# Computing Generators of Groups preserving a Bilinear Form over Residue Class Rings

Alexander Hulpke

*Department of Mathematics, Colorado State University, 1874 Campus Delivery, Fort Collins, CO, 80523-1874, USA*

**Abstract**

We construct generators for symplectic and orthogonal groups over residue class rings modulo an odd prime power. These generators have been implemented and are available in the computer algebra system GAP.

*Key words:* Symplectic Group, Generators, Residue Class Ring

## 1. Introduction

Let $p$ be an odd prime. Consider a matrix $J \in M_n(\mathbb{Z})$ which is non-singular modulo $p$ and for which $J^T = \pm J$. This matrix $J$ then defines a bilinear form over the field $\mathbb{F}_p$ with $p$ elements, as well as over all residue class rings $R = \mathbb{Z}/q\mathbb{Z}$, $q = p^a$. We will use $\mathbb{Z}_q$ as a shorthand for $\mathbb{Z}/q\mathbb{Z}$.

Let $F_n(R)$ be the group of matrices preserving the form given by $J$, that is

$$F_n(R) = \left\{ A \in M_n(R) \mid A^T \cdot J \cdot A = J \right\}.$$

This group $F_n(R)$ is called an orthogonal group if $J$ is symmetric ($J = J^T$); it is called a symplectic group if $J$ is alternating ($J = -J^T$). Recent work in number theory by Jones and Rouse (2010) motivates the study of symplectic groups $\mathrm{Sp}_n(\mathbb{Z}_q)$ where $q$ is a proper prime power.

If $q$ is prime, generators for symplectic groups have been given in Taylor (1987). Similarly generators for orthogonal groups are given in Rylands and Taylor (1998). The purpose of this note is to show how to extend this result to obtain generators for these groups over a ring $R = \mathbb{Z}_q$ if $q$ is a proper odd prime power. It can be viewed as approximating quotients of the form-preserving groups over the $p$-adic numbers.

*Email address:* hulpke@math.colostate.edu (Alexander Hulpke).

*URL:* http://www.math.colostate.edu/ hulpke (Alexander Hulpke).

## 2. Lifting Generators

The heart of the construction is the sequence of reduction homomorphisms that iteratively approximate $F_n(\mathbb{Z}_{p^k})$ by quotient groups.

$$\cdots \to F_n(\mathbb{Z}_{p^k}) \to \cdots F_n(\mathbb{Z}_{p^3}) \to F_n(\mathbb{Z}_{p^2}) \to F_n(\mathbb{F}_p).$$

Our goal will be to construct generators for the groups by stepping through this sequence from right to left, starting with the form-preserving group $F_n(\mathbb{F}_p)$ defined over the prime field for which we assume that generators are known from Taylor (1987) and Rylands and Taylor (1998).

We shall consider a single step in this sequence. Let $q = p^a$, $a > 1$, $r = p^{a-1}$, $G = F_n(\mathbb{Z}_q)$ and $H = F_n(\mathbb{Z}_r)$. Reduction modulo $r$ yields the homomorphism $\varphi\colon G \to H$. We will represent elements of both groups using matrices with integer entries.

Consider an element $h \in H$, which is represented by a matrix $B \in M_n(\mathbb{Z})$ such that $B^T \cdot J \cdot B \equiv J \pmod{r}$, that is $B^T \cdot J \cdot B = J + r \cdot E$ for a suitable matrix $E \in M_n(\mathbb{Z})$.

We want to find a matrix $C$ such that $C \equiv B \pmod{r}$ and that $C^T \cdot J \cdot C \equiv J \pmod{q}$.

With the ansatz $C = B + r \cdot D$ (again assuming $D \in M_n(\mathbb{Z})$) we get that

$$\begin{aligned} C^T \cdot J \cdot C &= (B^T + r \cdot D^T) \cdot J \cdot (B + r \cdot D) \\ &= B^T \cdot J \cdot B + r\left(D^T \cdot J \cdot B + B^T \cdot J \cdot D\right) + r^2 \cdot D^T \cdot J \cdot D \\ &\equiv J + r\left(E + D^T \cdot J \cdot B + B^T \cdot J \cdot D\right) \pmod{q}. \end{aligned}$$

The condition $C^T \cdot J \cdot C \equiv J \pmod{q}$ then becomes

$$r\left(E + D^T \cdot J \cdot B + B^T \cdot J \cdot D\right) \equiv 0 \pmod{q}.$$

Dividing by $r$, we can write this as

$$E + D^T \cdot J \cdot B + B^T \cdot J \cdot D \equiv 0 \pmod{p}$$

which for a fixed $B$ (and $E = \frac{1}{r}(B^T \cdot J \cdot B - J)$) is a system of linear equations in the entries of $D$.

We claim that for symmetric or alternating $J$ this system has a solution:

First consider the case that $J$ is alternating. Then $E$ is alternating as well and the condition becomes (setting $X = D^T \cdot J \cdot B$) $E \equiv -X + X^T \pmod{p}$, which clearly has a solution in setting $X$ to be the negative upper triangular part of $E$.

If $J$ is symmetric a similar argument holds: In this case $E$ is symmetric and the condition becomes $E \equiv X + X^T \pmod{p}$ (again with $X = D^T \cdot J \cdot B$). We get a solution for $X$ as an upper triangular matrix whose off-diagonal entries are equal to those $E$, and whose diagonal is half (using $p \neq 2$) the diagonal of $E$.

In either case we can solve modulo $p$ for $D$ from $X$, since we assumed $J$ and $B$ to be invertible modulo $p$. This shows that in these two cases $\varphi$ is surjective. (In general, $\varphi$ is not surjective, see the remark at the end of section 4.1.)

As $p \neq 2$ we observe that the condition of leaving the form invariant implies that $\det(B) \equiv \pm 1 \pmod{r}$ and $\det(C) \equiv \pm 1 \pmod{q}$. As $\det(C) = \det(B + r \cdot D) \equiv \det(B) \pmod{r}$ we thus have $\det(C) = \det(B) + ry$ for some $y \in \mathbb{Z}$. But then

$$1 \equiv (\det(C))^2 \equiv (\det(B) + ry)^2 \equiv \det(B)^2 + 2\det(B)ry \equiv 1 + 2\det(B)ry \pmod{q},$$

and thus $2\det(B)ry \equiv 0 \pmod q$. As $2\det(B)$ is invertible modulo $q$, this implies that $ry \equiv 0 \pmod q$ and thus $\det(C) \equiv \det(B) \pmod q$, that is the lifting process preserves the values of determinants. In particular this implies $\ker\varphi \leq \mathrm{SL}_n(q)$ as in this case $B = I$ has determinant 1.

### *2.1. Description of* $\ker\varphi$

To describe the kernel of $\varphi$, we set $B = I$ (and thus get $E = 0$). This yields a homogeneous system of equations

$$D^T \cdot J + J \cdot D \equiv 0 \pmod p \tag{1}$$

If $J$ is alternating (for $J = -J^T$ the condition simply states that $JD$ must be symmetric) the solution space of of this system has dimension $\frac{n(n+1)}{2}$, that is $|\ker\varphi| = p^{\frac{n(n+1)}{2}}$. Similarly, if $J$ is symmetric the solution space has dimension $\frac{n(n-1)}{2}$ and $|\ker\varphi| = p^{\frac{n(n-1)}{2}}$.

The kernel of $\varphi$ thus consists of elements of the form $I + r \cdot D$ such that (1) holds. For such an element $C$, we call $D = \frac{1}{r}(C - I)$ the *$r$-relic*. Multiplication in $\ker\varphi$ happens by addition of the elements $r$-relics, as

$$(I + rD_1)(I + rD_2) = I + r(D_1 + D_2) + r^2 D_1 D_2 \equiv I + r(D_1 + D_2) \pmod q.$$

Using this linearization we can calculate in $\ker\varphi$ as a vector space over $\mathbb{F}_p$.

This linearization in particular implies that $\ker\varphi$ is an elementary abelian $p$-group; thus the form preserving group $F_n(R)$ is an iterated extension of copies of an $\mathbb{F}_p$ vector space by $F_n(\mathbb{F}_p)$.

**Lemma 1.** *The action of $g \in G$ on $k \in \ker\varphi$ is by conjugating the $r$-relic of $k$ with the image of $g$ in $F_n(p)$.*

*Proof.* Let $k \in \ker\varphi$ represented by $I + rD \in M_n(\mathbb{Z})$ and $g \in G$, represented by $C \in M_n(\mathbb{Z})$. As $gkg^{-1} \in \ker\varphi$, we can represent $gkg^{-1}$ by $I + r\widetilde{D} \in M_n(\mathbb{Z})$ and have that

$$C + rCD \equiv C\,(I + rD) \equiv \left(I + r\widetilde{D}\right) C \equiv C + r\widetilde{D}C \pmod q$$

thus $CD \equiv \widetilde{D}C \pmod p$, thus $\widetilde{D} \equiv CDC^{-1} \pmod p$. □

**Corollary 2.** *Denote by $\psi$ the reduction of $F_n(\mathbb{Z}_q)$ modulo $p$. Then elements of* $\ker\psi$ *act trivially on* $\ker\varphi$.

### *2.2. Obtaining Generators*

We now use this lifting process to obtain generators. In each step ($r = p^{a-1}$, $q = p^a$) we will assume that we have a generating set $\underline{\mathbf{h}} = \{h_i\}$ for $H = F_n(\mathbb{Z}_r)$ and want to obtain a generating set for $G = F_n(\mathbb{Z}_q)$. Initializing in the first step with the known generators for $F_n(\mathbb{Z}_p)$ this step is repeated up to the desired value of $q$. As above, $\varphi\colon G \to H$ denotes reduction modulo $r$.

The first part of the construction of a generating set for $G$ is to obtain – using the lifting process from section 2 – for each generator $h_i$ a pre-image $g_i \in G$ with $g_i^{\varphi} = h_i$. Together they form a set $\underline{\mathbf{g}} = \{g_i\}$.

We now need to ensure that $G = \langle\underline{\mathbf{g}}\rangle$. This is equivalent to showing that $\ker\varphi \subset \langle g_i\rangle$. If $\ker\varphi$ is known to be irreducible this is already guaranteed if we know that $\langle\underline{\mathbf{g}}\rangle \cap \ker\varphi \neq$

$\langle 1\rangle$, which in turn is guaranteed if we know that $G$ does not split over $\ker\varphi$. Both conditions usually hold in the case of symplectic groups as will be shown in section 3 below.

In case this information is not available, we can test the condition directly: Solving (1) provides a basis for $\ker\varphi$.

We then form a few (in examples often just one or two were sufficient) random elements of $\ker\varphi$ by evaluating relators for $H$ in the $g_i$ and take the subgroup $S \leq \ker\varphi$ generated by these elements. Suitable relators can be formed for example as $w^k$ where $w$ is a short word in the generators of $H$, and $k$ the order of the element $w(\underline{\mathbf{h}}) \in H$ obtained from evaluating this word. (Removing randomness, we could use a presentation for $H$, initially starting with the classical group modulo $p$, and for the next step transform this into a presentation for $G$, using methods from Babai et al. (1997).)

We then use conjugation action of $\langle\underline{\mathbf{g}}\rangle$ (as we know that $G = \langle\underline{\mathbf{g}}, \ker\varphi\rangle$ this is equivalent to the action of $G$) to form the normal closure $N$ of $S$ under $G$. This calculation takes place in $\ker\varphi$, and we can use the linearization, described after equation (1), to compute a basis of $N$, using only linear algebra. If $N \neq \ker\varphi$ we add sufficiently many elements of $\ker\varphi$ (computed as solutions of (1)) to $\underline{\mathbf{g}}$ to obtain a generating set of $G$.

As we know the dimension (and thus the order) of $\ker\varphi$, this also yields $|G|$ from $|H|$.

We will describe an algorithm, implementing this process, below in section 4

## 3. The structure of symplectic groups

The aim of this section is to show that in the case of symplectic groups (with the exception of $\mathrm{Sp}_2(\mathbb{Z}_9)$) the lifted generators $\underline{\mathbf{g}}$ are guaranteed to generate $G$. We will do so (as already indicated in the previous section) by showing that $\ker\varphi$ is irreducible and that $G$ does not split over $\ker\varphi$.

First consider irreducibility. From lemma 1, we see that the action of $G$ on $\ker\varphi$ is in fact the adjoint representation of $\mathrm{Sp}_n(p)$. By Theorem 2.4.13 in Goodman and Wallach (2009) this representation is irreducible for the complex Lie group $\mathrm{Sp}_n(\mathbb{C})$, and by Curtis (1960) this result carries over to the corresponding Lie-type groups over finite fields.

In the remainder of this section we shall prove that $G$ is in general not split over $\ker\varphi$. In particular we shall prove the following:

**Theorem 3.** *Let $n$ be even, $a \geq 1$, $R = \mathbb{Z}_{p^a}$, $J = \begin{pmatrix} & I_{\frac{n}{2}} \\ -I_{\frac{n}{2}} & \end{pmatrix}$, $G = F_n(R) = \mathrm{Sp}_n(R)$ the symplectic group, and $\varphi\colon G \to \mathrm{Sp}_n(\mathbb{Z}_{p^{a-1}})$ the reduction modulo $p^{a-1}$.*

*Then $G$ does not split over $K = \ker\varphi$, unless $n = 2, p = 3, a = 2$ in which case it splits.*

Again, we shall identify elements of the groups with matrices in $M_n(\mathbb{Z})$.

We first consider the case of dimension $n = 2$, the result them will follow for larger dimensions by lemma 6.

In the first step we show that the theorem holds once $a > 2$:

**Lemma 4.** *If $n = 2$ and $a > 2$ then $G$ is not split over $K$.*

*Proof.* Denote by $L = \{g \in G \mid g \equiv I \pmod{p^{a-2}}\}$ the kernel of the projection from $G$ onto $\mathrm{Sp}_2(\mathbb{Z}_{p^{a-2}})$. Let $v = 1 + p^{a-2}$. Then $\gcd(v, p^a) = 1$ and thus $v^{-1} \bmod p^a$ exists. Consider the matrix

$$A = \begin{pmatrix} v & 0 \\ 0 & v^{-1} \end{pmatrix} \bmod p^a.$$

Then we get that $A^T \cdot J \cdot A = J$ and $A \equiv I \pmod{p^{a-2}}$ but $A \not\equiv I \pmod{p^{a-1}}$. This means that $A \in G$, $A \in L$, but $A \notin K$.

By the binomial formula we have that $v^p \equiv 1 + p^{a-1} \pmod{p^a}$ and $v^{p^2} \equiv 1 \pmod{p^a}$. Thus $A$ represents an element of order $p^2$.

If $G$ were to split over $K$, then $L$ would split over $K$ as well. But by corollary 2 the group $L$ acts trivially on $K$. This would imply that $L$ was elementary abelian, contradicting the existence of an element of order $p^2$. □

We now consider the case $a = 2$ and larger primes:

**Lemma 5.** *Theorem 3 is true for $n = 2$, $a = 2$ and $p > 3$.*

*Proof.* Let $B = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. Then $B$ represents an element of order $p$ in $\mathrm{Sp}_2(p)$. Using the method of section 2, we find that the pre-images of $B$ in $G = \mathrm{Sp}_2(\mathbb{Z}_{p^2})$ have the form $C = \begin{pmatrix} (1 + xp) & zp \\ (-1 - (x + y)p), & (1 - (x + z)p) \end{pmatrix}$ for values $x, y, z \in \{0, \ldots, p - 1\}$. Then

$$C^k \equiv \begin{pmatrix} (1 + kxp - \frac{k(k-1)}{2} zp) & kzp \\ (-k - k(x + y)p + \frac{(k-1)k(k+1)}{6} zp), & (1 - kxp - \frac{k(k+1)}{2} zp) \end{pmatrix} \pmod{p^2}.$$

(This is seen by an induction argument whose base case $k = 1$ is trivial, and whose step follows immediately from a symbolic matrix multiplication modulo $p^2$.) We note that the formal fraction $\frac{(k-1)k(k+1)}{6}$ actually is an integer as one of the numerator factors must be a multiple of 3 and at least one a multiple of 2. Similarly $\frac{k(k+1)}{2}$ is an integer.

Setting $k = p$ in this formula we obtain that $C^p \equiv \begin{pmatrix} 1 & 0 \\ -p & 1 \end{pmatrix} \pmod{p^2}$.

That means that the order of the element represented by $C$ is strictly larger than $p$ which in turn implies that the group $\langle K, C \rangle$ does not split over $K$ (otherwise there would be at least one lift $C$ for $B$ that had order $p$) and therefore $G$ cannot split over $K$ either. □

For $p = 3$, we consider the cases $n = 4$ and $n = 2$ explicitly: Construct $\mathrm{Sp}_4(\mathbb{Z}_9)$ (respectively $\mathrm{Sp}_2(\mathbb{Z}_9)$) using the method from the previous section. By acting on the vectors of $(\mathbb{Z}_9)^4$ (respectively $(\mathbb{Z}_9)^2$) we obtain a faithful permutation representation of the group of degree 6561 (respectively 81). We now can use the methods of (Holt et al., 2005, Section 7.6.2) to test whether the group splits over $\ker \varphi$. An explicit calculation in GAP (2012) shows that $\mathrm{Sp}_2(\mathbb{Z}_9)$ splits over $\ker \varphi$, but $\mathrm{Sp}_4(\mathbb{Z}_9)$ does not split.

We finally extend the result to arbitrary dimensions:

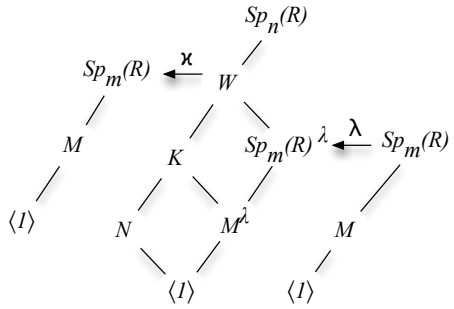


Fig. 1. Illustration for the proof of lemma 6

**Lemma 6.** *Let $p$ be an odd prime, $R = \mathbb{Z}_{p^a}$ and $n \geq 4$ even. Then $\mathrm{Sp}_n(R)$ is not split over $\ker\varphi$.*

*Proof.* Let $p$ be an odd prime and $n \geq 4$ even. If $p > 3$ we let $m = 2$, if $p = 3$ let $m = 4$. From the previous calculations we already know that $\mathrm{Sp}_m(R)$ does not split over its $\ker\varphi$ and we thus can assume without loss of generality that $n > m$.

Consider the homomorphism

$$\lambda\colon \mathrm{Sp}_m(R) \to \mathrm{Sp}_n(R), \qquad g \mapsto \begin{pmatrix} I_{\frac{n-m}{2}} & & \\ & g & \\ & & I_{\frac{n-m}{2}} \end{pmatrix}$$

which is obviously injective. Let $\varphi_n\colon \mathrm{Sp}_n(R) \to \mathrm{Sp}_n(\mathbb{Z}_{p^{a-1}})$ and $\varphi_m\colon \mathrm{Sp}_m(R) \to \mathrm{Sp}_m(\mathbb{Z}_{p^{a-1}})$ the reduction maps in both groups and let $K = \ker\varphi_n$, $M = \ker\varphi_m$ and $W = K \cdot (\mathrm{Sp}_m(R)^\lambda)$ (see figure 1).

Then $M^\lambda \leq K$. Let

$$N = \left\{ I + pD \;\middle|\; (JD)^T = JD, \quad D = \begin{pmatrix} * & * & * \\ * & 0_m & * \\ * & * & * \end{pmatrix} \right\},$$

that is $N$ consists of those matrices in $K$ whose central $m \times m$ block is $I_m$. As multiplication in $K$ is done by addition of relics, $N$ is a group. The conditions on $D$ imply that $JD$ is symmetric and has the central $m \times m$ block zero, thus $N$ has $p$-dimension $\frac{n(n+1)}{2} - \frac{m(m+1)}{2}$. As $N \cap \mathrm{Sp}_m(R)^\lambda = \langle 1\rangle$ this means that $N$ is a complement to $M^\lambda$ in $K$. Matrix multiplication shows that $N$ is normal under $\mathrm{Sp}_m(R)^\lambda$, thus $N \lhd W$ and $W/N \cong \mathrm{Sp}_m(R)$. Let $\kappa\colon W \to \mathrm{Sp}_m(R)$, then $K^\kappa = M$.

If $\mathrm{Sp}_n(R)$ were to split over $K$, then $W$ also would have to split over $K$, denote a complement by $A$. Then $A^\kappa$ would be a complement to $M = K^\kappa$ in $\mathrm{Sp}_m(R)$, contradiction. □

This concludes the proof of theorem 3.

## 4. Algorithms

The lifting process described in section 2 is implemented by the following algorithm. Again we represent elements of $G = \mathrm{Sp}_n(\mathbb{Z}_q)$ by integral matrices and represent elements of $\ker\varphi$ by their $r$-relic to consider $\ker\varphi$ as an $\mathbb{F}_p$ vector space using (1). If $X \in M_n(\mathbb{Z})$, $\det(X) \not\equiv 0 \pmod p$ describes an element of $G$ and $D$ is a $r$-relic, the conjugation image of $I + rD$ under $X$ then is described by its $r$-relic

$$\gamma(D, X) = \frac{1}{r}\left(X^{-1} \cdot (I + r \cdot D) \cdot X - I\right) \pmod p.$$

Algorithm `LiftFormPreserving(`$p$`,`$a$`,`$n$`,`$J$`,`$\underline{\mathbf{h}}$`)`

**Input:** An odd prime $p$, An exponent $a > 0$, a dimension $n > 0$, a symmetric or alternating matrix $J \in M_n(\mathbb{Z})$ describing a bilinear form, A set of elements $\underline{\mathbf{h}} \subset M_n(\mathbb{Z})$ that generate (when considering them as elements of $M_n(\mathbb{F}_p)$) the subgroup of $\mathrm{GL}_n(p)$ preserving $J$.

**Output:** A set of matrices $\underline{\mathbf{g}} \subset M_n(\mathbb{Z})$ that generate the subgroup of $\mathrm{GL}_n(\mathbb{Z}_{p^a})$ preserving $J$.

1: $\underline{\mathbf{g}} := \underline{\mathbf{h}}$; $e := 1$;$r := p$;
2: **while** $e < a$ **do**
3: $\underline{\mathbf{g}} := []$;
4: **for** $B \in \underline{\mathbf{h}}$ **do**
5: Let $E = 1/r \cdot (B^T \cdot J \cdot B - J)$;
6: By solving a system of linear equations modulo $p$ (whose variables are the entries in $D$), determine a single $D \in M_n(\mathbb{Z})$ such that

$$E + D^T \cdot J \cdot B + B^T \cdot J \cdot D \equiv 0 \pmod p$$

7: Append $B + r \cdot D$ to $\underline{\mathbf{g}}$;
8: **od**;
9: **if** it is not known a priori that $G = \langle\underline{\mathbf{g}}\rangle$ **then**
10: Determine a basis $\underline{\mathbf{k}}$ for the nullspace of the system of linear equations (whose variables are the entries in $D$)

$$D^T \cdot J + J \cdot D \equiv 0 \pmod p;$$

11: $i := 1$; $\underline{\mathbf{s}} := []$;
12: **while** $i <= 10$ and $|\underline{\mathbf{s}}| < |\underline{\mathbf{k}}|$ **do**
13: Let $A$ be a random product in $\underline{\mathbf{g}}$, using Celler et al. (1995);
14: Let $o$ be the order of $A$ as an element of $\mathrm{GL}_n(\mathbb{Z}_{p^e})$; {use `MatrixOrder` routine below.}
15: Let $B := \frac{1}{r}(A^o - I)$;
16: **if** $B \notin \langle\underline{\mathbf{s}}\rangle_{\mathbb{F}_p}$ (vector space span) **then**
17: Add $B$ to $\underline{\mathbf{s}}$;
18: **for** $D \in \underline{\mathbf{s}}$ **do**
19: **for** $X \in \underline{\mathbf{g}}$ **do**
20: Let $Y := \gamma(D, X)$;
21: **if** $Y \notin \langle\underline{\mathbf{s}}\rangle_{\mathbb{F}_p}$ **then**
22: Add $Y$ to $\underline{\mathbf{s}}$;
23: **fi**;

24: **od**;
25: **od**;
26: **fi**;
27: $i := i + 1$;
28: **od**;
29: **if** $|\underline{\mathbf{s}}| < |\underline{\mathbf{k}}|$ **then**
30: Determine $\underline{\mathbf{e}} \subset \underline{\mathbf{k}}$, extending $\underline{\mathbf{s}}$ to a basis $\underline{\mathbf{s}} \cup \underline{\mathbf{e}}$ of $\langle \underline{\mathbf{k}} \rangle$.
31: **for** $E \in \underline{\mathbf{e}}$ **do**
32: Add $(I + r \cdot E)$ to $\underline{\mathbf{g}}$
33: **od**;
34: **fi**;
35: $r := r \cdot p$; $e := e + 1$;
36: **fi**;
37: **od**;
38: **return** $\underline{\mathbf{g}}$.

Lines 4-8 lift the known generators modulo $r$ to generators modulo $p \cdot r$. Line 10 determines $\ker \varphi$ in linearized form. Lines 13-15 determine pseudo-random elements of $\ker \varphi$. We consider this kernel as an $\mathbb{F}_p$ vector space, the subspace $S$ spanned by the elements found so far is given by the basis $\underline{\mathbf{s}}$. Lines 18-25 implement a basic spinning algorithm (Holt et al., 2005, p.231) that forms the closure of $S$ under the action of $G$ given by $\gamma$. Due to the choice of random elements, it is possible that not all of $\ker \varphi$ was found (though so far this has not happened in a single example tested), Lines 29-34 therefore add elements if necessary. (Again, one could add elements one-by-one and use the spinning algorithm.)

*4.1. Example*

For $\mathrm{Sp}_2(5)$, Taylor (1987) gives the generators and form

$$B_1 = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}; \qquad B_2 := \begin{pmatrix} 4 & 1 \\ 4 & 0 \end{pmatrix}; \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

In line 5 of the algorithm, we get corresponding values for $E = 1/r \cdot (B^T \cdot J \cdot B - J)$:

$$E_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \qquad E_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Setting $D = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the equation system in line 6 for $E_1$ results in the equation $3a + 2d + 1 \equiv 0 \pmod 5$. We choose the solution $D = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$, and thus get the first generator $G_1 = B_1 + 5 \cdot D = \begin{pmatrix} 7 & 0 \\ 0 & 18 \end{pmatrix}$. Similarly we get from $B_2$ and $E_2$ the equation

$4b + c - 4d + 1 \equiv 0 \pmod 5$ with correcting matrix $D = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}$ and generator $G_2 = B_2 + 5 \cdot D = \begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix}$. The arguments from section 3 show that $G_1$ and $G_2$ are generators of $\mathrm{Sp}_2(25)$.

By modifying the example we see that for arbitrary $\varphi$ we do not have surjectivity of $\varphi$: Let $J = \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}$, which is neither alternating, nor symmetric. Then $\mathrm{Sp}_2(5)$ of course remains the subgroup of $\mathrm{GL}_2(5)$ preserving $J$. However working modulo 25, one gets (by an explicit stabilizer computation in $\mathrm{GL}_2(\mathbb{Z}_{25})$) that the group stabilizing $J$ modulo 25 is

$$\left\langle \begin{pmatrix} 2 & 0 \\ 0 & 13 \end{pmatrix}, \begin{pmatrix} 2 & 10 \\ 0 & 13 \end{pmatrix}, \begin{pmatrix} 13 & 0 \\ 10 & 2 \end{pmatrix} \right\rangle$$

of order 500. The image this group under the reduction homomorphism $\varphi$ has only order 4, showing that $\varphi$ is not surjective in this case.

### *4.2. Element orders*

The determination of matrix orders over finite fields can be done efficiently using the linear algebra techniques of Celler and Leedham-Green (1997). Over residue class rings these methods don't immediately apply, which has the potential to make the determination of the order $o$ in line 14 of the algorithm very costly. To avoid this bottleneck we again use the factor structure given by reduction modulo smaller powers of $p$:

Consider the homomorphism $\psi\colon G \to \mathrm{GL}_n(\mathbb{F}_p)$ given by reduction modulo $p$. To determine the order of $x \in G$, we first determine the order $a = \left|x^\psi\right|$ in the factor group over a finite field. We then replace $x$ by $y = x^a \in \ker\psi$, clearly $|x| = a \cdot |y|$.

By the remark following equation (1) we furthermore know that $\ker\psi$ is composed from $p$-elementary abelian layers. Consider the reduction $\varphi$ modulo $p^2$. Then either $y \in \ker\varphi$, or $y^\varphi$ has order $p$. In this second case we replace $y$ by $y^p$ to descend to $\ker\varphi$. Iterating, and remembering how often a $p$-th power was taken yields $|y|$ as desired.

More formally, we get the following algorithm for element orders over $\mathbb{Z}_{p^a}$:

Algorithm `MatrixOrder(`$x$`,`$p$`,`$a$`)`
**Input:** A matrix $x \in \mathrm{GL}_n(\mathbb{Z}_{p^a})$.
**Output:** The multiplicative order of $x$.

1: Let $y := x \bmod p \in \mathrm{GL}_n(\mathbb{F}_p)$.
2: Let $o := |y|$. {using Celler and Leedham-Green (1997)}
3: Let $z := x^o$. $e := p$
4: **while** $e < p^a$ **do**
5: $\quad e := e \cdot p$;
6: $\quad$ **if** $z \not\equiv I \pmod e$ **then**
7: $\quad\quad o := o \cdot p$;
8: $\quad\quad z := z^p$;

9: **fi**;
10: **od**;
11: **return** $o$.

*Proof.* After each iteration of the **while**-loop $z \equiv I \pmod{e}$, thus $z = I$ when the algorithm terminates. This is done by taking powers of $z$, which are accumulated in $o$. So clearly $|x|$ is a divisor of $o$. If $|x|$ was strictly smaller, either the calculation of $o$ in line 2, or the congruence test in line 6 would have had to fail. □

For example, let $x = \begin{pmatrix} 44 & 107 \\ 76 & 57 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_{5^3})$. Modulo 5 we have that $x \equiv y \in \mathrm{GL}_2(5)$ with $|y| = 6$. We set $z = x^6 \bmod 5^3 = \begin{pmatrix} 101 & 75 \\ 100 & 26 \end{pmatrix}$. Then $z \equiv I \pmod{5^2}$, so in the first iteration of the **while**-loop nothing happens. But $z \not\equiv I \pmod{5^3}$, so we set $z := z^5 \bmod 5^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and obtain order $6 \cdot 5 = 30$.

Using these routines, it is now easy to construct generating sets for particular geometric conditions:

Algorithm `SymplecticGenerators(`$n$`,`$p^a$`)`
**Input:** A dimension $n > 0$ and an odd prime power $p^a$.
**Output:** A set of matrices $\underline{\mathbf{g}} \subset M_n(\mathbb{Z})$ that generate $\mathrm{Sp}_n(\mathbb{Z}_{p^a})$./
1: Using Taylor (1987), determine generators $\underline{\mathbf{h}}$ for $\mathrm{Sp}_n(p)$; Let $J \in M_n(\mathbb{Z})$ be the alternating matrix representing the form preserved by this group;
2: return the result of `LiftFormPreserving(`$p$`,`$a$`,`$n$`,`$J$`,`$\underline{\mathbf{h}}$`)`

By choosing different generating sets in line 1, one can get generators for general or special orthogonal groups.

Functionality for such generating sets will be available in the computer algebra system GAP (2012), in release 4.5.3 [1], using the functions
`SymplecticGroup(`*dim*`,Integers mod `*q*`)`,
`GeneralOrthogonalGroup(`*dim*`,`*sign*`, Integers mod `*q*`)`, and
`SpecialOrthogonalGroup(`*dim*`,`*sign*`, Integers mod `*q*`)`.

## 5. Performance

The following table shows runtimes (in seconds on a 2.66GHz Mac Pro, time averages over 10 runs) for constructing generators of $\mathrm{Sp}_n(\mathbb{Z}_{3^a})$ for some values of $n$ and $a$. For each increase of $a$ by 1 the order of the group generated increases by a factor of $3^{n(n+1)/2}$, i.e. for example $\mathrm{Sp}_{10}(\mathbb{Z}_{3^{12}})$ has order roughly $10^{314}$.

[1] Note to reviewer: This release is not yet publicly available as of this writing, but I expect it will be so before the paper is published.

To illustrate the behavior of the test for kernel generation, these tests did not use the shortcut in line 9 of the generator set algorithm (the property holds for symplectic groups as shown in section 3).

| n | a=2 | 4 | 8 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 0.1 | 0.5 | 1.1 | 1.5 | 1.8 | 1.9 | 2.2 | 2.3 | 2.5 | 2.8 | 3.0 | 3.2 |
| 12 | 0.9 | 2.8 | 7.1 | 9.0 | 10 | 11 | 12 | 14 | 15 | 16 | 17 | 18 |
| 16 | 3.4 | 11 | 26 | 33 | 37 | 40 | 44 | 48 | 54 | 57 | 62 | 65 |
| 20 | 9.9 | 31 | 73 | 94 | 106 | 115 | 129 | 137 | 150 | 161 | 171 | 187 |

These runtimes are dominated by the spinning algorithm in lines 17-24 and correspondingly scale roughly like $n^4$ ($n$ matrix multiplications at a cost of $n^3$ each) and linear in $a$ (as there are $a$ iterations in the main loop).

The behavior for other primes is similar.

If instead we use the shortcut in line 9, the runtimes reduce substantially, for example the last column (for $\mathrm{Sp}_n(\mathbb{Z}_{3^{18}})$) the times become $0.2, 0.9, 3, 7$ respectively, scaling roughly like the $n^3$ cost of solving a system of linear equations, but remaining linear in $a$.

While these times clearly leave space for improvement, this determination of group generators is typically invoked only once in a longer calculation with the time for determining generators being negligible in comparison to the actual calculations done later. Improvements therefore should concentrate on routines such as matrix arithmetic (in particular over residue class rings, for which improvements similar to the ones for element order in section 4.2 might be possible) will have a more general impact.

**Acknowledgements**

The author is grateful to Jeffrey D. Achter and to Cassandra Williams for posing the problem as well as for discussion. He is indebted to one of the referees for pointing out the direct argument for the surjectivity of $\varphi$ in the case of symmetric and alternating $J$, the counterexample at the end of section 4.1, as well as multiple corrections. Part of this work was done while the author was visiting the University of Auckland, whose hospitality is gratefully acknowledged. The author's work has been supported in part by NSF Grant DUE-0633333

**References**

Babai, L., Goodman, A. J., Kantor, W. M., Luks, E. M., Pálfy, P. P., 1997. Short presentations for finite groups. J. Algebra 194, 97–112.

Celler, F., Leedham-Green, C. R., 1997. Calculating the order of an invertible matrix. In: Finkelstein, L., Kantor, W. M. (Eds.), Proceedings of the 2nd DIMACS Workshop held at Rutgers University, New Brunswick, NJ, June 7–10, 1995. Vol. 28 of DIMACS: Series in Discrete Mathematics and Theoretical Computer Science. American Mathematical Society, Providence, RI, pp. 55–60.

Celler, F., Leedham-Green, C. R., Murray, S. H., Niemeyer, A. C., O'Brien, E. A., 1995. Generating random elements of a finite group. Comm. Algebra 23 (13), 4931–4948.

Curtis, C. W., 1960. On projective representations of certain finite groups. Proc. Amer. Math. Soc. 11, 852–860.

GAP, 2012. GAP – Groups, Algorithms, and Programming, Version 4.5.3. The GAP Group, `http://www.gap-system.org`.

Goodman, R., Wallach, N. R., 2009. Symmetry, representations, and invariants. Vol. 255 of Graduate Texts in Mathematics. Springer.

Holt, D. F., Eick, B., O'Brien, E. A., 2005. Handbook of Computational Group Theory. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL.

Jones, R., Rouse, J., 2010. Galois theory of iterated endomorphisms. Proc. Lond. Math. Soc. (3) 100 (3), 763–794, appendix A by Jeffrey D. Achter.

Rylands, L. J., Taylor, D. E., 1998. Matrix generators for the orthogonal groups. J. Symbolic Comput. 25 (3), 351–360.

Taylor, D. E., 1987. Pairs of generators for matrix groups. I. The Cayley Bulletin 3, 76–85.