In 1964 F.J. MacWilliams introduced the technique of permutation decoding which uses a subset of the automorphism group of the code, a so-called PD-set. A PD-set for a $t$-error-correcting code $C$ is a set $S$ of automorphisms of the code which is such that, every possible error vector of weight $t$ or less can be moved by some member of $S$ out of the information positions. Concerning the question how to apply a PD-set to decode a message we refer to W. C. Huffman: “Codes and groups” in [2], pp. 1345 – 1440 where an algorithm is given. The permutation decoding algorithm is more efficient the smaller the size of the PD-set. A lower bound on this size is given by D.M. Gordon in [1]. When a code has a large automorphism group it is likely that a PD-set can be found. In [3] there are presented examples of PD-sets $S$ for the codes related to some classical varieties. The size $|S|$ is in some cases minimal. But often the size of the PD-set is so much larger than the bound given by Gordon and you may be disappointed about the large difference. Here the question arises whether the Gordon bound is in any case sharp, that means: is there in any case a PD-set $S$ in the corresponding symmetric group such that the size $|S|$ is the Gordon bound? We will present four examples where the Gordon bound is not sharp. For this purpose we introduce the notion of an antiblocking system. The properties of such an antiblocking system may help to find PD-sets and to prove whether a PD-set of given size may exist or not.

References

