1 Summary of Nil-2 HSP Algorithm

Problem: Solve the HSP for $H \leq G$, where G is a nil-2 group.

1.1 Reduction Steps

1. Calculate the refined polycyclic representation of G.
2. Reduce to HSP in nil-2 p-groups
3. Reduce to case where H is either trivial or order p
4. Reduce to case where G has exponent p.
5. Reduce to finding a quantum hiding function for HG'
6. Reduce to finding an appropriate triple
7. Reduce to solving a large system of linear and quadratic equations

1.2 Quantum Algorithm

All of the above steps have efficient classical algorithms, except for the step of generating a quantum hiding function for HG' given an appropriate triple, so I'll focus on this step.

Summary:

1. Compute the superposition $\sum_{u \in G'} |u\rangle |aHG'_u\rangle$ for random $a \in G$, where $G_u = DFT(|u\rangle)$.
2. Do the last step n times in parallel for some large n
3. Solve the system of equations to get $\bar{j} \in (\mathbf{Z}_p)^n$
4. $\left|\Psi_g^{\bar{a},\bar{u},\bar{j}}\right\rangle = \bigotimes_{i=1}^n \left|a_i HG'_{u_i} \phi_{j_i}(g)\right\rangle$ as a function of $g \in G$ is a hiding function for HG', where ϕ_j are nice automorphisms of G.

The following properties of the automorphisms ϕ_j are used in the proof:

1. $|aHG'_u\rangle$ is an eigenvector for right multiplication by $\phi_j(g)$
2. ϕ_j maps HG' to HG'