Mathematics > Number Theory

An algorithm for list decoding number field codes

Jean-François Biasse, Guillaume Quintin

(Submitted on 12 Jul 2011 (v1), last revised 5 Apr 2012 (this version, v2))

We present an algorithm for list decoding codewords of algebraic number field codes in polynomial time. This is the first explicit procedure for decoding number field codes whose construction were previously described by Lenstra and Guruswami. We rely on an equivalent of the LLL reduction algorithm for $\OK$-modules due to Fieker and Stehl\'e and on algorithms due to Cohen for computing the Hermite normal form of matrices representing modules over Dedekind domains.

Subjects: **Number Theory (math.NT)**; Computational Complexity (cs.CC); Information Theory (cs.IT)

Cite as: **arXiv:1107.2321 [math.NT]**

(or **arXiv:1107.2321v2 [math.NT]** for this version)

Submission history

From: Jean-François Biasse [view email]

[v1] Tue, 12 Jul 2011 15:19:54 GMT (37kb)

[v2] Thu, 5 Apr 2012 17:16:43 GMT (85kb)

Which authors of this paper are endorsers?