Rational reconstruction of representations

Simon Nickerson

16 March 2004

Rational representations

In this talk, we will be interested in explicitly constructing rational representations of finite (simple/quasisimple/almost simple) groups.

One important subproblem is how to split up a representation into its irreducible constituents. This involves:

- finding proper invariant subspaces; and
- computing the action of the group on those subspaces.

In this talk, we will restrict our attention to the second part of this problem.

Computing the action of the group on an invariant subspace

Let $G = \langle a, b \rangle$ be a finite group. Suppose V is a $\mathbb{Q}G$-module with a submodule W (our invariant subspace).

If we have a basis $w_1, w_2 \ldots w_m$ for W, then we can calculate explicit matrices for the action of G on W:

1. Perform a Gaussian elimination on the vectors $w_1, w_2, \ldots w_n$ so that the basis looks upper-triangular.

2. For each $1 \leq i \leq m$, rewrite aw_i and bw_i as a linear combination of the new basis vectors, and hence as a linear combination of the w_j.

The coefficients in these linear combinations give matrices for the action of a and b on W.

The problem with $\mathbb{Q}$

Unfortunately, this requires doing Gaussian elimination in $\mathbb{Q}$, which for large representations is painfully slow. This is mainly because at later stages of the algorithm, the matrix entries often have extremely large numerators and denominators. In experiments, I often came across situations where the intermediate data were deemed by GAP to be '`<<integers too large to be printed>>`'!

Can we instead use a field (such as $\mathbb{F}_p$) which does not suffer from this problem?

Reducing rational numbers modulo m

Let $m > 1$ be an integer. There is a well-known ring homomorphism:

$$\begin{aligned} \vartheta_m : \mathbb{Z} &\to \mathbb{Z}_m \\ x &\mapsto [x]_m \end{aligned}$$

Let $\mathbb{Q}_m$ denote the set of rationals r/s where s is coprime to m. Then $\mathbb{Q}_m$ is a ring, and ϑ_m extends to a homomorphism:

$$\begin{aligned} \theta_m : \mathbb{Q}_m &\to \mathbb{Z}_m \\ r/s &\mapsto [r/s]_m \end{aligned}$$

Examples:

- $\theta_{40}(5/7) = \theta_{40}(5)\theta_{40}(23) = \theta_{40}(115) = [35]_{40} = \theta_{40}(35)$

- $\theta_m(1/2) = [(m+1)/2]_m$ for $m \geq 3$ odd

From $\mathbb{Q}$-reps to $\mathbb{Z}_m$-reps

Suppose G is a finite group with a rational representation $\rho : G \to GL_n(\mathbb{Q})$. Let s be the lowest common denominator of the matrix entries in $\rho(G)$. Then if m is coprime to s, then we get another representation

$$\rho_m : G \to GL_n(\mathbb{Z}_m)$$

where $[\rho_m(g)]_{ij} = \theta_m([\rho(g)]_{ij})$, i.e. by reducing modulo m.

Question: is it possible to reconstruct ρ from ρ_m?

Answer: maybe.

Observe that θ_m is not an injective function, and in fact any element of $\mathbb{Z}_m$ has an infinite number of preimages in $\mathbb{Q}$. However, if the matrices in our representation appear 'nice', then we may hope that the entries of the corresponding rational matrix are small.

Our strategy

1. Choose primes $p_1, \ldots p_k$.

2. Construct representations over $p_1, \ldots p_k$, making sure that they are 'compatible'.

3. Combine the representations using the Chinese Remainder Theorem: we get a representation over $\mathbb{Z}_m$, where $m = p_1 \cdots p_k$.

4. Use the rational reconstruction algorithm to *guess* a θ_m-preimage for each matrix entry in a set of generators of G in the $\mathbb{Z}_m$-representation.

5. Check whether the resulting matrices are correct. If not, add more primes and go back to step 2.

1. Choosing primes

There are finitely many 'bad' primes which we avoid.

Firstly, we do not use any p which divides the group order, to avoid complications of the representation no longer being irreducible.

Secondly, if p divides the denominator of a matrix entry in the $\mathbb{Q}$-representation we are trying to construct, then this $\mathbb{Q}$-representation does not have a modulo p reduction, and thus any $\mathbb{F}_p$-representation that we manage to construct will be incompatible. This might be difficult to predict in advance.

In practice, primes greater than 100 are usually 'good'.

3. The Chinese Remainder Theorem

The set of simultaneous congruences:

$$\begin{aligned} x &\equiv r_1 \pmod{m_1} \\ x &\equiv r_2 \pmod{m_2} \\ &\vdots \qquad\quad \vdots \\ x &\equiv r_n \pmod{m_n} \end{aligned}$$

(with $x, r_1, r_2 \ldots r_n \in \mathbb{Z}$, and $m_1, m_2 \ldots m_n \in \mathbb{N}$ pairwise coprime) has a unique solution r modulo $m_1 m_2 \cdots m_n$. The value of r can easily be computed.

Hence for our primes $p_1, \ldots p_k$, we can find a representation of G over $\mathbb{Z}_m$ with $m = p_1 \cdots p_k$.

4. Rational reconstruction

Suppose we wish to find a rational reconstruction of a (mod b). Perform Euclid's algorithm for GCD to the numbers $n_0 = b$, $n_1 = a$:

$$\begin{aligned} n_0 &= q_1 n_1 + n_2 \\ n_1 &= q_2 n_2 + n_3 \\ &\vdots \qquad \vdots \qquad \vdots \\ n_{r-1} &= q_r n_r + n_{r+1} \\ n_r &= q_{r+1} n_{r+1} + 0 \end{aligned}$$

where for each $2 \leq i \leq r+1$, $0 < n_r < n_{r-1}$.

Let $n_0 = b$, $n_1 = a$. Choose any $2 \leq i \leq r+1$, and perform backward substitution from the $(i-1)$th line above to get an equation of the form:

$$n_i = r n_0 + s n_1$$

Then providing s and $n_0 (= b)$ are coprime, we get:

$$a \equiv n_i / s \pmod{b}$$

Example: $a = 900$, $b = 4199$

$$\begin{aligned} 4199 &= 4.900 + 599 \\ 900 &= 1.599 + 301 \\ 599 &= 1.301 + 298 \\ 301 &= 1.298 + 3 \\ 298 &= 99.3 + 1 \\ 3 &= 3.1 + 0 \end{aligned}$$

We get these equations and rationals a' with $a' \equiv a \pmod{b}$:

Equation	a'
$900 = 0 + a$	900
$599 = b - 4a$	$-599/4$
$301 = -b + 5a$	$301/5$
$298 = 2b - 9a$	$-298/9$
$3 = -3b + 14a$	$3/14$
$1 = 299b - 1395a$	$-1/1395$

For 'smallness' reasons, we take 3/14 as our guess.

5. Checking the matrices

Once we have found the putative representation, we need to test it, as there is a possibility that we made an incorrect guess along the way.

- If we have a presentation for G, we can check our matrices against the relations. If G is simple, then this is sufficient.

- If we know the submodule W, we can check that the action of our computed matrices on W is the same as the original group action.

Example: a 175-dimensional $\mathbb{Q}$-rep of $O_8^+(2)$

$O_8^+(2)$ is a simple group of order 174182400, and it has a subgroup A_9 of index 960. We construct a permutation representation ρ on the right cosets of this subgroup; ρ has decomposition:

$$\rho = 1 + 84_a + 175 + 700_a$$

Because ρ is multiplicity-free, it turns out to be computationally straightforward to find an explicit (irreducible) invariant subspace W of dimension 175. We now wish to find the action of the group generators on W.

We found 175×175 matrices giving the action of the group on W, by two different methods:

- rational reconstruction with the 10 primes p, $70 \leq p \leq 110$; and
- Gaussian elimination in $\mathbb{Q}$

Timings

Finding matrices by rational reconstruction with the 10 primes between 70 and 110: **130 seconds**

Checking the action of matrices on the submodule: **12 seconds** (N.B. We didn't have a presentation for $O_8^+(2)$ on the appropriate generators.)

Total: **142 seconds**

Constructing the representation by Gaussian elimination in $\mathbb{Q}$: **2041 seconds** (about 14 times as long)