

Logarithmic Bray sampling in symplectic and orthogonal groups

Alec Kriebel

ORCID: [0009-0001-9320-500X](https://orcid.org/0009-0001-9320-500X)

22 October 2026 Version 1.0.0 Unrefereed preprint

Abstract

Let t be an actual involution in a natural finite symplectic or orthogonal group over a field of odd order, with both eigenspaces of dimension between one third and two thirds of the natural dimension n . For each eigenspace separately we prove an unconditional $c/\log n$ lower bound for the probability that the even branch of Bray's construction induces a strong involution on that eigenspace. A graph chart reduces the problem to squarefree polynomials and self-adjoint operators. In the orthogonal case the argument retains all four determinant-character sectors, including $q = 3$ and zero-dimensional complements, and gives a square-spinor refinement. We prove a uniform theorem on 192 independently prescribed strong-involution classes using established fixed-point-ratio and maximal-subgroup bounds. A separate quotient-graph argument then proves that $O(\log n(1 + \log(1/\delta)))$ independent uniform samples generate a subgroup containing $C_G(t)''$, with probability at least $1 - \delta$, for all sufficiently large n . This addresses the symplectic and orthogonal parts of the sampling problem recorded in 2016. The corresponding linear and unitary results are prior work. The assertion concerns sample count in natural matrix groups, not total running time or all dimensions.

1 Problem, conventions, and main result

Praeger's 2016 Oberwolfach contribution [8, pp. 2160–2161] asks for a logarithmic improvement in the number of random selections used in Bray's involution-centraliser construction. In its explicit probability question, an odd-characteristic natural classical group G , a fixed strong involution t , and one sign ε are given; the desired lower bound is a constant divided by $\log n$ for the event that the even Bray output acts strongly on $E_\varepsilon(t)$. The two signs are separate assertions. The intended centraliser target is a subgroup containing $C_G(t)''$. The report records the special linear case as solved at the time, the unitary case as work in progress, and the symplectic and orthogonal cases as open.

Throughout, q is an odd prime power, V is a nondegenerate formed $\mathbb{F}_q$ -space of dimension n , and $\log$ means the natural logarithm. The group $\mathrm{Sp}(V)$ preserves a nondegenerate alternating bilinear form β . In the orthogonal case β is symmetric and $Q(v) = \beta(v, v)/2$; $\mathrm{O}(V)$ is its full isometry group, $\mathrm{SO}(V) = \ker \det$, and $\Omega(V) = \mathrm{SO}(V) \cap \ker \theta$, where the spinor norm of reflection in a nonsingular vector v is $Q(v)$ modulo squares. These are natural matrix groups, as in [6, Sections 1.1–1.2]; we do not identify them with their projective quotients. An involution is strong on a space U if both eigenspace dimensions belong to the closed interval $[\dim U/3, 2 \dim U/3]$. Set

$$\mathrm{inv}(y) = \begin{cases} y^{|y|/2} & |y| \text{ even,} \\ 1 & |y| \text{ odd,} \end{cases} \quad z(g) = \mathrm{inv}(tt^g), \quad t^g = g^{-1}tg.$$

Since t inverts tt^g , its unique involution commutes with t . Thus $z(g) \in C_G(t)$, including the odd-order case $z(g) = 1$.

Theorem 1.1. *There is an absolute integer N with the following property. Let $n \geq N$, let G be $\mathrm{Sp}(V)$, or one of $\mathrm{O}(V)$, $\mathrm{SO}(V)$, $\Omega(V)$, and let $t \in G$ be an actual strong involution. For independent uniformly distributed $g \in G$, each of the two events that $z(g)|_{E_\varepsilon(t)}$ is strong has probability at least $c/\log n$, where one may take $c = 1/40000$ for $\mathrm{Sp}(V)$ and $c = 1/5000000$ in the orthogonal cases. Moreover, for every $0 < \delta < 1$ there is an absolute K such that, from at most*

$$K \log n (1 + \log(1/\delta))$$

independent uniform samples, the subgroup generated by all the outputs $z(g)$ contains $C_G(t)''$ with probability at least $1 - \delta$.

The marginal estimates alone hold for $n \geq 49152$ in the symplectic case and $n \geq 98304$ in the orthogonal case. The generation threshold also involves an unspecified absolute constant from a published maximal-subgroup bound. No usable small threshold or efficient recognition procedure is claimed.

Dixon–Praeger–Seress [3, Theorem 1.1] already proved the linear marginal statement; Glasby–Praeger–Roney-Dougal [5, Theorems 1–2] proved the unitary marginal and the linear/unitary generation statements. Their distinguished 2-part method and their use of a final independent sample to escape a diagonal subgroup are antecedents of our approach. The exact special-group transfer introduces no new probability estimate: the full linear or unitary group is its special subgroup times the centraliser of t , because a determinant of arbitrary value can be realised on one eigenspace. Consequently the conjugacy-class laws coincide. We make no claim of a new linear or unitary solution.

The 2026 stingray theorem [4, Theorems 1.1, 1.3] constructs a naturally embedded subgroup of dimension $O(\log n)$ from powers of $O(\log n)$ random elements. Its sampling objects and target differ from the even Bray law for every fixed strong t . Our priority discussion is a bounded comparison with the identified literature, not a proof of worldwide absence of an equivalent theorem. Full bibliographic inspection limits are recorded with the source package.

2 A graph chart and its spectral meaning

Write $V = A \perp B$, with $t = -1$ on A and $+1$ on B , and order the dimensions so that $\dim A \leq \dim B$. Replacing t by $-t$ does not change tt^θ or its centraliser; this replacement need not lie in G . In the orthogonal case we first justify the conjugacy law used below. If both eigenspaces have dimension at least three, each contains a hyperbolic plane and represents every nonzero scalar under Q . Reflections in either eigenspace centralise t , and give both pairs $(\det, \theta) = (-1, 1), (-1, \nu)$, where ν is a nonsquare class. These generate $\mathrm{O}(V)/\Omega(V)$. Therefore

$$\mathrm{O}(V) = \Omega(V)C_{\mathrm{O}(V)}(t).$$

It follows that the O , SO , and Ω conjugacy classes of t are identical as sets. Uniform conjugation in any one of them gives the same uniform distribution on this class. This also permits the relabelling of the two eigenspaces just made without an assumption about $-1 \in G$.

For $F : A \rightarrow B$ let F^* be the adjoint and $K = F^*F$. Suppose K and $1+K$ are invertible. Then F is injective and $F(A)$ is nondegenerate. Its graph $W = \{(u, Fu) : u \in A\}$ has form $\beta_A(1+K)$. If this form is isometric to β_A , the involution s_W which is -1 on W and $+1$ on $W^\perp$ is conjugate to t . Distinct F give distinct graphs. In the symplectic case this isometry condition is automatic; in the orthogonal case it is

$$\chi(\det(1+K)) = 1, \tag{1}$$

where χ is the quadratic character of $\mathbb{F}_q$. If $c = \dim B - \dim A = 0$, the additional embedding condition is

$$\chi(\det K) = \chi(\text{disc } B / \text{disc } A). \quad (2)$$

If $c > 0$, a complementary quadratic space of dimension c and required discriminant always exists; its type is fixed by K . Here and below discriminants mean determinants of bilinear forms modulo squares, without an inserted dimension sign.

Projection onto W along $W^\perp$ is $P_W(u, v) = (w, Fw)$, where $w = (1 + K)^{-1}(u + F^*v)$. Thus $s_W = 1 - 2P_W$, and on $A \oplus F(A)$, using coordinates (u, Fv) , multiplication by t gives

$$ts_W = \begin{pmatrix} (1 - K)(1 + K)^{-1} & 2K(1 + K)^{-1} \\ -2(1 + K)^{-1} & (1 - K)(1 + K)^{-1} \end{pmatrix}. \quad (3)$$

It is identity on $F(A)^\perp \cap B$. For a root $\kappa \neq 0, -1$ of a squarefree polynomial of K , the two eigenvalues satisfy

$$\lambda + \lambda^{-1} = \frac{2(1 - \kappa)}{1 + \kappa}, \quad \kappa = -\frac{(\lambda - 1)^2}{(\lambda + 1)^2}. \quad (4)$$

They are distinct and different from ± 1 . In particular this chart produces semisimple products. All the eigenvalues associated with one irreducible factor have the same 2-part of their orders, since Frobenius and inversion preserve it. If one factor has a strictly larger, nontrivial 2-part than every other factor, $\text{inv}(ts_W)$ is -1 precisely on its entire block. Its negative dimensions on A and B are equal: $2k$ in the symplectic case and k in the orthogonal case, if the factor degree is k in the parametrisations below.

3 Unconditional chart masses

3.1 Symplectic mass

Put $\dim A = 2a$, $\dim B = 2b$, so $a \leq b \leq 2a$. Let f be a monic squarefree polynomial of degree a coprime to $X(X + 1)$. Choose self-adjoint K with minimal polynomial f and characteristic polynomial f^2 . For a factor of degree d , put $L = \mathbb{F}_{q^d}$. Self-adjointness means that the primary space is a two-dimensional L -space with an L -balanced alternating form. The trace pairing on L is nondegenerate, so the balanced form uniquely lifts to an L -bilinear form with that trace. For every $x \in L$, self-adjointness and odd characteristic give $\beta(xu, u) = -\beta(xu, u) = 0$; nondegeneracy of the trace pairing then makes the lift alternating. It is nondegenerate because its trace is. All such forms are isometric, and its isometry centraliser is $\text{Sp}_2(q^d)$. Primary summands are orthogonal: coprime polynomials and self-adjointness give this directly by Bezout's identity. Hence the number of such K is

$$\frac{|\text{Sp}_{2a}(q)|}{\prod_{d \in \deg f} |\text{Sp}_2(q^d)|}.$$

For a fixed K , embeddings of $(A, \beta_A K)$ into B form one orbit, with pointwise stabiliser $\text{Sp}_{2(b-a)}(q)$, by extension of an isometry between nondegenerate subspaces. There are $|\text{Sp}_{2b}| / |\text{Sp}_{2(b-a)}|$ maps F . Division by the full conjugacy-class size $|\text{Sp}_{2(a+b)}| / (|\text{Sp}_{2a}| |\text{Sp}_{2b}|)$, rather than by a conditional chart size, gives the unconditional probability mass

$$P_f = \frac{|\text{Sp}_{2a}|^2 |\text{Sp}_{2b}|^2}{|\text{Sp}_{2(a+b)}| |\text{Sp}_{2(b-a)}| \prod_{d \in \deg f} |\text{Sp}_2(q^d)|} = q^{-a} \frac{\psi_a^2 \psi_b^2}{\psi_{a+b} \psi_{b-a}} \prod_{d \in \deg f} (1 - q^{-2d})^{-1}, \quad (5)$$

where $\psi_r = \prod_{j=1}^r (1 - q^{-2j})$ and $\psi_0 = 1$. The order formula $|\mathrm{Sp}_{2r}| = q^{2r^2+r} \psi_r$ verifies the exponent. Since $\psi_r \geq 1 - \sum_{j \geq 1} q^{-2j} \geq 7/8$, we obtain $P_f > q^{-a}/2$. The case $a = b$ uses the actual order $|\mathrm{Sp}_0| = 1$.

3.2 Orthogonal mass

Now put $\dim A = a$, $\dim B = b$, $a \leq b \leq 2a$. A squarefree self-adjoint K with characteristic polynomial f has on a degree- d primary summand the form $\mathrm{Tr}_{L/\mathbb{F}_q}(cuv)$. This follows from the nondegenerate trace pairing applied to $\beta(u, \cdot)$ and the balancing identity $\beta(xu, v) = \beta(u, xv)$. Changing the L -basis multiplies c by a square. There are exactly two coefficient types; each has isometry centraliser of order two. Their discriminants differ by $N_{L/\mathbb{F}_q}(c)$, and norm preserves quadratic character, as follows from $N(c)^{(q-1)/2} = c^{(q^d-1)/2}$. For s factors, precisely 2^{s-1} coefficient choices realise the prescribed discriminant of A . Each has orbit size $|\mathrm{O}(A)|/2^s$. Thus the total number of K for a fixed f is exactly $|\mathrm{O}(A)|/2$.

The two determinant characters depend only on f :

$$\chi(\det K) = \chi((-1)^a f(0)), \quad \chi(\det(1 + K)) = \chi((-1)^a f(-1)).$$

For $c = b - a > 0$, select any one desired sign for the first determinant, and the sign $+1$ for the second. For $c = 0$ the first sign must instead be the right side of (2). In every case the complement C has fixed isometry type, and the embedding fibre has size $|\mathrm{O}(B)|/|\mathrm{O}(C)|$. The class denominator is $|\mathrm{O}(V)|/(|\mathrm{O}(A)||\mathrm{O}(B)|)$. Consequently every f in this sector has unconditional mass

$$P_f = \frac{|\mathrm{O}(A)|^2 |\mathrm{O}(B)|^2}{2 |\mathrm{O}(V)| |\mathrm{O}(C)|} > \frac{1}{8} q^{-a}. \quad (6)$$

For completeness, write $|\mathrm{O}(U)| = q^{d(d-1)/2} \eta(U)$. For positive dimension,

$$\eta(2r+1) = 2 \prod_{j=1}^r (1 - q^{-2j}), \quad \eta(2r, \varepsilon) = 2(1 - \varepsilon q^{-r}) \prod_{j=1}^{r-1} (1 - q^{-2j}).$$

These give $7/6 \leq \eta \leq 8/3$ (also for dimension one), and $\eta(0) = 1$. Substitution in (6) gives exponent $-a$ and factor at least $2401/18432 > 1/8$. This retains the odd-dimensional full orthogonal orders and the zero-complement constraint. Omitting either would give an incorrect sampling law.

4 Polynomial counting and the two separate marginals

Lemma 4.1. *Let $d = 2^h \geq 4$ and let k/d be odd. There are at least $q^k/(8k)$ monic irreducible polynomials f_* of degree k with the following property. All associated eigenvalues in (4) have 2-part $(q^k - 1)_2$, whereas every factor of degree not divisible by d has strictly smaller 2-part. In the orthogonal parametrisation the two determinant characters of f_* are $+1, -1$, respectively.*

Proof. In the cyclic group $\mathbb{F}_{q^k}^\times$, exactly half the elements have the maximal 2-part. Elements in proper subfields are at most $\sum_{j=1}^{\lfloor k/2 \rfloor} q^j < 3q^{k/2}/2$. Thus at least $q^k/4$ maximal-2-part elements have degree k , for $k \geq 4$, $q \geq 3$. Associate κ by (4). Its degree is k or $k/2$, because λ is quadratic over $\mathbb{F}_q(\kappa)$. The latter possibility would force $\lambda^{q^{k/2}} = \lambda^{-1}$, so its order divides $q^{k/2} + 1$, whose 2-part is two since $k/2$ is even. This contradicts $(q^k - 1)_2 \geq 8$. The map has fibres $\{\lambda, \lambda^{-1}\}$; division by $2k$ proves the count.

Put $E = v_2(q^2 - 1)$. Lifting the elementary factorisation of $q^{2j} - 1$ gives $v_2(q^k - 1) = E + h - 1$. For a factor of degree j , its associated eigenvalue lies in a split or nonsplit quadratic torus: its order divides $q^j - 1$ or $q^j + 1$. If j is odd both possibilities have 2-part at most 2^{E-1} ; if j is even the bound is $2^{E+v_2(j)-1}$. Degrees not divisible by d have a strictly smaller bound. Finally, -1 is a square in $\mathbb{F}_{q^k}$, so κ is a square, while $1 + \kappa = 4\lambda/(\lambda + 1)^2$ is a nonsquare. Norm preserves these characters and gives the asserted determinants. $\square$

Lemma 4.2. *There are at least $q^r/3$ monic squarefree degree- r polynomials coprime to $X(X+1)$. Excluding irreducible factors whose degrees are divisible by d removes at most $q^r(1 + \log a)/d$ for $r \leq a$. For $r \geq 8$, each of the four pairs $(\chi(f(0)), \chi(f(-1)))$ occurs at least $q^r/16$ times before this exclusion. Hence if $d \geq 32(1 + \log a)$, each pair still occurs at least $q^r/32$ times afterwards.*

Proof. For $q \geq 5$ and $r \geq 2$, nonsquarefree polynomials number q^{r-1} , and each forbidden linear root excludes q^{r-1} ; their union leaves at least $q^r(1 - 3/q) \geq q^r/3$. Degrees zero and one are immediate. For $q = 3$, the normalised counting generating function is

$$\frac{1 - u^2/3}{(1 - u)(1 + u/3)^2}.$$

Its coefficient is $3/8 + (-1)^r 3^{-r}(10 - 8r)/16$, at least $1/3$ for every $r \geq 0$ (check $r \leq 2$ directly, and the decreasing error thereafter). For each degree $jd \leq r$, at most $q^{jd}/(jd)$ irreducibles divide q^{r-jd} monic degree- r polynomials. Summing gives the stated exclusion bound.

Extend each of the three nonprincipal characters $\xi = \chi(f(0)), \chi(f(-1)), \chi(f(0)f(-1))$ by zero on forbidden roots. Their ordinary monic generating series is $1 + su$, because the two evaluations are independently uniform in degrees at least two. In degree one the sums are $-1, -\chi(-1), -1$, respectively, so $|s| = 1$. For the product character, the last value follows by counting solutions of $z^2 = c(c-1)$: the equation $(2c-1-2z)(2c-1+2z) = 1$ gives $q-1$ solutions, hence the character sum is -1 . The principal character series is $(1-u)^2/(1-qu)$. Euler products therefore give the squarefree nonprincipal series

$$\frac{(1 + su)(1 - qu^2)}{(1 - u^2)^2}.$$

The coefficients of degrees $2j$ and $2j+1$ are $1 - (q-1)j$ and $s(1 - (q-1)j)$, of absolute value at most $qr/2$ for $r \geq 2$. Fourier inversion on the two signs shows that each sector has size at least $q^r/12 - 3qr/8 \geq q^r/16$ for $r \geq 8$, since $18r \leq q^{r-1}$. The exclusion costs at most $q^r/32$ in any one sector, proving the last assertion. All four sectors are necessary even when $q = 3$. $\square$

For the symplectic case take the least power of two $d \geq 12(1 + \log a)$, so $d < 24(1 + \log a)$. If $a \geq 8192$, then $a \geq 576(1 + \log a) > 24d$; the inequality holds at the endpoint and its left-minus-right derivative is positive thereafter. For strength on A , allow $k \in [a/3, 2a/3]$, and for strength on B , allow

$$k \in [b/3, \min(2b/3, 5a/6)]. \tag{7}$$

Both closed intervals have width at least $a/6$ and upper endpoint at most $5a/6$. An interval of that width contains at least $a/(24d)$ integers of the form d times an odd number: their spacing is $2d$, and the count is at least $a/(12d) - 1 \geq a/(24d)$. In either interval $r = a - k \geq a/6$. By Lemmas 4.1–4.2, for each such k there are at least $q^k/(8k)$ choices of f_* and at least $q^r/4$ choices of the remainder f_0 having no factor of degree divisible by d . The products f_*f_0 are squarefree and counted once, because f_* is the unique factor whose degree is divisible by d . Since $k \leq a$, their total number is at least $q^a/(768d)$. Equation (5) gives probability greater than

$1/(1536d) > 1/(40000 \log n)$. Equation (3) gives negative dimension $2k$ on each eigenspace, precisely the required separate strengths. Strong t implies $a \geq n/6$, hence $n \geq 49152$ suffices.

In the orthogonal case use the least power of two $d \geq 32(1 + \log a)$, so $d < 64(1 + \log a)$. For $a \geq 32768$, $a \geq 1536(1 + \log a) > 24d$. The same intervals and count apply, with $r \geq a/6 \geq 8$. The two required determinant signs select one sector for f_0 , after accounting for the signs $+1, -1$ of f_* . Lemma 4.2 gives at least $q^r/32$ choices in that sector. Thus there are at least $q^a/(6144d)$ admissible products. Equation (6) gives probability greater than $1/(49152d) > 1/(5000000 \log n)$, using $1 + \log a \leq 1 + \log n$ and $n \geq 98304$. Negative dimension k gives each separate strength, including all endpoint and type possibilities.

Lemma 4.3. *In each of these orthogonal good-polynomial chart events, exactly half the mass has both components of z in $\Omega(A) \times \Omega(B)$. Consequently each of the two separate strong-component events, with this extra requirement, has probability at least $1/(10000000 \log n)$.*

Proof. The distinguished primary summand has dimension k divisible by four and square determinant for K . Since $r > 0$, there is at least one other primary summand. Among the 2^{s-1} equally weighted coefficient choices for the fixed total discriminant, exactly 2^{s-2} give square bilinear discriminant to the distinguished A -summand: changing its coefficient type and one other type preserves the total and reverses the chosen summand's discriminant. The centraliser orders and embedding fibre are unchanged. On the corresponding B -summand the discriminant is the same, multiplied by the square determinant of K . The output z is -1 on these summands and identity elsewhere. Its determinant there is $(-1)^k = 1$, and its spinor norm is 2^{-k} times the bilinear discriminant, by an orthogonal basis and the reflection formula. This is a square exactly for the selected half. The assertion is an exact fibre refinement, not an independence assumption about determinant and spinor norm. $\square$

5 Generation from prescribed strong classes

We now establish the exact uniform class-generation input used below rather than importing an unverified scope from [9]. The following published results are the non-elementary inputs. Burness [2, Definitions 1–2, Theorem 1, Corollary 1] proves, for prime-order x and any non-subspace maximal action of an almost simple classical group with natural dimension e , that

$$\text{fpr}(x, S/M) < |x^S|^{-1/2+1/e+\iota}. \quad (8)$$

For the symplectic and orthogonal simple groups here, in sufficiently large dimension, the corrections in his table satisfy $0 \leq \iota \leq 1/(e-2)$. His definition separates subspace actions, namely stabilisers of the relevant nondegenerate or totally singular subspaces; in characteristic two there is an additional orthogonal case which is absent here. Liebeck–Pyber–Shalev [7, Theorem 1.1] give an absolute constant C with the number of maximal subgroups of a finite simple classical group of rank r at most $Cr^{-2/3}|S|$. We use these as established theorems, including their classification-based proofs, not as assertions verified by the finite computations of this paper.

Theorem 5.1. *There is an absolute e_0 such that, for $e \geq e_0$ and odd q , let $J = \text{Sp}_e(q)$ or $\Omega(U)$ for a nondegenerate orthogonal e -space U . From any prescribed sequence of 192 strong-involution conjugacy classes of the actual natural group J , independent uniform choices generate J with probability at least $1 - q^{-e}$. The classes need not coincide.*

Proof. We give the subspace estimates explicitly. In a formed e -space let D be its full isometry group. A nondegenerate k -space of specified type has orbit size

$$\frac{21}{128}q^{k(e-k)} \leq \frac{|D(U)|}{|D(W)||D(W^\perp)|} \leq 2q^{k(e-k)}. \quad (9)$$

For symplectic spaces this follows from the ψ bounds; for orthogonal spaces it follows from the η bounds above. Empty or full spaces have count one and satisfy the same estimates. There are at most two orthogonal types. The number $T(e, k)$ of totally singular k -spaces is

$$T(e, k) = \prod_{j=0}^{k-1} \frac{N_{e-2j}}{q^{k-j} - 1}, \quad N_d = \begin{cases} q^d - 1 & \text{Sp,} \\ q^{d-1} - 1 & \text{O, } d \text{ odd,} \\ (q^{m-1} + \varepsilon)(q^m - \varepsilon) & \text{O, } d = 2m. \end{cases}$$

Indeed choose an ordered singular basis successively in its orthogonal quotient, multiplying by q^j possible lifts at step j , and divide by the ordered-basis count of a k -space. This yields the displayed product. For feasible k it implies

$$\frac{1}{2}q^{F_\sigma(e,k)} \leq T(e, k) \leq 8q^{F_\sigma(e,k)}, \quad F_\sigma(e, k) = ke - (3k^2 + \sigma k)/2, \quad (10)$$

where $\sigma = -1$ for Sp, $+1$ for O. The denominator product $\prod_{i=1}^k (1 - q^{-i})$ is greater than $1/2$; for $q = 3$ this follows from $(1 - 1/3)(1 - \sum_{i \geq 2} 3^{-i}) > 1/2$, and larger q improves it. The negative numerator factors have product at least $1/2$; positive factors have product at most $2 \exp(1/(q-1)) < 4$. These estimates include both maximal-singular families in the split even orthogonal space, using their combined count in the product formula.

If a strong involution x has eigenspace dimensions $a, b \geq e/3$, every invariant subspace splits into intersections of dimensions i, j with $i + j = k$. For nondegenerate subspaces the invariant count is at most $16(k+1)q^{i(a-i)+j(b-j)}$, taking the maximum over i . The exponent loss relative to $k(e-k)$ is

$$ib + ja - 2ij \geq ek/12 \quad (k \leq e/2).$$

To verify it, with $i + j = k$ and $a, b \geq e/3$, the loss is at least $ek/3 - k^2/2 \geq ek/12$. For totally singular spaces the analogous invariant count is at most $64(k+1)$ times the maximum $q^{F_\sigma(a,i)+F_\sigma(b,j)}$. Now $i \leq a/2$, $j \leq b/2$, so $ib + ja \geq 4ij$; also $ib + ja \geq ek/3$. The loss is $ib + ja - 3ij \geq (ib + ja)/4 \geq ek/12$. Dividing by (9) or (10), for either kind of fixed subspace we obtain the uniform fixed-space probability

$$128(k+1)q^{-ek/12}. \quad (11)$$

In the orthogonal case the full O-class of a strong involution in Ω is one Ω -class, by the reflection argument in Section 2. Thus the probability is indeed the full-isometry class probability, even if the subspace orbit itself splits under Ω .

Every reducible subgroup fixes either a nonzero totally singular subspace (the radical of an invariant degenerate subspace), or a nondegenerate subspace with dimension at most $e/2$, taking an orthogonal complement if necessary. For each k the relevant subspaces number at most $12q^{ek}$ by (9)–(10). For $e \geq 384$, $128(k+1) \leq 256^k \leq 3^{8k} \leq q^{ek/48}$. For 192 independent prescribed classes, the union bound therefore gives reducibility probability at most

$$12 \sum_{k \geq 1} q^{ek} q^{-192ek/16} < 13q^{-11e} < \frac{1}{2}q^{-e}.$$

Put $S = J/Z(J)$. In the dimensions under consideration J is perfect, S is nonabelian simple and $|Z(J)| \leq 2$; the exact standard exceptions are excluded by large dimension [10, Theorems 8.7–8.8, 11.47–11.48]. A strong natural involution has class size at least $(21/128)q^{ab}$, with $ab \geq 2e^2/9$, by (9). A projective class fibre has size at most two: a conjugator fixes the projective element precisely when it sends the lift to that lift times a central scalar. Hence its image has class size at least $(21/256)q^{2e^2/9} \geq q^{e^2/5}$ for $e \geq 16$.

For any non-subspace maximal subgroup M of S , (8) has exponent at most $-1/3$ for $e \geq 16$. Class membership therefore has probability at most $q^{-e^2/15}$. This follows also directly by counting conjugators: the proportion of a class in M equals the fixed-point ratio on S/M . The LPS bound and $|S| < q^{e^2}$ bound the probability that 192 choices lie in any such maximal subgroup by

$$Cq^{e^2}q^{-192e^2/15} = Cq^{-59e^2/5}.$$

Choose

$$e_0 = \left\lceil \max\{384, \sqrt{\log_3(2 \max(1, C))}\} \right\rceil.$$

Then $C \leq q^{e^2}/2$, and the last bound is less than $q^{-e}/2$. Combining the subspace and non-subspace cases, the images generate S with probability at least $1 - q^{-e}$. If their natural subgroup is K , then $KZ(J) = J$ implies $J = J' = (KZ(J))' = K' \leq K$, which lifts generation to the full natural group. This is why the theorem generates the central covers, not merely projective images. $\square$

6 From marginal outputs to the actual centraliser

Let $a = \dim A \leq b = \dim B$, and set

$$D = D_A \times D_B, \quad L = L_A \times L_B,$$

where $D_U = L_U = \text{Sp}(U)$ in the symplectic case, and $D_U = \text{O}(U)$, $L_U = \Omega(U)$ in the orthogonal case. Here a, b are natural dimensions, unlike the half-dimensions in the symplectic counting section. Write $C = C_G(t)$. It is exactly D for Sp or full O , the total-determinant kernel in D for SO , or the total-determinant and total-spinor kernel for Ω . In large dimension L is perfect, $L \leq C$ and C/L is abelian. Consequently

$$C' = C'' = L : \tag{12}$$

indeed $C' \leq L$ and $L = L' \leq C'$, and taking a further derived subgroup gives the second equality.

The law of z is invariant under C -conjugacy, since replacing g by gc conjugates the output by c . For every involution z centralising t , its four joint (t, z) -eigenspaces are nondegenerate and one has dimension at least $n/4$. When $n/4 \geq 3$, reflections within this space realise both spinor values and determinant -1 . They belong to $C_D(z)$ and map onto all of D/C . Thus

$$D = CC_D(z), \quad z^C = z^D = z_A^{D_A} \times z_B^{D_B}. \tag{13}$$

For Sp this is immediate because $C = D$. Conditioned on a pair of component classes, the two components are therefore independent uniform choices. Conditioning on strength, or on membership in L , preserves this conclusion, since these conditions are class properties.

Call an output admissible if it lies in L . In Sp all outputs are admissible; in the orthogonal case Lemma 4.3 gives enough such outputs without asserting this for every output. Let $\kappa = 1/40000$ in the symplectic case and $1/10000000$ in the orthogonal case. For each target eigenspace separately, an output is admissible and strong there with probability at least $\kappa/\log n$. Given this event and its actual component class, it is uniform in that strong class of L_U . In the orthogonal case the D_U and L_U strong classes coincide by the earlier reflection argument.

Lemma 6.1. *For U of sufficiently large dimension, the conjugation map $D_U \rightarrow \text{Aut}(L_U/Z(L_U))$ has kernel of order at most two.*

Proof. If h acts trivially on the quotient, write $h x h^{-1} = x f(x)$ with $f(x) \in Z(L_U)$. Centrality makes f a homomorphism from the perfect group L_U to an abelian group, hence trivial. Thus h centralises L_U on its natural module. In the symplectic case the image of $T_u - 1$ for a nontrivial transvection is the line $\langle u \rangle$. Commuting with every transvection forces h to preserve every line, hence to be scalar.

Here is the analogous elementary verification for $\Omega(U)$, to avoid an assumed representation-theoretic centraliser. For a singular u and $v \in u^\perp$, the Siegel isometry

$$\rho_{u,v}(x) = x + \beta(x, u)v - \beta(x, v)u - Q(v)\beta(x, u)u$$

belongs to $\Omega(U)$ [10, Theorem 11.24]. The common fixed space of these transformations as v varies is exactly $\langle u \rangle$: modulo that line, if $\beta(x, u) \neq 0$ the v term is nonzero for some v ; otherwise the fixed condition for all v says $x \in (u^\perp)^\perp = \langle u \rangle$. Thus h preserves each singular line. In a Witt basis e_i, f_i , at least two hyperbolic pairs exist. The singular lines $e_i + e_j$ and $e_i + f_j$ for $i \neq j$ force all scalars on these basis vectors to equal one common c . For an anisotropic vector w perpendicular to the hyperbolic part, the two singular vectors $e_1 + w - Q(w)f_1$ and $e_1 - w - Q(w)f_1$ span distinct lines. Their images are scalar multiples of themselves; their sum is $2(e_1 - Q(w)f_1)$, already multiplied by c . Independence forces both multiples to be c , whence $h(w) = cw$. Therefore $h = c1$ on all of U . An isometry scalar is ± 1 , proving the claim in both cases. $\square$

We use Goursat's elementary subgroup lemma in a form that includes every abstract quotient graph, without assumptions about equality of dimensions or orthogonal types. If $K \leq D$ projects onto groups containing L_A, L_B , then $K' \leq L$ projects onto both perfect factors. Write $S_U = L_U/Z(L_U)$. Its image in $S_A \times S_B$ is either the full product or a graph of an isomorphism $\phi : S_A \rightarrow S_B$. Indeed the kernels of the two projections are normal in the simple factors; they are either trivial or the whole factor, giving exactly these alternatives. If the image is full, $K'Z(L) = L$, and perfectness gives $L = (K'Z(L))' \leq K'$. If it is a graph and an extra admissible output z still does not produce L , then the derived subgroup of $\langle K, z \rangle$ has a graph image containing the previous graph. These graphs have equal orders, so it is the same graph. Since that derived subgroup is normal in $\langle K, z \rangle$, the actions must satisfy

$$a_B(z_B) = \phi a_A(z_A) \phi^{-1}, \tag{14}$$

where a_U denotes conjugation on S_U . By Lemma 6.1, fixing z_A leaves at most two possible z_B in the full group satisfying (14). There is no union over possible ϕ ; it is fixed by K before the new output is drawn. A strong B -class has size at least $(21/128)q^{2b^2/9}$, so, conditioned on a strong B -component class and any A -component class, the probability of this obstruction is at most

$$13q^{-2b^2/9}. \tag{15}$$

This handles all quotient isomorphisms and does not lift a graph isomorphism to the central covers.

Fix $0 < \eta < 1$. Divide independent samples into 385 disjoint blocks of length

$$\ell = \left\lceil \kappa^{-1} \log n \log(385/\eta) \right\rceil.$$

Use the first 192 blocks to select the first admissible output strong on A , the next 192 for B , and the last for one more such B -output. Each block fails with probability at most $(1 - \kappa/\log n)^\ell \leq \eta/385$,

so all succeed with probability at least $1 - \eta$. This selection is a proof device; the algorithm retains all outputs and need not identify success.

For clarity, conditioning on success of a length- ℓ block does not bias the selected law: if E is its target event with probability p and W is any subset of E , the probability that the first success belongs to W is

$$\sum_{j=1}^{\ell} (1-p)^{j-1} \mathbb{P}(W) = \frac{1 - (1-p)^{\ell}}{p} \mathbb{P}(W).$$

Division by the success probability gives exactly $\mathbb{P}(W \mid E)$. Conditioning on all blocks succeeding preserves independence between blocks, since both their samples and their success events are independent. Conditional on the 384 prescribed actual component classes, Theorem 5.1 gives projection-generation failure at most $q^{-a} + q^{-b}$. Conditional on any successful first 384 blocks and their generated subgroup, the last block is independent and (15) eliminates the remaining graph. Thus the subgroup generated by all 385 ℓ outputs fails to contain $L = C''$ with probability at most

$$\eta + q^{-a} + q^{-b} + 13q^{-2b^2/9}. \quad (16)$$

Take $n \geq \max\{49152, 3e_0\}$ in the symplectic case or $n \geq \max\{98304, 3e_0\}$ otherwise, increasing these absolute thresholds if needed. With $\eta = 1/20$, the last three terms sum to less than $1/20$, so one trial fails with probability less than $1/10$. Repeat $\lceil \log(1/\delta)/\log 10 \rceil$ independent trials and retain their combined outputs. Failure of the combined group implies failure of every trial, and hence has probability at most δ . Their total sample count has the order stated in Theorem 1.1.

7 Scope, counterexamples, and reproducibility

The sufficiently-large-dimension qualification is substantive. In $\mathrm{Sp}_4(q)$ take t with a negative plane and a positive plane. Every $z(g)$ centralises t , and each restriction lies in $\mathrm{Sp}_2(q)$. An involution in $\mathrm{Sp}_2(q) = \mathrm{SL}_2(q)$ in odd characteristic is -1 (or identity if order divides two); neither is strong on a plane. Thus both marginal probabilities are zero, despite t itself being strong.

Nor do the marginal theorems assert simultaneous strength. In fact for any conjugate involutions t, s in odd characteristic, if $z = \mathrm{inv}(ts)$ then

$$\dim(E_-(z) \cap E_-(t)) = \dim(E_-(z) \cap E_+(t)). \quad (17)$$

Here is a proof allowing nonsemisimple products. Write $y = ts = y_2 y_o$ for its commuting 2-part and odd-order part. The involutions t, s invert y and both parts. If the order of y_2 is at least four, $E_-(z)$ contains only the primary y_2 -eigenvalues of maximal 2-power order, none equal to ± 1 ; t exchanges reciprocal primary spaces, so has trace zero there. If y_2 has order two, decompose into its $+1, -1$ spaces. On the first $s = ty_o$ is conjugate to t , and on the second $s = -ty_o$ is conjugate to $-t$, using an odd-order square root of y_o and the inversion relation. Thus the difference of traces of s and t is minus twice the trace of t on $E_-(y_2)$. Conjugacy of s, t forces that trace to be zero. Traces here may be read as ordinary integer differences of the two eigenspace dimensions, using the direct primary decompositions, so no modular-trace inference is involved. If $y_2 = 1, z = 1$ and the equality is immediate. This proves (17). For $\dim A = 2a, \dim B = 4a$ in a symplectic space, simultaneous strength would force the common negative dimension to equal $4a/3$. It is impossible whenever $3 \nmid a$, in arbitrarily large dimensions. Separate blocks in Section 6 are therefore essential.

The result is for independent exactly uniform samples and counts those samples. It asserts no total field-operation bound, no deterministic certificate for detecting completion, no all- n even-branch theorem, no characteristic-two case, and no extension to similitudes, projective involutions,

or order-four lifts. Amplification depends on the specified confidence; a fixed constant multiplying $\log n$ is not asserted to give error tending to zero. These distinctions follow the asymptotic and fixed-confidence conventions of [6, Section 2.1].

The source package contains exact standard-library finite diagnostics, expected results, dependency statements, and a deterministic offline packaging builder. The checks independently enumerate small graph charts, all four polynomial sign sectors over $\mathbb{F}_3$, boundary involutions and a weighted conditional-block model, and reject deliberate perturbations. They test interfaces and constants; finite enumeration is not a proof of the universal theorem. Earlier independent review calculations are attributed in the provenance notes and are not described as new mathematical results. The proofs above, together with the precisely identified standard structural inputs, supply the universal argument.

AI involvement and review status. AI tools were extensively involved in the mathematical research, proof development, computational verification, manuscript preparation, and adversarial auditing. This is an unrefereed preprint and has not undergone formal independent human peer review. Automated or AI-based checks are not human peer review.

References

- [1] J. N. Bray, An improved method for generating the centralizer of an involution, *Arch. Math.* 74 (2000), 241–245. <https://doi.org/10.1007/s000130050437>.
- [2] T. C. Burness, Fixed point ratios in actions of finite classical groups, I, *J. Algebra* 309 (2007), 69–79. <https://doi.org/10.1016/j.jalgebra.2006.05.024>.
- [3] J. D. Dixon, C. E. Praeger and À. Seress, Strong involutions in finite special linear groups of odd characteristic, *J. Algebra* 498 (2018), 413–447. <https://doi.org/10.1016/j.jalgebra.2017.11.047>.
- [4] S. P. Glasby, A. C. Niemeyer and C. E. Praeger, The probability that two elements with large 1-eigenspaces generate a classical group, arXiv:2603.22638v2 (2026). <https://arxiv.org/abs/2603.22638v2>.
- [5] S. P. Glasby, C. E. Praeger and C. M. Roney-Dougal, Involution centralisers in finite unitary groups of odd characteristic, *J. Algebra* 545 (2020), 245–299. <https://doi.org/10.1016/j.jalgebra.2019.09.009>; arXiv:1812.01362v2.
- [6] C. R. Leedham-Green and E. A. O’Brien, Constructive recognition of classical groups in odd characteristic, *J. Algebra* 322 (2009), 833–881. <https://doi.org/10.1016/j.jalgebra.2009.04.028>.
- [7] M. W. Liebeck, L. Pyber and A. Shalev, On a conjecture of G. E. Wall, *J. Algebra* 317 (2007), 184–197. <https://doi.org/10.1016/j.jalgebra.2006.10.047>.
- [8] C. E. Praeger, Finding strong involutions in finite classical groups in odd characteristic, in *Computational Group Theory*, Oberwolfach Reports 37/2016, 2160–2161. <https://ems.press/content/serial-article-files/46642>.
- [9] C. E. Praeger and À. Seress, Probabilistic generation of finite classical groups in odd characteristic by involutions, *J. Group Theory* 14 (2011), 521–545. <https://doi.org/10.1515/JGT.2010.061>.
- [10] D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann, 1992; author’s corrected electronic edition. <https://www.maths.usyd.edu.au/u/don/papers/gcg.pdf>.