Computation of centralizers of involutions

Ákos Seress

April 2011

Centralizers of involutions

Important in theory (e.g. classification of finite simple groups) and in computations

Centralizers of involutions

Important in theory (e.g. classification of finite simple groups) and in computations

Matrix recognition project

Given $G = \langle X \rangle$, find $|G|$, composition series, set up data structure for constructive membership

Structural divide-and-conquer: find homomorphisms, divide task into smaller subproblems on image and kernel
Reduction bottoms out at simple groups

Leads to theoretical problems about simple groups, not addressed by traditional group theory

Some problems leading to centralizers of involutions computations

Given a Lie-type simple group $G = \langle X \rangle$ and its characteristic, determine the isomorphism type of G

Random sampling in G, primitive prime divisor properties of sample element orders distinguish different types (Babai, Kantor, Pálfy, Seress) except $\mathrm{PSp}(2n, q)$ and $\mathrm{P\Omega}(2n+1, q)$ in odd characteristic

Some problems leading to centralizers of involutions computations

Given a Lie-type simple group $G = \langle X \rangle$ and its characteristic, determine the isomorphism type of G

Random sampling in G, primitive prime divisor properties of sample element orders distinguish different types (Babai, Kantor, Pálfy, Seress) except $\mathrm{PSp}(2n, q)$ and $\mathrm{P\Omega}(2n+1, q)$ in odd characteristic

There exists $t \in G = \mathrm{P\Omega}(2n+1, q)$, $t^2 = 1$, the isomorphism type of $C_G(t)$ cannot occur as a subgroup in $\mathrm{PSp}(2n, q)$ (Altseimer, Borovik)

Some problems leading to centralizers of involutions computations

Given a Lie-type simple group $G = \langle X \rangle$ and its characteristic, determine the isomorphism type of G

Random sampling in G, primitive prime divisor properties of sample element orders distinguish different types (Babai, Kantor, Pálfy, Seress) except $\mathrm{PSp}(2n, q)$ and $\mathrm{P\Omega}(2n+1, q)$ in odd characteristic

There exists $t \in G = \mathrm{P\Omega}(2n+1, q)$, $t^2 = 1$, the isomorphism type of $C_G(t)$ cannot occur as a subgroup in $\mathrm{PSp}(2n, q)$ (Altseimer, Borovik)

Given a simple group G of Lie type, its characteristic can be computed, utilizing some centralizer of involution computations (Liebeck, O'Brien)

Construction of Curtis-Tits system (Yalcinkaya)

Given G with $G/O_p(G)$ simple Lie-type of characteristic $p > 2$, find generators for $O_p(G)$ (Yalcinkaya, Parker, Wilson)

Construction of Curtis-Tits system (Yalcinkaya)

Given G with $G/O_p(G)$ simple Lie-type of characteristic $p > 2$, find generators for $O_p(G)$ (Yalcinkaya, Parker, Wilson)

Constructive recognition of classical groups of odd characteristic, in natural representation
Leedham-Green, O'Brien: find $x \in G$, $x^2 = 1$, eigenspaces of x roughly the same dimension
$C_G(x)$ is a small extension of the direct product of two smaller groups of the same type as G (acting on the (± 1)-eigenspaces of x)

Construction of centralizer of involutions: Bray's trick

$x \in G$, $x^2 = 1$, define $\zeta : G \to C_G(x)$

Take random conjugate x^g in G, $D = \langle x, x^g \rangle \cong D_{2m}$

$y = x \cdot x^g$ generates a cyclic subgroup $\cong C_m$

Construction of centralizer of involutions: Bray's trick

$x \in G$, $x^2 = 1$, define $\zeta : G \to C_G(x)$

Take random conjugate x^g in G, $D = \langle x, x^g \rangle \cong D_{2m}$

$y = x \cdot x^g$ generates a cyclic subgroup $\cong C_m$

Case 1 g even type: m even

$y^{m/2} \in Z(D)$, so $y^{m/2}$ centralizes $x \in D$, $\zeta(g) := y^{m/2} \in C_G(x)$

Construction of centralizer of involutions: Bray's trick

$x \in G$, $x^2 = 1$, define $\zeta : G \to C_G(x)$

Take random conjugate x^g in G, $D = \langle x, x^g \rangle \cong D_{2m}$

$y = x \cdot x^g$ generates a cyclic subgroup $\cong C_m$

Case 1 g even type: m even

$y^{m/2} \in Z(D)$, so $y^{m/2}$ centralizes $x \in D$, $\zeta(g) := y^{m/2} \in C_G(x)$

Case 2 g odd type: m odd

$$x^{y^{\frac{m+1}{2}}} = (xx^g)^{\frac{m-1}{2}} x (xx^g)^{\frac{m+1}{2}} =$$

$$xg^{-1}xg \cdots xg^{-1}xg \cdot \underline{x} \cdot xg^{-1}xg \cdots xg^{-1}xg = g^{-1}xg = x^g$$

$\zeta(g) := y^{\frac{m+1}{2}} g^{-1} \in C_G(x)$

Construction of centralizer of involutions: Bray's trick

$x \in G$, $x^2 = 1$, define $\zeta : G \to C_G(x)$

Take random conjugate x^g in G, $D = \langle x, x^g \rangle \cong D_{2m}$

$y = x \cdot x^g$ generates a cyclic subgroup $\cong C_m$

Case 1 g even type: m even

$y^{m/2} \in Z(D)$, so $y^{m/2}$ centralizes $x \in D$, $\zeta(g) := y^{m/2} \in C_G(x)$

Case 2 g odd type: m odd

$$x^{y^{\frac{m+1}{2}}} = (xx^g)^{\frac{m-1}{2}} x (xx^g)^{\frac{m+1}{2}} =$$

$$xg^{-1}xg \cdots xg^{-1}xg \cdot \underline{x} \cdot xg^{-1}xg \cdots xg^{-1}xg = g^{-1}xg = x^g$$

$\zeta(g) := y^{\frac{m+1}{2}} g^{-1} \in C_G(x)$

For $c \in C_G(x)$, $x^{cg} = x^g$, so g and cg have the same type

If g is odd type: $y^{\frac{m+1}{2}}(cg)^{-1} = y^{\frac{m+1}{2}} g^{-1} c^{-1}$

As cg runs through the coset $C_G(x) \cdot g$, $y^{\frac{m+1}{2}} g^{-1} c^{-1}$ runs through $C_G(x)$

Odd-type method gives uniformly distributed elements in $C_G(x)$

Theorem (C. Parker, R. Wilson)

G is simple group of Lie type of rank n, $x \in G$, $x^2 = 1$
Random $g \in G$ is of odd type with probability $\Omega(1/n^c)$,
$c \in \{1, 2, 3\}$

Theorem (C. Parker, R. Wilson)

G is simple group of Lie type of rank n, $x \in G$, $x^2 = 1$
Random $g \in G$ is of odd type with probability $\Omega(1/n^c)$,
$c \in \{1, 2, 3\}$

Enough for polynomial-time construction of centralizers

Most $g \in G$ are of even type
Can we use them to generate $C_G(x)$?

Theorem (C. Parker, R. Wilson)

G is simple group of Lie type of rank n, $x \in G$, $x^2 = 1$
Random $g \in G$ is of odd type with probability $\Omega(1/n^c)$,
$c \in \{1, 2, 3\}$

Enough for polynomial-time construction of centralizers

Most $g \in G$ are of even type
Can we use them to generate $C_G(x)$?

For $c \in C_G(x)$, $xx^{gc} = xc^{-1}g^{-1}x^{-1}gc = (xx^g)^c$, so g and gc have the same type
If g is even type: $(xx^g)^{m/2}$ and $(xx^{gc})^{m/2}$ are conjugate by c
As gc runs through the coset $g \cdot C_G(x)$, $(xx^{gc})^{m/2}$ runs through the conjugacy class of $(xx^g)^{m/2}$ in $C_G(x)$
Even-type method gives uniformly distributed elements in a conjugacy class of involutions in $C_G(x)$

Side remark about left and right cosets of $C = C_G(x)$

$x \in G$, $x^2 = 1$, $C = C_G(x)$

$$G = Cg_1C \cup \cdots \cup Cg_kC$$

double coset decomposition

For each double coset CgC, either all elements of CgC are even type, or all of them are odd type

If CgC is of odd type then $\zeta(CgC)$ covers C evenly

If CgC is of even type then $\zeta(CgC)$ covers a conjugacy class of involutions in C evenly

Setup

$G = G(n, q)$ classical quasisimple of dimension n, defined over $\mathrm{GF}(q)$, q odd, acting on natural module V

$x \in G$, $x^2 = 1$, $V = E_1(x) \oplus E_{-1}(x)$

$E_{\pm 1}(x)$: ± 1-eigenspaces of x

Setup

$G = G(n, q)$ classical quasisimple of dimension n, defined over $\mathrm{GF}(q)$, q odd, acting on natural module V

$x \in G$, $x^2 = 1$, $V = E_1(x) \oplus E_{-1}(x)$

$E_{\pm 1}(x)$: ± 1-eigenspaces of x

$E_1(x), E_{-1}(x)$ perpendicular, nondegenerate subspaces

$C_G(x)$ is direct product of same type classicals on $E_1(x), E_{-1}(x)$ (plus small extensions)

Setup

$G = G(n, q)$ classical quasisimple of dimension n, defined over $\mathrm{GF}(q)$, q odd, acting on natural module V
$x \in G$, $x^2 = 1$, $V = E_1(x) \oplus E_{-1}(x)$
$E_{\pm 1}(x)$: ± 1-eigenspaces of x
$E_1(x), E_{-1}(x)$ perpendicular, nondegenerate subspaces
$C_G(x)$ is direct product of same type classicals on $E_1(x), E_{-1}(x)$ (plus small extensions)

x strong involution: $n/3 \leq \dim(E_{-1}(x)) \leq 2n/3$
x (α, β)-balanced: $\alpha n \leq \dim(E_{-1}(x)) \leq \beta n$
$0 < \alpha < 1/2 < \beta < 1$

The grand plan

(joint work with Cheryl Praeger)

Given a strong involution $x \in G(n, q)$, q odd

(1) For many $g \in G$ of even type, $\zeta(g) = (xx^g)^{m/2}$ projects as (α, β)-balanced involution both on $E_1(x)$ and $E_{-1}(x)$

(2) Only few (α, β)-balanced involutions, that are uniformly distributed in their conjugacy class, are needed to generate a classical quasisimple group

Given a sequence $(\mathcal{C}_1, \ldots, \mathcal{C}_k)$ of conjugacy classes of (α, β)-balanced involutions in $G(n, q)$,
$(g_1, \ldots, g_k)$ is a class-random sequence
if g_i is a uniformly distributed random element of $\mathcal{C}_i$, for $1 \leq i \leq k$.

Theorem (Praeger, Seress)

There exists a function $c(\alpha, \beta)$, defined for $0 < \alpha < 1/2 < \beta < 1$:
If $(g_1, \ldots, g_k)$ is a class-random sequence for some sequence of conjugacy classes of (α, β)-balanced involutions, $k \geq c(\alpha, \beta)$, then $\langle g_1, \ldots, g_k \rangle = G(n, q)$ with probability at least $1 - q^{-n}$.

If $\langle g_1, \ldots, g_k \rangle \neq G(n,q)$ then $g_1, \ldots, g_k \in M$ for some maximal $M < G$

$$\mathrm{Prob}(g_1, \ldots, g_k \in M) \leq \prod_{i=1}^{k} \frac{|M \cap \mathcal{C}_i|}{|\mathcal{C}_i|}$$

enough: for each fixed sequence $(\mathcal{C}_1, \ldots, \mathcal{C}_k)$,

$$\sum_{M} \prod_{i=1}^{k} \frac{|M \cap \mathcal{C}_i|}{|\mathcal{C}_i|} < q^{-n}$$

For each conjugacy class $\mathcal{C}$ of balanced involutions, and each maximal subgroup $M < G(n,q)$, estimate $\frac{|M \cap \mathcal{C}|}{|\mathcal{C}|}$
fixed-point ratio estimates

For balanced involution classes $\mathcal{C}$, $|\mathcal{C}| = q^{\Theta(n^2)}$

Maximal subgroups in Aschbacher classes $\mathbf{C}_1, \ldots, \mathbf{C}_9$

Theorem (Burness)

If $M \in \mathbf{C}_i$ for some $2 \leq i \leq 8$ then

$$\frac{|M \cap \mathcal{C}|}{|\mathcal{C}|} < |\mathcal{C}|^{-\frac{1}{2}+O(1/n)} \qquad (*)$$

For $M \in \mathbf{C}_9$, $|M|$ is small, $\frac{|M\cap\mathcal{C}|}{|\mathcal{C}|} < \frac{|M|}{|\mathcal{C}|}$ suffices
Estimates for number of M in each class $\mathbf{C}_i$ are known, implying

$$\sum_{M\in\mathbf{C}_i, 2\leq i\leq 9} < q^{-cn^2}$$

Nasty case: $M \in \mathbf{C}_1$
The estimate $(*)$ does not hold!

M fixes an ℓ-dimensional subspace L
$x \in \mathcal{C}$, $\dim(E_{-1}(x)) = r$, $\dim(E_{-1}(x) \cap L) = s$

$$|M \cap \mathcal{C}| = \sum_s f(n, \ell, r, s, q) = q^{g(n,\ell,r,q)}$$

Nasty case: $M \in \mathbf{C}_1$
The estimate $(*)$ does not hold!

M fixes an ℓ-dimensional subspace L
$x \in \mathcal{C}$, $\dim(E_{-1}(x)) = r$, $\dim(E_{-1}(x) \cap L) = s$

$$|M \cap \mathcal{C}| = \sum_s f(n, \ell, r, s, q) = q^{g(n,\ell,r,q)}$$

For fixed $q, \ell, \frac{r}{n}$, and $n \to \infty$: $g(n, \ell, r, q) \sim c_1 n^2$
$0 < c_1 = c_1(q, \ell, \frac{r}{n})$, explicitly computed

Nasty case: $M \in \mathbf{C}_1$
The estimate $(*)$ does not hold!

M fixes an ℓ-dimensional subspace L
$x \in \mathcal{C}$, $\dim(E_{-1}(x)) = r$, $\dim(E_{-1}(x) \cap L) = s$

$$|M \cap \mathcal{C}| = \sum_s f(n, \ell, r, s, q) = q^{g(n,\ell,r,q)}$$

For fixed $q, \ell, \frac{r}{n}$, and $n \to \infty$: $g(n, \ell, r, q) \sim c_1 n^2$
$0 < c_1 = c_1(q, \ell, \frac{r}{n})$, explicitly computed

$|\mathcal{C}| = q^{h(n,r,q)}$, $h(n, r, q) \sim c_2 n^2$
$0 < c_2 = c_2(q, \frac{r}{n})$

Nasty case: $M \in \mathbf{C}_1$
The estimate $(*)$ does not hold!

M fixes an ℓ-dimensional subspace L
$x \in \mathcal{C}$, $\dim(E_{-1}(x)) = r$, $\dim(E_{-1}(x) \cap L) = s$

$$|M \cap \mathcal{C}| = \sum_s f(n, \ell, r, s, q) = q^{g(n,\ell,r,q)}$$

For fixed $q, \ell, \frac{r}{n}$, and $n \to \infty$: $g(n, \ell, r, q) \sim c_1 n^2$
$0 < c_1 = c_1(q, \ell, \frac{r}{n})$, explicitly computed

$|\mathcal{C}| = q^{h(n,r,q)}$, $h(n, r, q) \sim c_2 n^2$
$0 < c_2 = c_2(q, \frac{r}{n})$

There are cases when $c_1 = c_2$

$\frac{|M \cap \mathcal{C}|}{|\mathcal{C}|} = q^{o(n^2)}$

Nasty case: $M \in \mathbf{C}_1$
The estimate $(*)$ does not hold!

M fixes an ℓ-dimensional subspace L
$x \in \mathcal{C}$, $\dim(E_{-1}(x)) = r$, $\dim(E_{-1}(x) \cap L) = s$

$$|M \cap \mathcal{C}| = \sum_s f(n, \ell, r, s, q) = q^{g(n,\ell,r,q)}$$

For fixed $q, \ell, \frac{r}{n}$, and $n \to \infty$: $g(n, \ell, r, q) \sim c_1 n^2$
$0 < c_1 = c_1(q, \ell, \frac{r}{n})$, explicitly computed

$|\mathcal{C}| = q^{h(n,r,q)}$, $h(n, r, q) \sim c_2 n^2$
$0 < c_2 = c_2(q, \frac{r}{n})$

There are cases when $c_1 = c_2$

$\frac{|M \cap \mathcal{C}|}{|\mathcal{C}|} = q^{o(n^2)}$
$g(n, \ell, r, q) = c_1 n^2 + \mathrm{Error}_1$
$|\mathcal{C}| = c_2 n^2 + \mathrm{Error}_2$ need to estimate error terms

Task (1), slightly revisited

$x \in G(n,q)$, $x^2 = 1$, $C = C_G(x)$, $\mathcal{C} = x^G$

(1) For many $x' \in \mathcal{C}$, $y = xx'$ has even order m, and $y^{m/2}$ projects as (α, β)-balanced involution both on $E_1(x)$ and $E_{-1}(x)$

Currently, complete solution only in the linear case, so suppose $G = \mathrm{GL}(V) \cong \mathrm{GL}(n,q)$

Task (1), slightly revisited

$x \in G(n,q)$, $x^2 = 1$, $C = C_G(x)$, $\mathcal{C} = x^G$

(1) For many $x' \in \mathcal{C}$, $y = xx'$ has even order m, and $y^{m/2}$ projects as (α, β)-balanced involution both on $E_1(x)$ and $E_{-1}(x)$

Currently, complete solution only in the linear case, so suppose $G = \mathrm{GL}(V) \cong \mathrm{GL}(n,q)$

Introduce restrictions on x' so that still there are many x' satisfying the restrictions but $y = xx'$ becomes more manageable

$y \in \mathrm{GL}(n,q)$ regular semisimple: characteristic polynomial $c_y(t)$ has no repeated factors and y is semisimple

$\mathcal{C}(V) = \{x \in G \mid x^2 = 1, \dim(E_{-1}(x)) = n/2\}$

$y \in \mathrm{GL}(n,q)$ regular semisimple: characteristic polynomial $c_y(t)$ has no repeated factors and y is semisimple

$\mathcal{C}(V) = \{x \in G \mid x^2 = 1, \dim(E_{-1}(x)) = n/2\}$

First subtask: understand $x, x' \in \mathcal{C}(V)$, $y = xx'$ regular semisimple
$y^x = x \cdot xx' \cdot x = x'x = y^{-1}$,

y is self-conjugate

bijection between pairs $(y, x) \mapsto (x, x')$:

(i) y self-conjugate, regular semisimple, $x \in \mathcal{C}(V)$ inverts y

(ii) $x, x' \in \mathcal{C}(V)$, $y = xx'$ regular semisimple

For any monic polynomial
$h(t) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + a_0$ with $a_0 \neq 0$,
the conjugate polynomial is
$h^*(t) = (a_0 t^d + a_1 t^{d-1} + \ldots + a_{d-1}t + 1)a_0^{-1}$

Fact: For $g \in \mathrm{GL}(n, q)$, $c_{g^{-1}}(t) = c_g^*(t)$

For any monic polynomial
$h(t) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + a_0$ with $a_0 \neq 0$,
the conjugate polynomial is
$h^*(t) = (a_0 t^d + a_1 t^{d-1} + \ldots + a_{d-1}t + 1)a_0^{-1}$

Fact: For $g \in \mathrm{GL}(n, q)$, $c_{g^{-1}}(t) = c_g^*(t)$

In particular, $c_{y^{-1}}(t) = c_y^*(t)$

$c_y(t) = \prod_i h_i(t)$, no repeated factors
For simplicity, assume $t - 1$, $t + 1$ not factors of $c_y(t)$
$c_{y^{-1}}(t) = c_y^*(t) = \prod_i h_i^*(t) = c_y(t) = \prod_i h_i(t)$

$$c_y(t) = \prod_{i=1}^{r} f_i(t) \prod_{j=1}^{s} g_j(t) g_j^*(t)$$

$f_i^*(t) = f_i(t)$, $\deg f_i$ even

$$V = \bigoplus_{i=1}^{r} V_i \oplus \bigoplus_{j=1}^{s} W_j$$

$y_i = y\,|_{V_i}$, $y_j' = y\,|_{W_j}$
$c_{y_i}(t) = f_i(t)$, $c_{y_j'}(t) = g_j(t) g_j^*(t)$

$C_{\mathrm{GL}(V_i)}y_i \cong C_{q^{\deg f_i}-1}$ (Singer cycle)
number of inverting involutions is $q^{\deg f_i/2}+1$, all of them in $\mathcal{C}(V_i)$

$C_{\mathrm{GL}(W_j)}y_j' \cong C_{q^{\deg g_j}-1} \times C_{q^{\deg g_j}-1}$ (product of two Singer cycles)
number of inverting involutions is $q^{\deg g_j}-1$, all of them in $\mathcal{C}(W_j)$

$C_{\mathrm{GL}(V_i)}y_i \cong C_{q^{\deg f_i}-1}$ (Singer cycle)
number of inverting involutions is $q^{\deg f_i/2}+1$, all of them in $\mathcal{C}(V_i)$

$C_{\mathrm{GL}(W_j)}y'_j \cong C_{q^{\deg g_j}-1} \times C_{q^{\deg g_j}-1}$ (product of two Singer cycles)
number of inverting involutions is $q^{\deg g_j}-1$, all of them in $\mathcal{C}(W_j)$

Putting together, using also that in $\mathrm{GL}(V)$, y, z semisimple are conjugate if and only if $c_y(t) = c_z(t)$:
$\#(y, x)$, y with fixed characteristic polynomial $\prod f_i \prod g_j g_j^*$, $x \in \mathcal{C}(V)$ inverting involution is

$$\frac{|\mathrm{GL}(n,q)|}{\prod_i \left(q^{\frac{1}{2}\deg f_i}-1\right)\prod_j \left(q^{\deg g_j}-1\right)}$$

Introduce generating function

$$r(q;2d) := \frac{\#(y,x) \text{ in } \ 2d \ \text{ dimensions}}{|\mathrm{GL}(2d,q)|}$$

$$R(u) := \sum_{d\geq 1} r(q;2d)u^d =$$

$$\prod_{f=f^*}\left(1+\frac{u^{\frac{1}{2}\deg f}}{q^{\frac{1}{2}\deg f}-1}\right)\prod_{g,g^*}\left(1+\frac{u^{\deg g}}{q^{\deg g}-1}\right)$$

Introduce generating function

$$r(q;2d) := \frac{\#(y,x) \text{ in } \ 2d \ \text{ dimensions}}{|\mathrm{GL}(2d,q)|}$$

$$R(u) := \sum_{d\geq 1} r(q;2d)u^d =$$

$$\prod_{f=f^*}\left(1+\frac{u^{\frac{1}{2}\deg f}}{q^{\frac{1}{2}\deg f}-1}\right)\prod_{g,g^*}\left(1+\frac{u^{\deg g}}{q^{\deg g}-1}\right)$$

$N^*(q;\ell) := |\{f \mid f=f^*, \deg f = \ell\}|$
$M^*(q;\ell) := |\{\{g,g^*\} \mid g\neq g^*, \deg g = \ell\}|$

$$R(u) = \prod_{\ell\geq 1}\left(1+\frac{u^\ell}{q^\ell-1}\right)^{N^*(q;2\ell)}\prod_{\ell\geq 1}\left(1+\frac{u^\ell}{q^\ell-1}\right)^{M^*(q;\ell)}$$

Using some magic of Fulman, Neumann, Praeger

Theorem (Praeger, Seress)

$$\lim_{d\to\infty} r(q;2d) = \left(1-\frac{1}{q}\right)^2$$

$$\lim_{d\to\infty} s(q;2d) = \left(1-\frac{1}{q}\right)^2 \left(\prod_i (1-q^{-i})\right)^3$$

$x \in \mathcal{C}(V_{2d})$, $s(q;2d) := \mathrm{Prob}(xx' \ \text{ regular } \ \text{semisimple})$

Beautiful solution, but not the original problem

$x \in \mathcal{C}(V)$, $y = xx'$, y regular semisimple

need to control the 2-part of $|y|$

Beautiful solution, but not the original problem

$x \in \mathcal{C}(V)$, $y = xx'$, y regular semisimple
need to control the 2-part of $|y|$

$$c_y(t) = \prod_{i=1}^{r} f_i(t) \prod_{j=1}^{s} g_j(t) g_j^*(t), \quad V = \bigoplus_{i=1}^{r} V_i \oplus \bigoplus_{j=1}^{s} W_j$$

$f_i^*(t) = f_i(t)$, $\deg f_i$ even

$y_i = y \mid_{V_i}$, $y_j' = y \mid_{W_j}$

$c_{y_i}(t) = f_i(t)$, $c_{y_j'}(t) = g_j(t) g_j^*(t)$

$m = |y| = \operatorname{lcm}\{|y_i|, |y_j'|\}$
Subspaces V_i, W_j with $|y_i|_2 < |y|_2, |y_j'|_2 < |y|_2$ are stabilized pointwise by $y^{m/2}$

Fix $b \in \mathbb{Z}^+$, define $\mathbb{Z}^{<b} = \{\ell \mid 2^b \text{ does not divide } q^\ell - 1\}$

Consider only y satisfying the conditions:

For exactly one W_j, $\dim(W_j) = 2\ell$, $\ell \notin \mathbb{Z}^{<b}$

All other $\dim(V_i)/2, \dim(W_{j'})/2 \in \mathbb{Z}^{<b}$

$(q^\ell - 1)_2$ divides $|y_j'|$

Then $E_{-1}(y^{m/2}) = W_j$

Fix $b \in \mathbb{Z}^+$, define $\mathbb{Z}^{<b} = \{\ell \mid 2^b \text{ does not divide } q^\ell - 1\}$
Consider only y satisfying the conditions:
For exactly one W_j, $\dim(W_j) = 2\ell$, $\ell \notin \mathbb{Z}^{<b}$
All other $\dim(V_i)/2, \dim(W_{j'})/2 \in \mathbb{Z}^{<b}$
$(q^\ell - 1)_2$ divides $|y'_j|$
Then $E_{-1}(y^{m/2}) = W_j$

Key lemma

b can be chosen so that for $n/6 \leq \ell \leq n/3$,

$$\#(y, x) > \frac{|\mathrm{GL}(n, q)|}{48\ell}$$

Note that for such y, $y^{m/2}$ acts as strong involution on $E_{-1}(x)$ and on $E_1(x)$

Proof of Key lemma

Number of choices for W_j, y'_j, $\{g_j, g_j^*\}$ is easy
Hard part: other factors of $c_y(t)$ must have degrees from the set $\mathbb{Z}^{<b}$

Reduces to estimate coefficients in the power series form of

$$R(u)^{<b} = \prod_{\ell \in \mathbb{Z}^{<b}} \left(1 + \frac{u^\ell}{q^\ell - 1}\right)^{N^*(q;2\ell)} \prod_{\ell \in \mathbb{Z}^{<b}} \left(1 + \frac{u^\ell}{q^\ell - 1}\right)^{M^*(q;\ell)}$$

Fulman, Neumann, Praeger method is a good start, but no miracles
Difficult estimates of contour integrals on $\mathbb{C}$

Final step: x is a strong involution

$y = xx'$ has nontrivial fixed point space, but we may require no repeated factors of degree > 1 in $c_y(t)$
$y^{m/2}$ is $(\frac{1}{6}, \frac{2}{3})$-balanced on each $E_{\pm 1}(x)$
Estimates are straightforward

Final step: x is a strong involution

$y = xx'$ has nontrivial fixed point space, but we may require no repeated factors of degree > 1 in $c_y(t)$
$y^{m/2}$ is $(\frac{1}{6}, \frac{2}{3})$-balanced on each $E_{\pm 1}(x)$
Estimates are straightforward

Theorem (Praeger, Seress)

There exist explicitly computable constants n_0, c so that if $n > n_0$, $x \in \mathrm{GL}(n, q)$ is a strong involution, and $g \in \mathrm{GL}(n, q)$ is random then g is of even type and $\zeta(g)$ is a $(\frac{1}{6}, \frac{2}{3})$-balanced involution on each $E_{\pm 1}(x)$ with probability at least $c/\log n$.