Accepted Manuscript

A new method for recognising Suzuki groups

John N. Bray, Henrik Bäärnhielm

PII: S0021-8693(17)30369-1
DOI: http://dx.doi.org/10.1016/j.jalgebra.2017.05.040
Reference: YJABR 16280

To appear in: *Journal of Algebra*

Received date: 7 July 2016

Please cite this article in press as: J.N. Bray, H. Bäärnhielm, A new method for recognising Suzuki groups, *J. Algebra* (2017), http://dx.doi.org/10.1016/j.jalgebra.2017.05.040

A NEW METHOD FOR RECOGNISING SUZUKI GROUPS

JOHN N. BRAY AND HENRIK BÄÄRNHIELM

Abstract. We present a new algorithm for constructive recognition of the Suzuki groups in their natural representations. The algorithm runs in Las Vegas polynomial time given a discrete logarithm oracle. An implementation is available in the Magma computer algebra system.

1. Introduction

In [1] and [2], algorithms for constructive recognition of the Suzuki groups in the natural representation are presented. They depend on a technical conjecture, which is still open, although supported by substantial experimental evidence.

Here we present a new algorithm for this problem, which does not depend on any such conjectures, and which is also more efficient.

We shall use the notation of [2], but for completeness we state the important points here. The ground finite field is $\mathbb{F}_q$ where $q = 2^{2m+1}$ for some $m > 0$, and we define $t = 2^{m+1}$ so that $x^{t^2} = x^2$ for every $x \in \mathbb{F}_q$. For $a, b \in \mathbb{F}_q$ and $\lambda \in \mathbb{F}_q^\times$, define the following matrices.

$$U(a,b) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ a^{t+1}+b & a^t & 1 & 0 \\ a^{t+2}+ab+b^t & b & a & 1 \end{bmatrix}, \tag{1}$$

$$M'(\lambda) = \begin{bmatrix} \lambda^{t+1} & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda^{-1} & 0 \\ 0 & 0 & 0 & \lambda^{-t-1} \end{bmatrix}, \tag{2}$$

$$T = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}. \tag{3}$$

If $\omega \in \mathbb{F}_q$ is a primitive element, then $\mathrm{Sz}(q) = \langle U(1,0), M'(\omega), T \rangle$. This is our standard copy of $\mathrm{Sz}(q)$, denoted Σ. This group acts on the Suzuki ovoid, which is

$$\mathcal{O} = \{(1:0:0:0)\} \cup \left\{ (a^{t+2}+ab+b^t : b : a : 1) \mid a, b \in \mathbb{F}_q \right\}. \tag{4}$$

Let $\mathcal{F} = \left\{ U(a,b) \mid a, b \in \mathbb{F}_q \right\}$ and $\mathcal{H} = \left\{ M'(\lambda) \mid \lambda \in \mathbb{F}_q^\times \right\}$. Then $\mathcal{FH} = \mathcal{HF}$ is the stabiliser of $(1:0:0:0) \in \mathcal{O}$, a maximal subgroup of $\mathrm{Sz}(q)$ and $\mathcal{FH} = \langle U(1,0), M'(\omega) \rangle \cong \mathbb{F}_q.\mathbb{F}_q.\mathbb{F}_q^\times$. The group $\mathrm{Sz}(q)$ is partitioned into two sets as

$$\mathrm{Sz}(q) = \mathcal{FH} \cup \mathcal{FHTF} = \mathcal{HF} \cup \mathcal{HFTF}. \tag{5}$$

If G is a conjugate of $\mathrm{Sz}(q)$, so that $G^c = \mathrm{Sz}(q)$ for some $c \in \mathrm{GL}(4,q)$, we say that the ordered triple of elements $\alpha, h, \gamma \in G$ are *rewriting generators for G with respect to c* if

- $\alpha^c \in \mathcal{F}$, $h^c \in \mathcal{FH}$, $\gamma^c = T$,
- α has order 4 and h has odd order not dividing $r-1$ for any r such that q is a non-trivial power of r.