Non-Adjacent Digit Expansions

Clemens Heuberger

Motivated by applications in cryptography, we consider redundant digit expansions to various bases. The redundancy allows to decrease the weight, i.e., the number of non-zero digits, and therefore the execution time for scalar multiplication algorithms in abelian groups such as the point group of an elliptic curve.

We discuss the questions of existence and optimality and analyse the expected weight.