1071-20-254 **Robert M Beals*** (beals@idaccr.org), 805 Bunn Drive, Princeton, NJ 08540. *Optimal black-box algorithms for the symmetric groups.*

We give an algorithm to determine whether a given black-box group is isomorphic to the symmetric group S_n. The parameter n is unknown, although it is bounded by the inequality $n! \leq 2^\ell$, where ℓ is the number of bits in the encoding of an element. This algorithm requires that each group element be represented by a unique string. The complexity, if the group is given by r generators, is $O(rn)$ operations to prove that the group is S_n, and $O(r\ell/\log \ell)$ group operations if the group is not proved to be S_n. If the group is isomorphic to S_n, then the algorithm succeeds with probability $1 - \exp(-rn^{1-o(1)})$.

Our second main result is that both our algorithm and a related algorithm of Beals, Leedham-Green, Neimeyer and Praeger are optimal in their respective computational models. Our lower bound actually applies to all finite groups G: a one-sided Monte Carlo algorithm to determine that a given black-box group is isomorphic to G requires $\Omega(\log |G|/\log\log |G|)$ operations if group elements are represented by unique strings, and $\Omega(\log |G|)$ operations otherwise. (Received March 07, 2011)