–594. MR MR755785 (85h:65041)
10. Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien, *Handbook of computational group theory*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005. MR MR2129747 (2006f:20001)
11. Derek F. Holt and Sarah Rees, *Testing modules for irreducibility*, J. Austral. Math. Soc. Ser. A **57** (1994), no. 1, 1–16. MR MR1279282 (95e:20023)
12. Charles R. Leedham-Green, *The computational matrix group project*, Groups and computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 229–247. MR MR1829483 (2002d:20084)
13. D. S. Mitrinović, J. Sándor, and B. Crstici, *Handbook of number theory*, Mathematics and its Applications, vol. 351, Kluwer Academic Publishers Group, Dordrecht, 1996. MR MR1374329 (97f:11001)
14. Oscar Moreno, *On primitive elements of trace equal to 1 in $\text{GF}(2^m)$* , Discrete Math. **41** (1982), no. 1, 53–56. MR MR676862 (84c:12012)
15. Ákos Seress, *Permutation group algorithms*, Cambridge Tracts in Mathematics, vol. 152, Cambridge University Press, Cambridge, 2003. MR MR1970241 (2004c:20008)
16. Victor Shoup, *Efficient computation of minimal polynomials in algebraic extensions of finite fields*, Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC) (New York), ACM, 1999, pp. 53–58 (electronic). MR MR1802067 (2002b:12004)
17. Michio Suzuki, *A new type of simple groups of finite order*, Proc. Nat. Acad. Sci. U.S.A. **46** (1960), 868–870. MR MR0120283 (22 #11038)
18. ———, *On a class of doubly transitive groups*, Ann. of Math. (2) **75** (1962), 105–145. MR MR0136646 (25 #112)
19. ———, *On a class of doubly transitive groups. II*, Ann. of Math. (2) **79** (1964), 514–589. MR MR0162840 (29 #144)
20. Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, second ed., Cambridge University Press, Cambridge, 2003. MR MR2001757 (2004g:68202)

E-mail address: j.n.bray@qmul.ac.uk

SCHOOL OF MATHEMATICAL SCIENCES, QUEEN MARY, UNIVERSITY OF LONDON, MILE END ROAD, LONDON E1 4NS, UNITED KINGDOM

E-mail address: h.baarnhielm@qmul.ac.uk

SCHOOL OF MATHEMATICAL SCIENCES, QUEEN MARY, UNIVERSITY OF LONDON, MILE END ROAD, LONDON E1 4NS, UNITED KINGDOM