Journal of Symbolic Computation 64 (2014) 16–21

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

# Recovering a sum of two squares decomposition

Jaime Gutierrez [a,1], Álvar Ibeas [a,1], Antoine Joux [b,2]

[a] Dep. Matemática Aplicada y CC. Computación, Universidad de Cantabria, Spain
[b] Chaire de Cryptologie de la Fondation Partenariale de l'UPMC, UPMC/LIP6, UMR CNRS 7606, Inria Paris-Rocquencourt, France

ARTICLE INFO

*Article history:*
Received 29 November 2012
Accepted 9 October 2013
Available online 6 December 2013

*Keywords:*
Coppersmith method
Sum of squares

ABSTRACT

We present an algorithm that recovers a decomposition of an integer $N$ as sum of two squares from an approximation to one of the summands. It is based on Coppersmith's linearization technique which, applied directly to this problem, requires an approximation error smaller than $N^{1/6}$. Our algorithm performs a two-round linearization and allows approximation errors up to $N^{1/4}$.



## 1. Introduction

A well-known theorem of Fermat characterizes those integers which can be expressed as the sum of two squares. This property depends on the factorization of the integer, from which a sum of two squares decomposition (if exists) can be efficiently computed (Hardy et al., 1990). In this article we address the problem of recovering in polynomial time such a decomposition without access to the factorization, but from approximations to its summands. More generally, we look for integers $A, B$ such that $N = rA^2 + sB^2$; with the positive integers $N, r, s$ and approximations $A_0, B_0$ to $A$ and $B$ (respectively) as input data.

This task fits in the general setting in which small integer roots of a multivariate polynomial equation are searched for, which can be addressed using the linearization techniques introduced in Coppersmith (1997). We analyze the performance of these methods in terms of the size of the approximation errors which can be recovered, and present a combined technique which improves that error tolerance. In the setting we consider, both approximation errors are uniformly bounded by a single parameter $\Delta$. Note that, if we only have access to an approximation $A_0$ to one of the summands with maximum error $\Delta_A$, i.e. $A_0 - \Delta_A \leqslant A \leqslant A_0 + \Delta_A$; the other summand $B$ lies in the interval:

[1] Partially supported by the Spanish "Ministerio de Economía y Competitividad" grant MTM2011-24678.
[2] This research was done while the author was at the University of Versailles Saint-Quentin-en Yvelines.

0747-7171/$ – see front matter 
http://dx.doi.org/10.1016/j.jsc.2013.12.003

$$\left[\sqrt{\frac{N - r(A_0 + \Delta_A)^2}{s}}, \sqrt{\frac{N - r(A_0 - \Delta_A)^2}{s}}\right].$$

The approximation $B_0$ and maximum error $\Delta_B$ implicit in this expression satisfy $rA_0\Delta_A = sB_0\Delta_B$. This permits using the decomposition recovery results we prove (which require approximations to both summands) when only one approximation is given.

## 2. Background

Geometry of Numbers is the theory that deals with *lattices*, i.e., discrete subgroups of $(\mathbb{R}^m, +)$. The search of short elements in lattices is a key problem in this area and some interesting facts related to its computational complexity have been discovered, as the connection between the worst-case and the average-case complexity. The books (Gruber and Lekkerkerker, 1987; Micciancio and Goldwasser, 2002) are good examples of the vast literature dedicated to this theory, which has many applications in Computer Algebra and Cryptology.

Minkowski's Convex Body Theorem is a fundamental result in this theory, implying that in any lattice $\Lambda$ there is a nonzero element whose norm is upper bounded by $2(\Gamma(1 + n/2)\operatorname{vol}\Lambda)^{1/n}/\sqrt{\pi}$, where $\Gamma$ denotes the Euler Gamma function, $n$ is the lattice rank, and $\operatorname{vol}\Lambda$ its *volume*, i.e.

$$\lim_{t\to\infty} \frac{\operatorname{vol}_n(t)}{\#(\Lambda \cap B(t))},$$

being $B(t)$ the Euclidean ball of radius $t$ centered at the origin and $\operatorname{vol}_n(t)$ the volume of an $n$-dimensional Euclidean ball of radius $t$. The so-called *Gaussian heuristic* (Nguyen, 2010) assumes that the ratio above is a reasonable approximation to the lattice volume even for small $t$. We use this heuristic for the estimation of the performance of the simple linearization approach in Subsection 3.1. Namely, we might expect that a ball of radius significantly smaller than $(\operatorname{vol}\Lambda)^{1/n}$ does not contain more than three lattice elements: a nonzero one, its opposite, and the origin.

Every lattice is a free abelian group and can be described, therefore, by means of a basis, but not every basis is equally useful. In the case of lattices of rank two, optimization problems are efficiently solved using the following concept, implicit in Lagrange work (Lagrange, 1773), which was developed and popularized by Gauss (1966).

**Definition 1.** An ordered basis $(\mathbf{u}, \mathbf{v})$ of a lattice $\mathbb{Z}\langle\mathbf{u}, \mathbf{v}\rangle$ is called *reduced* if the following holds:

$$\|\mathbf{u}\| \leqslant \|\mathbf{v}\| \leqslant \|\mathbf{u} - \mathbf{v}\|, \|\mathbf{u} + \mathbf{v}\|.$$

There is a polynomial time algorithm which obtains a reduced basis for any two-rank lattice $\Lambda$. This basis contains the smallest nonzero lattice vector $\mathbf{u}$, and the smallest in $\Lambda\backslash\langle\mathbf{u}\rangle$ as well. On the other hand, a reduced basis of a lattice is as closest to orthogonal as possible. This gives the following result, which we will use in next section.

**Lemma 2.** *(See Gómez et al., 2006, Lemma 3.) Let $\{\mathbf{u}, \mathbf{v}\} \subset \mathbb{R}^m$ be a reduced basis of a two-rank lattice $\Lambda$ and $\mathbf{x} \in \Lambda$. For the unique pair of integers $(\alpha, \beta) \in \mathbb{Z}^2$ that satisfies $\mathbf{x} = \alpha\mathbf{u} + \beta\mathbf{v}$, we also have*:

$$\|\alpha\mathbf{u}\|, \|\beta\mathbf{v}\| \leqslant \frac{2}{\sqrt{3}}\|\mathbf{x}\|.$$

The neat reduction that Gauss' algorithm provides in the two-rank case is far from being obtained for general lattices. Several reduction definitions have been proposed, for which one has typically to choose between computational efficiency and good reduction parameters. The successful LLL algorithm (Lenstra et al., 1982) constitutes a good trade-off, computing in polynomial time a basis reduced enough for many applications. Among these, the linearization techniques introduced by Coppersmith (1997), which compute bounded integer roots of univariate polynomials over a residue ring or bivariate integer polynomials. More explicitly, in the second case: