Parameterized Complexity of some Permutation Group Problems

V. Arvind
Institute of Mathematical Sciences, Chennai
India
email arvind@imsc.res.in

January 9, 2013
Plan of Talk

• Permutation groups background.

• Fixed point free elements of a permutation group (and its parameterization).

• Computing a minimum base for a permutation group (and its parameterization).
Permutation Groups: Definitions

- \( S_n \) denotes the group of all permutations on \( n \) elements. Forms a group under permutation composition.

- A subgroup \( G \) of \( S_n \), denoted \( G \leq S_n \), is called a permutation group (of degree \( n \)).

- The permutation group \( \langle S \rangle \), generated by a subset \( S \subseteq S_n \) of permutations, is the smallest subgroup of \( S_n \) containing \( S \).

- Every finite group \( G \) has a generating set of size \( \log_2 |G| \). So, giving a generating set is a succinct presentation of a finite group as algorithmic input.
Definitions Contd.

• For a permutation $\pi \in S_n$, a point $i \in [n]$ is a fixed point if $\pi(i) = i$.

• $\text{fix}(\pi)$ is the number of points fixed by $\pi$.

• A permutation group $G \leq S_n$ induces an equivalence relation on the domain $[n]$: $i$ and $j$ are related iff $g(i) = j$ for some $g \in G$. The equivalence classes are the orbits of $G$.

• $G$ is called transitive if there is exactly one orbit.
Orbit Counting Lemma

Some ancient results (by CS standards):

**Lemma 1 (Orbit Counting)** Let $G \leq S_n$ be any permutation group and $\text{orb}(G)$ denote the number of orbits of $G$. Then

$$\text{orb}(G) = \frac{1}{|G|} \sum_{g \in G} \text{fix}(g).$$

**Theorem 2 (Jordan’s Theorem (1872) )** If $G \leq S_n$ is transitive then the group $G$ has a fixed point free element.

Follows easily from the Orbit Counting Lemma.
Cameron-Cohen’s Theorem

**Theorem 3 (CC92)** If $G \leq S_n$ is transitive then the group $G$ has a fixed point free element then there are at least $|G|/n$ many elements that are fixed point free.

**Remark 4** Let $G = \langle S \rangle$ be a permutation group given as input by generating set $S$. Using an algorithm of C. Sims [1970] it is possible to sample uniformly at random from $G$ in polynomial time. This gives a simple randomized algorithm for computing a fixed point free element.

We derandomize this as part of our FPT algorithm.
Fixed Point Free Elements

- Computing fixed point free elements in *nontransitive* permutation groups $G = \langle S \rangle$ given by generating sets is known to be NP-hard [Cameron-Wu 2010].

- This is similar to the NP-hard problem of computing a fixed point free automorphism of a graph [Lubiw 1980].

- We now introduce a parameterized version of the problem.
Fixed Point Free: Parameterized

- \textbf{\textit{k-MOVE} Problem:}

Input: A permutation group \( G = \langle S \rangle \leq S_n \) given by generators and a parameter \( k \).

Problem: Is there an element in \( G \) that \textit{moves} at least \( k \) points (i.e. the element fixes at most \( n - k \) points).

For \( k = n \) notice that such an element if fixed point free. Our first result:

\textbf{Theorem 5} \textit{The} \( k \)-\textit{MOVE problem is fixed parameter tractable} (in time \( 2^{2k+O(\sqrt{k} \lg k)} k^{O(1)} + n^{O(1)} \)).
**Proof Idea**

- Let $\text{move}(g)$ denote the number of points moved by $g \in G$ and $\text{move}(G)$ denote the number of points moved by some $g \in G$.

- The orbit counting proof method easily yields for any permutation group $G$ that $\frac{1}{|G|} \sum_{g \in G} \text{move}(g) \geq \text{move}(G)/2$.

- The left side in the above inequality is an expectation. We can “derandomize” this and find a $g \in G$ such that $\text{move}(g) \geq \text{move}(G)/2$ in polynomial time.

- If $\text{move}(G) \geq 2k$ we are done. If $\text{move}(G) \leq 2k$, the domain shrinks to size $2k$ giving a kernel of that size.
Bases for Permutation Groups

• Let $G \leq S_n$ be a permutation group. A subset of points $B \subseteq [n]$ is called a base for $G$ if the subgroup $G_B$ of $G$ that fixes every point of $G$ is the identity.

• This generalizes bases for vector spaces and has proven computationally useful. There is a library of nearly linear-time algorithms for small base groups due to Akos Seress and others.

• Finding minimum bases of permutation groups is NP-hard [Blaha 1992] even for cyclic groups and groups with bounded orbit size.
The $k$-BASE problem

We define the parameterized complexity with $|B|$ as parameter for cyclic and bounded orbit groups.

Input: A permutation group $G = \langle S \rangle \leq S_n$ given by generators and a parameter $k$.

Problem: Is there a base for $G$ of size at most $k$?

Our results:

**Theorem 6** • The $k$–BASE problem is fixed parameter tractable for cyclic permutation groups and for permutation groups with bounded orbit size.
Some Questions

For example:

- The parameterized complexity of $k$-BASE for general permutation groups?
- Parameterized versions of Graph Isomorphism and related problems...
THANKS!