Representing Integer Multiplication Using Binary Decision Diagrams

Håvard Raddum and Srimathi Varadharajan

The integer factorization problem is one of the most fascinating and formidable problems in mathematics dating back several centuries. In integer factorization, the input is an integer N and the task is to find its prime factors. Integer factorization forms the basis of the RSA public key cryptosystem. The RSA public key cryptosystem uses two primes p and q usually of the same bit size. The factorization of the RSA modulus $N = pq$ cannot be done efficiently in the classical computational model without the knowledge of p or q and this provides the security of RSA. An extensive amount of research has been done in RSA factorization.

In this paper we take a completely different approach to the integer factorization, compared to more well-known methods. The key point in our approach is to use Binary Decision Diagrams (BDD). A BDD is a directed acyclic graph in which every node has at most two outgoing edges. Each edge is labelled either 0 or 1. BDDs can be used to represent systems of Boolean equations. We treat the bits in the unknown factors p and q as variables, and then show how to build a BDD that represents the multiplication of p and q consistent with the known bits of N. The nodes in a BDD are arranged in levels where each level initially corresponds to one variable.

There are two basic operations we can perform on BDDs: swapping levels and adding levels. Adding levels results in levels being associated with linear combinations of variables, and not only single variables. Using these two operations we get linear combinations at each level, some of which are linearly dependent. Using the so-called linear absorption algorithm and reduction defined on BDDs, we can solve the inherent equation system $N = pq$, and thus find the unknown bits of p and q.

We show that the number of nodes in the initially constructed BDD is $\mathcal{O}(n^3)$ where n is the number of bits in p and q. Hence the multiplication of large RSA numbers that cannot be factored in practice can still be easily represented as a BDD. We have also run experiments to determine the complexity of the proposed factorization algorithm. The complexity we see is not as good as the best known methods, but our BDD representation is a radically different approach to the factorisation problem. The main contribution of this work is thus inspiration to look at the problem of integer factorization from a new angle.