Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Fault-tolerant modular reconstruction of rational numbers

John Abbott

Dipartimento di Matematica, Università di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

ARTICLE INFO

Article history:
Received 1 May 2015
Accepted 9 July 2016
Available online xxxx

MSC:
11A07
68W30

Keywords:
Fault-tolerant rational reconstruction
Chinese remaindering

ABSTRACT

In this paper we present two efficient methods for reconstructing a rational number from several residue-modulus pairs, some of which may be incorrect. One method is a natural generalization of that presented by Wang et al. in (Wang et al., 1982) (for reconstructing a rational number from *correct* modular images), and also of an algorithm presented in Abbott (1991) for reconstructing an *integer* value from several residue-modulus pairs, some of which may be incorrect. The other method is heuristic, but much easier to apply; it may be viewed as a generalization of Monagan's MQRR (Monagan, 2004). We compare our heuristic method with that of Böhm et al. (2015). Our method is clearly preferable when the rational to be reconstructed is unbalanced.

1. Introduction

The problem of intermediate expression swell is well-known in computer algebra, but has been greatly mitigated in many cases by the use of modular methods. There are two principal techniques: those based on the *Chinese Remainder Theorem*, and those based on *Hensel's Lemma*. In this paper we consider only the former approach.

Initially modular methods were used in cases where integer values were sought (*e.g.* for computing GCDs of polynomials with integer coefficients); the answer was obtained by a direct application of the Chinese Remainder Theorem. Then in 1981 Wang presented a method allowing the reconstruction of rational numbers (Wang, 1981) from their modular images: the original context was the computation of partial fraction decompositions. Wang's idea was justified in a later paper Wang et al. (1982)

E-mail address: abbott@dima.unige.it.

http://dx.doi.org/10.1016/j.jsc.2016.07.030
0747-7171/

which isolated the rational number reconstruction algorithm from the earlier paper. More recently, Collins and Encarnación (1994) corrected a mistake in Wang's paper, and described how to obtain an especially efficient implementation. Wang's method presupposes that all residue-modulus pairs are correct; consequently, the moduli used must all be coprime to the denominator of the rational to be reconstructed.

A well-known problem of modular methods is that of **bad reduction**: this means that the modular result is not correct for some reason. Sometimes it will be obvious when the modular result is bad or "relatively bad" (and these can be discarded), but other times it can be impractically hard to tell (*e.g.* in implicitization, see Abbott et al., 2016b); so we need a way to reconstruct the correct answer despite the possible presence of bad reductions. The *Continued Fraction Method*, an algorithm for the fault-tolerant reconstruction of integer values when some of the modular images may be bad was presented in Abbott (1991); apparently a very similar algorithm was implicit in Mandelbaum (1976).

In this paper we consider the problem of reconstructing a rational number from its modular images allowing for some of the modular images to be erroneous. We combine the corrected version of Wang's algorithm with the *Continued Fraction Method*. Our resulting new *FTRR* Algorithm (see section 4) reconstructs rational numbers from several modular images allowing some of them to be bad. The *FTRR* Algorithm contains both old methods as special cases: when it is known that all residues are correct we obtain Wang's corrected method, and if the denominator is restricted to being 1 then we obtain the original *Continued Fraction Method*. Finally, we note that the correction highlighted in Collins and Encarnación (1994) is a natural and integral part of our method.

Our *FTRR* Algorithm gives a strong guarantee on its result: if a suitable rational exists then it is unique and the algorithm will find it; conversely, if no valid rational exists then the algorithm says so. However, the uniqueness depends on bounds which must be given in input, including an upper bound for the number of incorrect residues. Since this information is often not known in advance, we present also the *HRR* Algorithm (see section 5) — it is a heuristic reconstruction technique based on the same principle as *FTRR*. This heuristic variant is much simpler to apply since it requires only the residue-modulus pairs as input. It will find the correct rational provided the correct modular images sufficiently outnumber the incorrect ones; if this is not the case then *HRR* will usually return an *indication of failure* but it may sometimes reconstruct an incorrect rational. *HRR* turns out to be a natural generalization of Monagan's MQRR (Monagan, 2004) for the heuristic reconstruction of rationals when all residue-modulus pairs are correct.

In section 6 we briefly compare our *HRR* algorithm with the *Error Tolerant Lifting* Algorithm presented in Böhm et al. (2015) which is based on lattice reduction, and which serves much the same purpose as *HRR*. We mention briefly also some combinatorial reconstruction schemes (presented in Abbott, 1991) which could be readily adapted to perform fault tolerant rational reconstruction, but are computationally significantly more costly.

In section 7 we present some approaches to fault-tolerant "rational vector reconstruction" (*i.e.* simultaneous reconstruction of several rationals). When there is a small common denominator the method with best overall modular cost is the "cascade method" using the *HRR* algorithm for each individual reconstruction; this approach is particularly well-suited to enabling the use of modular methods to solve the **hypersurface implicitization problem** (Abbott et al., 2016b): we know that there are only finitely many bad primes, but there is no reasonable way to detect them all *a priori*.

The perfect reconstruction algorithm would require only the minimum number of residue-modulus pairs (thus not wasting time on "redundant" iterations), and never reconstructs an incorrect rational (thus not wasting time checking "false positives"). Our *HRR* algorithm comes close to having both characteristics. Our variant of *ETL* from Böhm et al. (2015) also comes close to having both characteristics provided the rational to be reconstructed is balanced.

An anonymous referee pointed out that Pernet's *Mémoire d'habilitation à diriger des recherches* (Pernet, 2014) includes a brief consideration of fault-tolerant rational reconstruction in the context of error-correcting codes (see section 2.5 of that document).

Please cite this article in press as: Abbott, J. Fault-tolerant modular reconstruction of rational numbers. J. Symb. Comput. (2016), http://dx.doi.org/10.1016/j.jsc.2016.07.030