Hidden Subgroup Minicourse - Extraspecial groups

Gábor Ivanyos
MTA SZTAKI & TU/e

CWI Amsterdam, October 30 - November 3, 2006

Contents

On commutators and exponentiation

- Commutator: $[x,y]=x^{-1}y^{-1}xy=(yx)^{-1}xy$ $xy=yx[x,y]$
- $[y,x]=[x,y]^{-1}$
- If $G'\le Z(G)$ then $[xx',yy']=[x,y][x,y'][x',y][x',y']$
  $[xx',y]=x'^{-1}x^{-1}y^{-1}xx'y=x'^{-1}x^{-1}y^{-1}xyx'[x',y]=$
  $x'^{-1}[x,y]x'[x',y]=[x,y][y,x]$
- If $G'\le Z(G)$ then $(xy)^t=[x,y]^{-t(t-1)/2}x^ty^t$.
  Let $z_t=(xy)^t(x^ty^t)^{-1}$. Then $(xy)^t=z_tx^ty^t$.
  $(xy)^{t+1}=z_tx^ty^txy=z_tx^{t+1}x^{-1}y^txy=z_tx^{t+1}[x,y^{-t}]y^{t+1}=$
  $z_t[x,y^{-t}]x^{t+1}y^{t+1}$, so $z_{t+1}=z_t[x,y^{-t}]$
  $z_t=\prod_{i=0}^{t-1}[x,y^{-i}]=[x,\prod_{i=0}^{t-1}y^{-i}]=[x,y^{-t(t-1)/2}]=$
  $[x,y]^{-t(t-1)/2}$.
- If p is odd, $G'\le Z_G$, and G' is of exponent p, then $(xy)^p=x^py^p$.
- If p is odd, $G'\le Z_(G)$, $x^p=y^p=1$ then $(xy)^p=1$.
  (Elements of order $\le p$ form a subroup.)

Extraspecial groups

- p prime, G a finite p-group. G is extraspecial if
  - $G' = \mathbb{Z}(G)$
  - G/G' elementary abelian (i.e. $\cong \mathbb{Z}_p^\ell$ for some ℓ).
  - $Z(G) \cong \mathbb{Z}_p$
- From now on, assume p is odd.
- Two maps to G':
  - $[,] : G \times G \to G'$ homomorphism in both coordinates
  - $\hat{}^p : G \to G'$
  - both are well-defined on G/G'
    $[xz, y] = [x, y][z, y] = [x, y]$ because $z \in G' = Z(G)$
    $(xz)^p = x^p z^p = x^p$ because $z \in G' = Z(G) \cong \mathbb{Z}_p$

Extraspecial groups - symplectic view

- $V = G/G' \cong \mathbb{Z}_p^m$, consider as vector space over the field Z_p.
- $G' = Z(G) \cong \mathbb{Z}_p$. Fix any generator $z \in Z(G)$ and identify it with $1 \in \mathbb{Z}_p^*$.
- $[,]$ gives a non-degenerate skew-symetric bilinear function V. non-degenerate since $Z_G = G'$.
- $f : x \mapsto x^p$ gives a linear function on V.

Extraspecial groups - basis selection

- case $f = 0$:
  - choose $x_1 \in V$ and then $y_1 \in V$ s.t. $[x_1, y_1] = 1$
  - $i + 1$-th step:
    choose $x_{i+1} \in V_i$ and then $y_{i+1} \in V_i$ s.t. $[x_1, y_1] = 1$
  - where $V_i = \{x_1, y_1, \ldots, x_i, y_i\}^\perp$.
- case $f \neq 0$:
  - chose y_1 s.t. $f(y_1) = 1$.
  - $(\ker f)^\perp$ is one dimensional subspace of $\ker f$,
    $y_1 \notin (\ker f)^{\perp\perp} = \ker f$
    choose $x_1 \in (\ker f)^\perp$ such that $[x_1, y_1] = 1$.
  - Notice $\ker f = x_1^\perp$ and proceed as above.
- consequence: m even.

Extraspecial groups - presentation

- p odd, $m = 2r$. Groups H_r and E_r
- generators $x_1, y_1, \ldots, x_r, y_r$ and z.
- Relations:
  - $x_1^p = x_i^p = y_i^p = 1$ $(i = 2, \ldots, r)$
  - $y_1^p = 1$ (H_{2r}) or $y_1^p = z$ (E_{2r})
  - $[x_i, x_j] = [y_i, y_j] = 1$, $[x_i, y_j] = z^{\delta_{ij}}$ $(i, j = 1, \ldots, r)$
- Elements:

$$x_1^{i_1} \cdots x_r^{i_r} y_1^{j_1} \cdots y_r^{j_r} z^k$$

$(i_1, \ldots, i_r, j_1, \ldots, j_r, k \in \mathbb{Z}_p)$

Extraspecial groups - central products

- Subgroups $U_i = \langle x_i, y_i \rangle$ $U_i = x_i^s y_i^t z^u$. Extraspecial groups of order p^3.
- Direct product of U_i:

$$x_1^{i_1} \cdots x_r^{i_r} y_1^{j_1} \cdots y_r^{j_r} z_1^{k_1} \ldots, z_r^{k_r}$$

  $(i_1, \ldots, i_r, j_1, \ldots, j_r, k_1, \ldots, k_r \in \mathbb{Z}_p)$
- Our group: factor of this by the relation $z_1 = \ldots = z_r$.
  (By the normal subgroup generated by $z_1^{-1} z_2, \ldots, z_1^{-1} z_r$.)
- This will be useful for determining representations.

Some properties of p-groups

G finite p-group.

- $\mathbb{Z}(G) > 1$.

  sizes of conjugacy classes: powers of p. (Orbits of conjugacy action). Cannot be there only 1 class of size 1,

- $\exists\ 1 = G_0 < G_1 < \ldots < G_m = G$ such that $G_i \lhd G$ and $G_i/G_{i-1} \cong \mathbb{Z}_p$. (So G is supersolvable.)

  Let $z \in Z(G)$ of order p and set $G_1 = \langle z \rangle$. Then $G_1 \lhd G$. Proceed in G/G_1.

- If $K < G$ then $N_G(K) > K$. (So every subgroup is subnormal.)

  $Z(G) \neq 1$. If $K \not\geq Z(G)$ then $K < KZ(G) \leq N_G(H)$.
  If $K \geq Z(G)$ then induction to $K/Z(G)$ in $G/Z(G)$)

General HSP reductions in p-groups

- p-cyclic HSP: $H = 1$ or $|H| = p$.
- G finite p-group. HSP in G is reducible to p-cyclic *HSP* in factors of subgroups of G.

(1) Take a chain $1 = G_0 < G_1 < \ldots < G_m$ with $G/G_i \cong \mathbb{Z}_p$. Find the first i, such that $H \cap G_i \neq 1$. Set $H_0 = H \cap G_i$.

(2) Find $N_H(H_0) = N_G(H_0) \cap H$ with recursion to a HSP in $N_G(H_0)/H_0$.

If $H > H_0$ then $N_H(H_0) > H_0$.

(3) If $N_H(H_0) = H_0$ then $H = H_0$. Otherwise repeat (2) with $H(0) \leftarrow N_H(H_0)$

Subgroups of extraspec groups

- If H not commutative then $H \geq G'$.

  H contains a power of z, which generate G'.
- If the exponent of H is bigger than p then $H \geq G'$.

  If $x^p \neq 1$ the x^p generates G'.
- Easy to test whether $H \geq G'$.
- If $H \geq G'$, Fourier sampling of G/G' finds H.
- Remain: abelian H of exponent p.
- The elements of order p in E_r are in the subgroup $K = \langle x_1 \rangle \times \langle x_2, y_2, \ldots, x_r, y_r \rangle$. So $H \leq K$.
- embed K into H_r as a subgroup, extend the hiding function to H_r.

Subgroups of exponent p extraspecial groups

- Remains: HSP in H_r
- Cyclic HSP in factors of subgroups of H_r. These groups are either abelian or isomorphic to subgroups of H_r.

  $G = H_r$, $N \lhd K \le G$. If K/N is not abelian then $N \cap G' = 1$ and $N' \le N \cap G' = 1$.
  $[K,N] \le N$ (since $N \lhd K$). On the other hand
  $[K,N] \le [G,G]$, so $[K,N] = 1$, i.e., $K \le C_G(N)$.
  $N = \langle u_1 \rangle \times \cdots \times \langle u_\ell \rangle$
  Take a basis x_i, y_i of G that extends $u_1, \ldots, u_\ell$:
  $x_1 = u_1, \ldots, x_\ell = u_\ell$.
  $C_G(N) = \langle x_1, \ldots, x_r, y_{\ell+1}, \ldots, y_r, z \rangle$
  $C_G(N)/N \cong H_{r-\ell} \le H_r$
- Remains: cyclic HSP in H_r.

High-dimensional irreps of H_1

.

$\omega = \sqrt[p]{1}$, $u \in \mathbb{Z}_p^*$, $p \times p$ matrices:

$$X_u = \begin{pmatrix} 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1.. & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

$$Y_u = \begin{pmatrix} \omega^{0u} & 0 & \dots & 0 & 0 \\ 0 & \omega^{1u} & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \omega^{(p-2)u} & 0 \\ 0 & 0 & \dots & 0 & \omega^{(p-1)u} \end{pmatrix}$$

High-dim irreps of H_1 2.

.

- H_1: generators x, y (and z); relations $x^p = y^p = z^p = 1$, $[x, y] = z$.
- $X_u^p = Y_u^p = 1$, $Z_u = [X_u, Y_u] = \omega^u I$ satisfy the relations for H_1.
- $x \mapsto X_u$, $y \mapsto Y_u$ extends to a p-dimensional representations of H_1.
- $Tr(X_u^i Y_u^j Z_u^k) = 0$ if $i \neq 0$ (no diagonal entries).
- $Tr(Y_u^j Z_u^k) = \omega^{uk} \sum_{\ell=0}^{p-1} \omega^{jl} = 0$ if $i = 0$ but $j \neq 0$.
- $Tr(Z_u^k) = p\omega^{uk}$
- $\chi_u = Tr(\rho_u)$ character. $(\chi_u, \chi_u) = \frac{1}{p^3} \sum_{g \in G} |\chi_u(g)|^2 = \frac{1}{p^3} \sum_{g \in \langle z \rangle} p^2 = 1$
- ρ_u irred.

Irreps of H_1

.

- ρ_u irred.
- for $u \neq u' \in \mathbb{Z}_p^*$, $\chi_u(z) = p\omega^u \neq p\omega^{u'} = \chi_{u'}(z)$
- so ρ_u's are nonequivalent irreps. of dimension p.
- $\sum_{u \in \mathbb{Z}_p^*} (\dim \rho_u)^2 = (p-1)p^2$.
- $+p^2$ from the 1-dim reps.
- That's all.

Irreps of H_r

.

- H_r is a central product of H_1's: a factor of H_1^r by $\langle z_i z_j^{-1} \rangle$.
- $\rho_u^{\otimes r}$ is irrep of H_1^r (dim: p^r), mapping $z_i z_j^{-1}$ to I.
- So $\tilde{\rho}_u = \rho_u^{\otimes r}$ is a well-defined irrep of H_1 with $\tilde{\rho}_u(z) = \omega^u I_{p^r}$.
- for $u \neq u' \in \mathbb{Z}_p^*$ $\tilde{\chi}_u(z) = p^r \omega^u \neq p^r \omega^{u'} = \tilde{\chi}_{u'}(z)$
- so $\tilde{\rho}_u$'s are nonequivalent irreps. of dimension p^r.
- $\sum_{u \in \mathbb{Z}_p^*} (\dim \rho_u)^2 = (p-1)p^{2r}$.
- $+p^{2r}$ from the 1-dim reps.
- That's all.

Outline of the algorithm

- We have the p-cyclic HSP in $G = H_r$.
- May assume that $H \neq G'$
- First determine HG'

  With Fourier sampling of G/G'. This requires an action with stabilizer HG'
- Then H is a hidden subgroup in the abelian group HG'.

Tensor product of irreps of H_r

- $\rho_1 = \rho_{u_1}, \ldots, \rho_k = \rho_{u_k}$ high-dim irreps. of H_r, $\rho = \rho_1 \otimes \cdots \otimes \rho_k$.
- If $u = \sum_{i=1}^k u_i \neq 0$ then $\rho = \rho_u^{p^{r(k-1)}}$ (direct power).
  - $\rho(z) = \omega^u I_{p^{rk}} \Rightarrow$ Irred constituents of ρ are ρ_u.
- If $u = \sum_{i=1}^k u_i = 0$ then $\rho = \rho_0^{p^{r(k-2)}}$, where $\rho_0 = \bigoplus$ of the 1-dim reps.
  - If μ is a 1-dim rep then $\mu \otimes \rho_{u_1} \cong \rho_{u_1}$. (Because $(\mu \otimes \rho_{u_1})(z) = \omega^{u_1} I$.)
  - ρ_0 is a sum of 1-dim reps (Because $\rho_0(z) = I$.)
  - $\mu \otimes \rho_0 \cong \rho_0$, hence the multiplicities are equal.

Forcing ρ_0

- ρ_0 is the representation we like: $\rho_0(G) \cong G/G'$, $\rho_0(H) = \rho_0(HG')$. Fourier sampling for ρ_0 would determine HG'.
- How to enforce ρ_0?
- Assume we have a module $V_\phi = V_1 \otimes \cdots \otimes V_r$ where V_i module for $\rho_i = \rho_{u_i}$.
- $\rho(g)$ is lin. extension of $v_1 \otimes \cdots \otimes v_r \mapsto \rho_1(g)v_1 \otimes \cdots \otimes \rho_r(g)v_r$.

Twist

- $V_\phi = V_1 \otimes \cdots \otimes V_r$
  $\rho(g)(v_1 \otimes \cdots \otimes v_r) = \rho_1(g)v_1 \otimes \cdots \otimes \rho_r(g)v_r$.
- If ϕ is an endomorphism of G and μ is a representation of G, then $\mu \circ \phi$ is a representation as well (of thew same dimension).
- We can replace each ρ_i with $\rho_i \circ \phi_i$ where $\phi_i \in Aut(G)$.
- For $j \in \mathbb{Z}_p^*$ $\exists$ automorphism ϕ_j that induces $g \mapsto g^j$ on G/G' (means: $\phi_j(g)G' = g^j G'$ and $\phi_j(z) = z^{j^2}$.
    - On generators $\tilde{\phi}_j : G \to G$ on generators $x_i \mapsto x_i^j, y_i \mapsto y_i^j$, $z \mapsto z^{j^2}$.
    - $\tilde{\phi}_j$ extends to an automorphism ϕ_j of G since x_i^j, y_i^j, z_{2j} satisfy the original relations

Twist 2

- Automorphism ϕ_j that induces $v \mapsto v^j$ on G/G' and $\phi_j(z) = z^{j^2}$.
- $\rho_u \circ \phi_j = \rho_{j^2 u}$
$$\rho(\phi_j(z)) = \rho_u(z^{j^2}) = (\rho_u(z))^{j^2} = \omega^{uj^2} I = \rho_{uj^2}.$$
- So $\rho_{u_1} \circ \phi_{j_1} \otimes \cdots \otimes \rho_{u_1} \circ \phi_{j_k} \cong$ a direct power of ρ_u, where $u = u_1 j_j^2 + \ldots + u_k j_k^2$ (in $\mathbb{Z}_p$).
- $u = 0$ if $u_1 j_j^2 + \ldots + u_k j_k^2 = 0$ (in $\mathbb{Z}_p$).

Twist 2.

- Work with right coset states. $g \leftrightarrow g^{-1}: \; gH \leftrightarrow Hg^{-1}$
- $|Ha_1\rangle \dots |Ha_k\rangle$
- Weak Fourier Sampling: $\rho_1(Ha_1) \otimes \dots \otimes \rho_k(Ha_k)$
- Instead, we apply (a version of) Fourier of G':

$$\begin{aligned}\Phi : |x^{t_x} y^{t_y}\rangle |z^{t_z}\rangle \quad &\mapsto \quad \frac{1}{\sqrt{p}} \sum_{u \in \mathbb{Z}_p} \omega^{ut_z} |x^{t_x} y^{t_y}\rangle |u\rangle \\ &\mapsto \quad \sum_{u \in \mathbb{Z}_p} \omega^{ut_z} |u\rangle |x^{t_x} y^{t_y}\rangle |e_u\rangle\end{aligned}$$

where $|e_u\rangle = \frac{1}{p} \sum_{j \in \mathbb{Z}_p} \omega^{-ju} |z^j\rangle$.

Twist 3.

- $z^t e_u = \omega^{ut} e_u$, $\Phi(z^t) = \sum_{\omega\in\mathbb{Z}_p} |\omega\rangle|ze_u\rangle$
- $\Phi|g\rangle = \sum_{u\in\mathbb{Z}_p} |u\rangle|ge_u\rangle$.
- $|zge_u\rangle = |gze_u\rangle = \omega^u|ge_u\rangle$,
- So for $u \neq 0$, $\mathbb{C}Ge_u$ is the sum of submodules of $\mathbb{C}G$ isomorphic to V_u.
- And for $u = 0$ $\mathbb{C}Ge_u \cong V_0$.

Twist 4.

- For multiple coset states: $|Ha_1, \ldots, Ha_k\rangle$
- Apply $\Phi^{\otimes k}$, measure $|u_1, \ldots, u_k\rangle$:
- State $w = |a_1 He_{u_1}, \ldots, a_k He_{u_k}\rangle$
- If some $u_i = 0$, apply Fourier of G/G' to $|a_i He_0\rangle$ and measure a lin repr. μ with $HG' \subseteq \ker \mu$.
- Unfortunately, with high prob. no $u_i = 0$.
- state w is in a submodule V of $\mathbb{C}G^{\otimes k}$, which is $\cong$ a power of $V_{u_1} \otimes \cdots V_{u_k}$ (diagonal action of G).
- assume we find $j_1, \ldots, j_k \in \mathbb{Z}_p$, not all j_i zero, s.t. $\sum_{i=1}^{k} u_{j_i}^2 = 0$.

Twist 5.

- Twisted action
  $\rho(g) : v_1 \otimes \cdots \otimes v_k \mapsto \phi_{j_1}(g)v_1 \otimes \cdots \otimes \phi_{j_k}(g)v_k$
  makes $V \cong$ a power of V_0 (the module we like).
- What is $\{\rho(g)w | g \in G\}$?
- If $f \notin gHG'$ then $fw \perp gw$,
  - if $j_1 \neq 0$ already $|fHa_1e_1\rangle \perp |gHa_1e_1\rangle$ because
    $supp(|\phi_{j_1}(f)Ha_1\rangle) \subseteq \phi_{j_1}(f)Ha_1G' = \phi_{j_1}(g)HG'a_1$,
    $supp(|\phi_{j_1}(g)Ha_1\rangle) \subseteq \phi_{j_1}(g)HG'a_1$
    and $\phi_{j_1}(f)HG'a_1 \cap \phi_{j_1}(g)HG'a_1 = \emptyset$.

Twist 6.

- Twisted action
  $\rho(g) : v_1 \otimes \cdots \otimes v_k \mapsto \phi_{j_1}(g)v_1 \otimes \cdots \otimes \phi_{j_k}(g)v_k$
- If $f \in gHG'$, say $f = ghz^\ell$ then

$$\begin{aligned}\phi_{j_i}(f)Ha_ie_{u_i} &= \phi_{j_i}(g)\phi_{j_i}(hz^\ell)Ha_ie_{u_i} = \omega^{u_i\ell j^2}\phi_{j_i}(g)\phi_{j_i}(h)Ha_ie_{u_i} \\ & \ \phi_j(h) \in h^jG', \text{ so } \phi_j(h) = h^jz^{\alpha(j,h)}\ (\alpha(j,h) \in \mathbb{Z}_p) \\ &= \omega^{u_i(\ell j^2+\alpha(j_i,h))}\phi_{j_i}(g)Ha_ie_{u_i}\end{aligned}$$

$\rho(f)w = \omega^{\sum_{i=1}^r u_i(\ell^2+\alpha(j_i,h))}\rho(g)w,.$

a scalar multiple $\rho(g)w$, thanks to that $\phi_j(H) \leq G'H$.

Twist 7.

- If $f \in gHG'$, say $f = ghz^{\ell}$ then $\rho(f)w = \omega^{\sum_{i=1}^{r} u_i(\ell^2 + \alpha(j_i,h))}\rho(g)w,.$ a scalar multiple $\rho(g)w$, thanks to that $\phi_j(H) \leq G'H$.
- $z^{\alpha(j,h)} = h^{-j}\phi_j(h)$.
- Example: If $h = x_1 z^m$ then $\phi_j(h) = x_1^j z^{mj^2} = h^j z^{m(j^2-j)}$
- Claim: For every $h \in G$ $\exists x = x_h \in G'h$ such that for every $j \in \mathbb{Z}_p^*$ $\phi_j(x) = x^j$.

Twist 8.

.

- Claim: For every $h \in G$ $\exists x = x_h \in G'h$ such that for every $j \in \mathbb{Z}_p^*$ $\phi_j(x) = x^j$.
  - j_0 primitive element (generator for) $\mathbb{Z}_p^*$. $j = j_0^t$ for every $j \in \mathbb{Z}_p$ and $\phi_j = \phi_j^t$.
  - If $\phi_{j_0}(x_h) = x_h^{j_0}$ then $\phi_j(x_h) = \phi_j^t(x_h) = x_h^{j_0^t}$.
  - Consider $W = G'H \cong \mathbb{Z}_p^2$, $\phi = \phi_{j_0}|_W$ is an automorphism of W. Additively, ϕ is a lin. transf. of W.
  - G' is an eigenspace of ϕ: eigenvalue j^2. In the basis z, h, the matrix of ϕ:

$$\begin{pmatrix} j_0^2 & * \\ 0 & j_0 \end{pmatrix}$$

  - The eigenvalues of ϕ are $j_0 \neq j_0^2$, x_h will be the appropriate element of the j_0-eigenspace.

Twist 9.

- Claim: For every $h \in G$ $\exists x = x_h \in G'h$ such that for every $j \in \mathbb{Z}_p^*$ $\phi_j(x) = x^j$.
- Claim: For every $h \in H$ $\exists m_h \in \mathbb{Z}_p$ such that $\alpha(j, h) = m_h(j^2 - j)$ (for every $j \in \mathbb{Z}_p^*$).
  - $h = h_x z^{m_h}$.
  - $\phi_j(h) = h_x^j z^{m_h j^2} = h^j z^{m_h(j^2 - j)}$.
- Consequence: if $\sum_{i=1}^k u_i j_i^2 = 0$ and $\sum_{i=1}^k u_i(j_i^2 - j_i) = 0$ then the states $|gw\rangle$ are pairwise orthogonal, and the stabilizer of w is $G'H$.

The algorithm 1.

- $k = 3$.
- Use Fourier of G'^3 to obtain the state

$$w = |Ha_1 e_{u_1}, Ha_2 e_{u2}, Ha_3 e_{u_3}\rangle$$

  where $u_1, u_2, u_3 \in \mathbb{Z}_p$ random.
- Set $j_3 = 1$, $j_2 = \frac{-u_1 j_1 - u_3}{u_2}$, solve $u_1 j_1^2 + (u_1 j_1 + u_3)^2 + u_3 = (u_1^2 + u_1) j_1^2 + 2u_1 u_3 j_1 + u_3^2 + u_3$ in u_1. It can be solved for a constant fraction of cases.
- Define the action $\rho(g)$ on $|v_1, v_2, v_3\rangle$ as $\rho(g)|v_1, v_2, v_3\rangle = |\phi_{j_1}(g)v_1, \phi_{j_2}(g)v_2, \phi_{j_3}(g)v_3\rangle$.
- As $\rho(g) = \rho(z^\ell g)$ for $z^\ell \in G'$, for $g = x^{t_x} y^{t_y} z^{t_z}$

$$\rho(g)|v_1, v_2, v_3\rangle = |x^{j_1 t_x} y^{j_1 t_y} v_1, x^{j_2 t_x} y^{j_2 t_y} v_2, x^{j_3 t_x} y^{j_3 t_y} v_3\rangle.$$

The algorithm 2.

- for $g = x^{t_x} y^{t_y} z^{t_z}$

$$\rho(g)|v_1, v_2, v_3\rangle = |x^{j_1 t_x} y^{j_1 t_y} v_1, x^{j_2 t_x} y^{j_2 t_y} v_2, x^{j_3 t_x} y^{j_3 t_y} v_3\rangle.$$

  defines an action of $\mathbb{Z}^{2r} = G/G'$ on the orthonormal system $\{\rho(g)w | g \in G\}$ with stabilizer HG'.
- Fourier sampling in $G/G' \cong \mathbb{Z}^{2r}$ (for the function $\overline{g} \mapsto \rho(g)w$) gives a random 1-dim rep μ of G with $HG' \subseteq \ker \mu$.

Mehtod generalizable to p-groups with $G' \leq Z(G)$.