

# Product Representations of Polynomials

Jacques Verstraëte

Department of Combinatorics and Optimization

University of Waterloo

200 University Avenue West

Waterloo, Ontario, Canada N2L 3G1.

`jverstraete@math.uwaterloo.ca`

## Abstract

The quadratic sieve is a randomized factoring algorithm which consists in finding, given an integer  $n$ , a square which is a product of positive integers of the form  $x^2 - n$ . In this talk, we discuss a more general framework of finding integer factorizations of points in the value set of a given polynomial. Our main result is to determine the asymptotic behaviour of the maximum size of a set  $A \subset \{1, 2, \dots, N\}$  such that no product of  $k$  distinct elements of  $A$  is in the value set of a given polynomial  $f$  of prime degree. The methods used include a little algebraic geometry, the probabilistic method and some extremal combinatorics, and generalize earlier results of Erdős (1963) and Erdős, Sós and A. Sárközy (1995). These results lead to algorithms for finding small linear dependences in a matrix over  $\mathbb{F}_q$  which are significantly faster than Gaussian elimination, and lead to new results on partial Steiner systems which are common to every Steiner system.