Solving Systems of Linear Congruences

Andreas Dolzmann*and Thomas Sturm†
FMI, University of Passau, Germany

MIP-0101
February 2, 2001

Abstract

Based on an extended quantifier elimination procedure for discretely valued fields, we devise algorithms for solving multivariate systems of linear congruences over the integers. This includes determining integer solutions for sets of moduli which are all power of a fixed prime, uniform p-adic integer solutions for parametric prime power moduli, lifting strategies for these uniform p-adic solutions for given primes, and simultaneous lifting strategies for finite sets of primes. The method is finally extended to arbitrary moduli.

*`dolzmann@uni-passau.de`, `http://www.fmi.uni-passau.de/~dolzmann/`
†`sturm@uni-passau.de`, `http://www.fmi.uni-passau.de/~sturm/`

1 Introduction

We devise methods for testing multivariate systems of linear congruences for feasibility. In the positive case we obtain at least one sample solution for the system. Our methods allow to prescribe for each constraint a particular modulus in contrast to having only one modulus for the entire system:

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &\equiv b_1 \mod \mu_1 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &\equiv b_m \mod \mu_m, \end{aligned}$$

where $a_{ij} \in \mathbb{Z}$. In the easiest case, $\mu_1, \ldots, \mu_m$ are various powers of a fixed prime number p:

$$\mu_1 = p^{k_1}, \quad \ldots, \quad \mu_m = p^{k_m}.$$

We then extended our approach to a parametric p, which stands for an arbitrary prime. Finally, we can apply the methods derived for such a parametric p to the general situation where

$$\mu_1, \quad \ldots, \quad \mu_m \in \{2, 3, 4, \ldots\}.$$

This is an important multivariate generalization of the problem solved by one of the key algorithms in computer algebra: The Chinese Remainder Theorem, which states the feasibility and gives a solution procedure for the special case where the $\mu_1, \ldots, \mu_m$ are pairwise relatively prime, and there is only one variable with coefficient 1, i.e.,

$$n = 1, \quad a_{11} = \cdots = a_{m1} = 1.$$

See Theorem 12 for details.

Our method will reduce the problem of solving such systems to one or several *extended quantifier elimination* problems over the rational numbers with p-adic valuations. The obtained p-adic integer sample solutions are then lifted to the integers. Similar extended quantifier elimination procedures have been successfully applied for constraint solving over the reals [DSW98, Stu99].

The complexity of our methods is dominated by the complexity of the extended quantifier elimination procedure. This is single exponential in the number of variables but only polynomial in the number of congruences.

The plan of the paper is as follows: In Section 2 we recall some basic facts about p-adically valued fields, in which we compute our solutions before lifting them to the integers. In Section 3 we describe the connection between p-adic solving and integer solving. In Section 4 we give an overview on our method for the p-adic solving step which is extended quantifier elimination. Quantifier elimination procedures operate on first-order formulas. Section 5 explains how to obtain a suitable input formula for a system of linear congruences. One crucial advantage of quantifier elimination procedures for solving is that they can process parametric input in a very natural way. Section 6 exhibits how to exploit this for linear congruence systems with parametric moduli. We can then obtain p-adic, i.e. unlifted, solutions that are, up to a finite case distinction, uniformly correct for all possible choices of primes. We also demonstrate the theoretical limits for such uniform solving. In Section 7, we explain how and to what extent also the lifting step from our uniform p-adic solutions to integer solutions can be performed uniformly. The methods developed here for the simultaneous lifting for finite sets of primes allow us to finally extend our method to congruence systems to arbitrary, i.e. not necessarily prime, moduli. This is described in Section 8. The conclusions in Section 9 summarize and evaluate our results.

All methods and algorithms discussed here are efficiently implemented within the widespread computer algebra system REDUCE, based on the package REDLOG [DS97b] by the authors. All our computations have been performed using 32 MB Lisp heap on an 800 MHz Athlon PC running Linux.

2 P-adic Valuations

For a given prime p, the p-adic *valuation* on the rational numbers is a map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$, where

$$\begin{aligned} v_p(0) &= \infty \\ v_p(r/s) &= \max\{\, n \in \mathbb{N} : p^n \mid r \,\} - \max\{\, n \in \mathbb{N} : p^n \mid s \,\}. \end{aligned}$$

Such valuations have the following properties: $v(a) = \infty$ if and only if $a = 0$, and

$$v(ab) = v(a) + v(b), \quad v(a+b) \geq \min\{v(a), v(b)\}.$$

It follows that $v(a+b) = \min\{v(a), v(b)\}$ if $v(a) \neq v(b)$. This fact is referred to as the *ultra-metric triangle equality.* Note that for $z \in \mathbb{Z}$ we have $v_p(p^z) = z$, i.e., v_p is onto. Due to a famous theorem by Ostrowski [Ost18] the p-adic valuations are essentially the only maps with these properties.

The elements of non-negative value form a ring, the *valuation ring*

$$\mathbb{Z}_p = \{\, r/s \in \mathbb{Q} : \gcd(r, s) = 1 \text{ and } p \nmid s \,\}.$$

The elements of $\mathbb{Z}_p$ are called the *p-adic integers.* In $\mathbb{Z}_p$ the elements of positive value form a maximal ideal, the *valuation ideal* $p\mathbb{Z}_p$, which is the only maximal ideal in $\mathbb{Z}_p$. The elements $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ form the multiplicative group of units of $\mathbb{Z}_p$:

$$\begin{aligned} p\mathbb{Z}_p &= \{\, r/s \in \mathbb{Q} : \gcd(r,s) = 1 \text{ and } p \mid r \,\} \\ \mathbb{Z}_p \setminus p\mathbb{Z}_p &= \{\, r/s \in \mathbb{Q} : \gcd(r,s) = 1,\ p \nmid r \text{ and } p \nmid s \,\}. \end{aligned}$$

From the maximality of $p\mathbb{Z}_p$ it follows that $\mathbb{Z}_p/p\mathbb{Z}_p$ is a field, the *residue class field* wrt. v_p. Up to isomorphism, this residue class field is particularly simple:

$$\mathbb{Z}_p/p\mathbb{Z}_p = (\mathbb{Z} + p\mathbb{Z}_p)/p\mathbb{Z}_p \simeq \mathbb{Z}/(\mathbb{Z} \cap p\mathbb{Z}_p) = \mathbb{Z}/p\mathbb{Z}.$$

All ideals in the ring $\mathbb{Z}_p$ of p-adic integers are of the form

$$\begin{aligned} p^k\mathbb{Z}_p &= \{\, x \in \mathbb{Z}_p : v_p(x) \geq k \,\} \\ &= \{\, r/s \in \mathbb{Q} : \gcd(r,s) = 1,\ p^k \mid r \,\} \qquad (k \in \mathbb{N}). \end{aligned}$$

A valuation can be essentially recovered from its valuation ring. To avoid a two-sorted language, we may thus drop the information about the concrete values by using the language of rings together with *abstract divisibilities.* These divisibilities express ordering relations in the value group $\mathbb{Z}$ by relating rational numbers:

$$\begin{aligned} x \mid y \ &:\longleftrightarrow\ v(x) \leq v(y) \\ x \sim y \ &:\longleftrightarrow\ v(x) = v(y) \\ x \not\sim y \ &:\longleftrightarrow\ v(x) \neq v(y). \end{aligned}$$

We furthermore add a constant π of value 1 to our language, which is interpreted as the p of our p-adic valuation. Note that our language does not include reciprocals. For convenience, we allow ourselves to identify terms with polynomials in $\mathbb{Z}[\mathbf{x}, \pi]$ where $\mathbf{x} = (x_1, \ldots, x_n)$ are the contained variables, and π is the constant of our language.

3 Solving Congruences

In the previous section we have introduced the valuation rings $\mathbb{Z}_p$ wrt. p-adic valuations on the rational numbers. We have demonstrated that these rings have a particularly nice algebraic structure, which suggests that they admit sophisticated algebraic methods for solving. We are going to focus on such methods in the following section, after here making clear the connection between solving over $\mathbb{Z}_p$ on one hand, and solving over the integers, which we are actually interested in, on the other hand.

The following lemma shows that p-adic solutions can easily be lifted to integer solutions, while integer solution are themselves already p-adic solutions.

Lemma 1 *Let $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ be polynomials that are linear in $x_1, \ldots, x_n$. Let p be prime, and let $k_1, \ldots, k_m \in \mathbb{N}$. Consider the following systems S and S' of congruences over $\mathbb{Z}$ and $\mathbb{Z}_p$, respectively:*

$$\begin{aligned} S &= \{ f_j(\mathbf{x}) \equiv 0 \bmod p^{k_j}\mathbb{Z} : 1 \leq j \leq m \} \\ S' &= \{ f_j(\mathbf{x}) \equiv 0 \bmod p^{k_j}\mathbb{Z}_p : 1 \leq j \leq m \}. \end{aligned}$$

Then S has a solution $\mathbf{a} \in \mathbb{Z}^n$ iff S' has a solution $\mathbf{a}' \in \mathbb{Z}_p^n$. More precisely, every solution $\mathbf{a} \in \mathbb{Z}^n$ for S is already a solution for S', and every solution $\mathbf{a}' \in \mathbb{Z}_p^n$ for S' can be easily lifted to a solution $\overline{\mathbf{a}'}$ for S in $\mathbb{Z}^n$.

Proof To begin with, observe that $\mathbb{Z}$ is a subring of $\mathbb{Z}_p$, and that for our p, $k_1, \ldots, k_m$, the corresponding ideals $p^{k_j}\mathbb{Z}$ are exactly the restrictions of the ideals $p^{k_j}\mathbb{Z}_p$; more precisely

$$p^{k_j}\mathbb{Z} = p^{k_j}\mathbb{Z}_p \cap \mathbb{Z} \subseteq p^{k_j}\mathbb{Z}_p \quad (1 \leq j \leq m).$$

Let now $\mathbf{a}$ be a solution for S over $\mathbb{Z}$. Then $f_j(\mathbf{a}) \equiv 0 \bmod p^{k_j}\mathbb{Z}$ corresponding to $f_j(\mathbf{a}) \in p^{k_j}\mathbb{Z}$ implies $f_j(\mathbf{a}) \in p^{k_j}\mathbb{Z}_p$, which in turn corresponds to $f_j(\mathbf{a}) \equiv 0 \bmod p^{k_j}\mathbb{Z}_p$.

Let vice versa $\mathbf{a}' = (r_1/s_1, \ldots, r_n/s_n) \in \mathbb{Z}_p^n$ be a solution for S'. Let $k = \max\{k_1, \ldots, k_m\}$. We restrict our attention to r_1/s_1. This is a p-adic integer, and thus s_1 is relatively prime to p. We compute using the extended Euclidean algorithm a multiplicative inverse $\overline{s_1}$ of s in $\mathbb{Z}/p^k$:

$$1 = \gcd(s_1, p^k) = \overline{s_1}s_1 + xp^k,$$

i.e., $\overline{s_1}s_1 \equiv 1 \bmod p^k\mathbb{Z}$ over $\mathbb{Z}$, and certainly $\overline{s_1}s_1 \equiv 1 \bmod p^k\mathbb{Z}_p$ over $\mathbb{Z}_p$. Moreover, the corresponding congruences obviously hold for all $k_1, \ldots, k_m$. This means that $r_1 s_1 \overline{s_1}/s_1 = r_1\overline{s_1}$ constitutes an integer solution for x_1 that is congruent to r_1/s_1 wrt. all the $p^{k_1}\mathbb{Z}_p, \ldots, p^{k_m}\mathbb{Z}_p$. We set $\overline{a_1'} = r_1\overline{s_1}$ and applying our method to the other coordinates, we obtain a complete integer solution $\overline{\mathbf{a}'}$ for S' over $\mathbb{Z}_p$. According to our initial observations, this $\overline{\mathbf{a}'}$ is obviously a solution for S over $\mathbb{Z}$.

Although we use to speak of integer solutions, it is also quite natural to consider these solutions as elements in $(\mathbb{Z}/p^k)^n$, where k is the highest power of p in S. Viewed in this way, the solutions obtained by the lifting procedure in the proof of Lemma 1 will in general not be the canonical representatives, i.e., we have to expect to obtain integers $x_i = \overline{a_i'} \geq p^k$. We can however easily derive from any such solution another solution, which is well-behaved.

Lemma 2 *Let S be a system of linear congruence as in Lemma 1, and let $\mathbf{a} \in \mathbb{Z}^n$ be an integer solution for S. Let $k = \max\{k_1, \dots, k_m\}$. Then all elements of $\mathbf{a} + (p^k\mathbb{Z})^n$ are integer solutions of S. In particular there is one solution $\mathbf{c} = (c_1, \dots, c_n) \in \mathbf{a} + (p^k\mathbb{Z})^n$ with $0 \le c_i < p^k$ for $i \in \{1, \dots, n\}$.*

Proof Our $\mathbf{a} = (a_1, \dots, a_n)$ solves S if and only if it solves for $j \in \{1, \dots, m\}$ the equation $f_j = 0$ over $\mathbb{Z}/p^{k_j}\mathbb{Z}$. Let $\mathbf{b} \in (p^k\mathbb{Z})^n$. Then $\mathbf{b} = 0$ in $(\mathbb{Z}/p^{k_j}\mathbb{Z})^n$, and thus $\mathbf{a} + \mathbf{b} = \mathbf{a}$ is a solution of $f_j = 0$ over $\mathbb{Z}/p^{k_j}\mathbb{Z}$. Accordingly, for $i \in \{1, \dots, n\}$ we can obtain c_i by division with positive remainder of a_i by p^k.

It is not hard to see that $\mathbf{a} + (p^k\mathbb{Z})^n$ in Lemma 2 does not describe the complete solution space of S. As an example consider the system

$$5x_1 + 7x_2 + 1 \equiv 0 \bmod 11.$$

Here $(5, 1)$ is a solution, but so is also $(-3, 2) \notin (5, 1) + (11\mathbb{Z})^2$.

4 Extended Quantifier Elimination

For solving our linear constraints, we use an effective linear quantifier elimination procedure based on *virtual substitution of test points.* Based on ideas of Ferrante and Rackoff [FR79] for decision problems, virtual substitution methods for quantifier elimination date back to a theoretical paper by Weispfenning [Wei88]. Corresponding methods over the reals have been successfully used for solving problems from numerous areas in science and engineering [DSW98].

For eliminating the quantifiers from an input formula

$$\varphi(u_1, \dots, u_m) \equiv \mathsf{Q}_1 x_1 \dots \mathsf{Q}_n x_n \psi(u_1, \dots, u_m, x_1, \dots, x_n)$$

where $\mathsf{Q}_i \in \{\exists, \forall\}$, the elimination starts with the innermost quantifier regarding the other quantified variables within ψ as extra parameters. Universal quantifiers are handled by means of the equivalence $\forall x \psi \longleftrightarrow \neg\exists x \neg\psi$. We may thus restrict our attention to a formula of the form

$$\varphi^*(u_1, \dots, u_k) \equiv \exists x \psi^*(u_1, \dots, u_k, x),$$

where the $u_{m+1}, \dots, u_k$ are actually x_i quantified from further outside. The idea is now to find a finite *elimination set E* of terms in $u_1, \dots, u_k$ such that

$$\exists x \psi^*(u_1, \dots, u_k, x) \equiv \bigvee_{t \in E} \psi^*[x/t](u_1, \dots, u_k).$$

That is, the above disjunction is a quantifier-free equivalent for φ^*. Note that it is not necessary to perform any transformation on the boolean structure of ψ^*. The elimination method is single exponential in the number of quantified variables, and double exponential in the number of quantifier blocks. It has turned out suitable for parallelization [DGS98].

By keeping track of the terms t substituted during the elimination process, we obtain instead of a quantifier-free equivalent $\bigvee_{i=1}^{k} \psi^*[x/t_i]$ a guarded expression [DS97a]

$$\begin{bmatrix} \psi^*[x/t_1] & x = t_1 \\ \vdots & \vdots \\ \psi^*[x/t_k] & x = t_k \end{bmatrix}$$

including satisfying sample points. This process of *extended quantifier elimination* can also be repeated for several existential quantifiers. The result then is a set of conditions each associated with an answer for each eliminated variable obtained by back-substitution.

The construction of elimination sets for linear formulas in valued fields has been described by the second author [Stu00]. Before, Weispfenning had given elimination sets for special cases of valued fields including the case of p-adic valuations [Wei88]. Necessary simplification strategies and implementation issues have been discussed in [DS99].

The existence of a quantifier elimination procedure for the general case including non-linear formulas has been shown independently by Ax and Kochen [AK66] and Ershov [Ers65]. The first explicit procedure has been given by Cohen [Coh69]. Considerable progress has been made by Macintyre [Mac76] turning to a more reasonable language including root predicates in analogy to the reals. This has been made explicit by Weispfenning [Wei84].

5 Solving by Extended Quantifier Elimination

We consider for $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ linear, p prime, and $k_1, \ldots, k_m \in \mathbb{N}$, a system of congruences

$$S = \{f_1(\mathbf{x}) \equiv 0 \bmod p^{k_1}\mathbb{Z}, \ \ldots, \ f_m(\mathbf{x}) \equiv 0 \bmod p^{k_m}\mathbb{Z}\}.$$

According to Lemma 1 it suffices to solve instead the corresponding system

$$S = \{f_1(\mathbf{x}) \equiv 0 \bmod p^{k_1}\mathbb{Z}_p, \ \ldots, \ f_m(\mathbf{x}) \equiv 0 \bmod p^{k_m}\mathbb{Z}_p\}.$$

over $\mathbb{Z}_p$. The solvability of this new system S' can be expressed by a first order formula as follows:

$$\Phi(S') \equiv \exists x_1 \cdots \exists x_n \Big(\bigwedge_{i=1}^{n} 1 \mid x_i \wedge \bigwedge_{j=1}^{m} p^{k_j} \mid f_j(x_1, \dots, x_n) \Big).$$

Here, the first conjunction restricts the x_i to be in the valuation ring $\mathbb{Z}_p$. Extended quantifier elimination applied to this formula will decide feasibility and, in the positive case, yield one sample solution. Our notion of *solving* thus resembles the standard notion used in constraint solving. Recall from Lemma 2 that in our situation such a sample solution even describes an infinite subset of the solution space.

Algorithm 3 (Solving Integer Congruences)
Input: A system

$$S = \{ f_j(\mathbf{x}) \equiv 0 \bmod p^{k_j}\mathbb{Z} : 1 \le j \le m \}.$$

of congruences over $\mathbb{Z}$ with $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$ linear, p prime, and $k_1, \dots, k_m \in \mathbb{N}$.
Output: "infeasible," or a sample solution $\mathbf{c} = (c_1, \dots, c_n)$ over $\mathbb{Z}$ for S with $0 \le c_i < p^{\max\{k_1,\dots,k_m\}}$ for $i \in \{1, \dots, n\}$.

1. Change from S to S' according to Lemma 1
2. Generate from S' the first-order formula $\Phi(S')$ as described above
3. Apply extended quantifier elimination to $\Phi(S')$
4. (a) if the elimination result is false then return "infeasible"
   (b) else lift the solution $\mathbf{a}' \in \mathbb{Z}_p^n$ to a solution $\mathbf{a} \in \mathbb{Z}^n$ according to Lemma 1
5. Apply Lemma 2 to derive from $\mathbf{a}$ a solution

$$\mathbf{c} = (c_1, \dots, c_n),$$

   where $0 \le c_i < p^{\max\{k_1,\dots,k_m\}}$ for $i \in \{1, \dots, n\}$.

Proof The correctness follows from Lemma 1, Lemma 2, the definition of extended quantifier elimination, and the correspondence between S' and $\Phi(S')$ discussed above.

In our algorithm, the quantifier elimination step (3) constitutes due to the particular form of $\Phi(S')$ an extreme special case of p-adic quantifier elimination. From the elimination point of view, the crucial syntactic feature of $\Phi(S')$ is that all the x_i occur only on the right hand sides of the abstract divisibilities. That is, we only impose lower bounds on the values of these x_i but no upper bounds.

Restating the elimination procedure given in [Stu00] for this special case in our congruence framework, the p-adic solutions will be determined as follows.

Definition 4 For a congruence $\gamma = f(\mathbf{x}) \equiv 0 \bmod I$ we denote by $\gamma^{(=)}$ the corresponding equation $f(\mathbf{x}) = 0$. This naturally extends to the notion of a system $S^{(=)}$ of equations corresponding to a system S of congruences.

Algorithm 5 (Deciding p-adic Congruences)
Input: A system

$$S' = \{\, f_j(\mathbf{x}) \equiv 0 \bmod p^{k_j}\mathbb{Z}_p : 1 \le j \le m \,\}$$

of congruences over $\mathbb{Z}$ with $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ linear, p prime.
Output: “infeasible,” or a sample solution $\mathbf{a}' \in \mathbb{Z}_p^n$ for S'.

BEGIN
    $\mathcal{S} := \{(S', \emptyset)\}$
    $\mathcal{S}' := \emptyset$
    for each variable $x \in \{x_1, \ldots, x_n\}$ **do**
        for each $(S, \sigma) \in \mathcal{S}$ **do**
            for each constraint γ in S **do**
                if γ contains x **then**
                    $a :=$ solution in $\mathbb{Q}$ wrt. x for $\gamma^{(=)}$
                    $S_a := S$ with a plugged in for x
                    $\mathcal{S}' := \mathcal{S}' \cup \{(S_a, \sigma \cup \{x = a\})\}$
                fi
            od
            $S_0 := S$ with 0 plugged in for x
            $\mathcal{S}' := \mathcal{S}' \cup \{(S_0, \sigma \cup \{x = 0\})\}$
        od
        $\mathcal{S} := \mathcal{S}'$
        $\mathcal{S}' := \emptyset$
    od
    if there is $(\{0 \equiv 0, \ldots, 0 \equiv 0\}, \sigma)$ in $\mathcal{S}$ **then**
        return σ
    else

return "infeasible"
fi
END

Proof This is a straightforward consequence of Corollary 8.5 in [Stu00] applied to $\Phi(S')$.

Example 6 We apply our implementation of Algorithm 3 to the following randomly generated system S of congruences:

$$\begin{aligned}
70x_1 + 6x_3 + 89x_4 + 7x_6 + 30 &\equiv 0 \quad \bmod \quad 103^{10}\\
87x_1 + 93x_2 + 78x_3 + 73x_4 + 53 &\equiv 0 \quad \bmod \quad 103^{9}\\
87x_2 + 41x_5 + 3 &\equiv 0 \quad \bmod \quad 103^{3}\\
12x_2 + 37x_3 + 69x_4 + 15x_6 + 53 &\equiv 0 \quad \bmod \quad 103^{3}\\
75x_1 + 90x_3 + 65x_4 + 14x_5 + 41 &\equiv 0 \quad \bmod \quad 103\\
91x_5 + 96x_6 + 55 &\equiv 0 \quad \bmod \quad 103^{2}.
\end{aligned}$$

Extended quantifier elimination applied to $\Phi(S')$ yields the following sample solution over $\mathbb{Z}_{103}$ for S':

$$\begin{aligned}
x_1 &= \frac{1120921235}{6450196079}, & x_2 &= -\frac{2555928514}{19350588237},\\
x_3 &= -\frac{2265478209}{6450196079}, & x_4 &= -\frac{2512869252}{6450196079},\\
x_5 &= \frac{1335886309}{6450196079}, & x_6 &= -\frac{4961733734}{6450196079}.
\end{aligned}$$

After lifting this results in the following corresponding sample solution for the original system S over $\mathbb{Z}$:

$$\begin{aligned}
x_1 &= 18804386104945290509\\
x_2 &= 8303843175527713857\\
x_3 &= 6309069755640464645 6\\
x_4 &= 8369658051489505641 5\\
x_5 &= 9382637398778301034 4\\
x_6 &= 13364656665295088119 2.
\end{aligned}$$

The total computation time is 2.3 s, which is almost completely spent for the extended quantifier elimination step. All other steps, in particular the lifting, take less than the accuracy of the system clock, which is 0.01 s.

6 Parametric Moduli

So far, we have considered integer congruence systems with prime power moduli for a fixed prime p. Algorithm 5 suggests that the first-order framework of quantifier elimination is not necessary for solving this problem. The entire elimination procedure can easily be described in terms of manipulating lists of congruence systems. This changes when turning to more general questions. The first more general problem we are going to discuss here, is solving our congruence systems uniformly for a parametric prime p.

Let us take a look at our Algorithm 3 wrt. this generalization:

1. The p-adic system S' can be generated as before now containing parametric ideals $p^{k_j}\mathbb{Z}_p$.

2. The first-order formula $\Phi(S')$ now contains the constant π of our language denoting the parametric p.

3. The extended quantifier elimination is now not a decision procedure. Notice that variable-free atomic formulas cannot be decided. For our generalized Algorithm 5 this means that we drop the final **if** statement but return the extended quantifier elimination result. The conditions in this result will contain two types of atomic conditions:

   (a) Positive conditions on p resulting from the substitution into the congruences.

   (b) Negative conditions on p, which are guarding conditions introduced with substitution for excluding zero denominators.

4/5. The lifting step depends on the concrete choice for p, and has to be considered separate from the p-adic solution phase. The p-adic solution provided by the generalized Algorithm 5 will thus be the final output of our generalized Algorithm 3.

Example 7 We recompute our Example 6 replacing the base 103 of the moduli by a parametric p. We then obtain after 7.43 s the following solution, which is uniform over $\mathbb{Z}_p$ for the valid moduli $p \notin \{3, 6450196079\}$:

$$\left[\ 3 \sim 1 \wedge 6450196079 \sim 1 \quad \mathbf{a}'\ \right],$$

where the p-adic integer solution $\mathbf{a}'$ happens to be identical to that for the case $p = 103$ in Example 6. Our $\mathbf{a}'$ can be lifted e.g. for $p = 103$ within less then 0.01 s to the integer solution we know from Example 6.

Notice that we have found in the above example a uniform p-adic solution, subject to a guarding condition that straightforwardly states that the system is unsolvable for $p \in \{3, 6450196079\}$.

The remainder of this section is devoted to studying what kind of results concerning uniformity and explicitness we may expect wrt. the stated problem on one hand, and our particular approach to it on the other hand.

Example 8 Consider the following system of two congruences:

$$\begin{aligned} 3x_1 + 5x_2 &\equiv 1 \mod p \\ 5x_1 + 3x_2 &\equiv 1 \mod p. \end{aligned}$$

Our elimination procedure yields the following result distinguishing two cases:

$$\left[\begin{array}{ll} 2 \not\sim 1 & \{x_1 = \frac{1}{3}, \quad x_2 = 0\} \\ 2 \sim 1 & \{x_1 = \frac{1}{8}, \quad x_2 = \frac{1}{8}\} \end{array} \right].$$

With the result in the example, we would for $p = 2$ be only allowed to lift the first solution, while for all other primes p only the second one is valid. Since we have to know p for lifting anyway, it is easy to automatically detect the correct branch. Anyway, the question arises whether there exists also a uniform solution, which we would consider an intermediate result of better quality. This is in fact not the case here as we going to exhibit in the sequel.

To begin with, note that by inspection of our elimination procedure, we know that our sample solutions will always be numbers not involving the constant $\pi = p$ of our language.

Lemma 9 *A rational number a is a p-adic integer for all primes p if and only if it is an integer. In other words,*

$$\bigcap_{p \text{ prime}} \mathbb{Z}_p = \mathbb{Z}.$$

Proof Let $a = n/d \in \bigcap_p \mathbb{Z}_p$ be reduced to lowest terms. Then $p \nmid d$ for all primes p. It follows that $d = 1$ and thus $a \in \mathbb{Z}$. Let conversely $a = a/1 \in \mathbb{Z}$, and let p be prime. Then $p \nmid 1$ and thus $a \in \mathbb{Z}_p$.

Let now S be a system of congruences with parametric modulus base p over $\mathbb{Z}$. Denote by S' the corresponding system over $\mathbb{Z}_p$ as made precise in Lemma 1, and by $S^{(=)}$ the corresponding system of equations according to Definition 4.

We learn from Lemma 9 above that a uniform p-adic integer solution for S' is in fact a uniform integer solution for S' and thus also for S. By choosing

p sufficiently large, it is not hard to see that this uniform integer solution even solves the corresponding system $S^{(=)}$ of linear equations. Conversely, any integer solution for $S^{(=)}$ is obviously a uniform integer solution for S and thus for S'. The following proposition states this observation more concisely:

Proposition 10 *Let S be a system of linear congruences over $\mathbb{Z}$, let S' be the corresponding system over $\mathbb{Z}_p$, and let $S^{(=)}$ be the corresponding system of linear equations over $\mathbb{Z}$. Assume we determine a (uniform) solution* $\mathbf{a}$ *for one of these three systems. Then* $\mathbf{a}$ *is up to some natural homomorphism also a (uniform) solution for the other two systems.*

Consider now the system of equations over $\mathbb{Z}$ corresponding to the congruence system in Example 8:

$$\begin{aligned} 3x_1 + 5x_2 &= 1 \\ 5x_1 + 3x_2 &= 1. \end{aligned}$$

Subtracting the first equation from the second one, we obtain the consequence $x_1 = x_2$. A solution $x_1 = x_2 = a \in \mathbb{Z}$ would thus have to satisfy $8a = 3a + 5a = 1$, which is obviously impossible. Proposition 10 now tells us that there is no uniform solution for the original congruence system, neither over $\mathbb{Z}$ nor over $\mathbb{Z}_p$. Concerning the case distinction, our solution in Example 8 is optimal.

Our procedure is however not optimal in general. In the following example we miss finding a uniform solution, although there exists one.

Example 11 Consider the system consisting of the sole congruence

$$5x_1 + 7x_2 + 1 \equiv 0 \bmod p.$$

Application of our elimination procedure yields that this is solvable for all primes p, giving two guarded sample solutions. The first one holds uniformly, except for $p = 5$, while the second one holds uniformly except for $p = 7$:

$$\begin{bmatrix} 5 \sim 1 & \{x_1 = -\frac{1}{5}, & x_2 = 0\} \\ 7 \sim 1 & \{x_1 = 0, & x_2 = -\frac{1}{7}\} \end{bmatrix}.$$

Here $x_1 = -3$ and $x_2 = 2$ solves the corresponding system of equations over $\mathbb{Z}$, and thus constitutes a uniform solution for all p.

In the non-parametric case we could obviously easily obtain either "true" or "false" for each guarding condition, and then pick a "true" solution. In the parametric case here, we have seen conditions of the form $p \sim 1$ and $p \not\sim 1$ for primes p.

In fact, every variable-free formula over our language is simplified to "true," "false," or a formula of one of the forms

$$p_1 \not\sim 1 \vee \cdots \vee p_k \not\sim 1, \quad p_1 \sim 1 \wedge \cdots \wedge p_k \sim 1,$$

where $p_1 < \cdots < p_k$ prime. The first formula states $p \in \{p_1, \ldots, p_k\}$, while the second one states $p \notin \{p_1, \ldots, p_k\}$. We observe, as a consequence, that any parametric congruence system of our considered form is of one of the following four types:

1. generally feasible for all primes p,
2. generally infeasible for all primes p,
3. feasible for finitely many p,
4. feasible for all but finitely many p.

In particular, there is no such system for which there exists a partition $P_1 \dot\cup P_2$ of all primes into infinite sets P_1 and P_2, such that the system is feasible for all $p \in P_1$ but infeasible for all $p \in P_2$.

Guarding conditions of the form $p_1 \not\sim 1 \vee \cdots \vee p_k \not\sim 1$ restricting p to a finite set of primes are typically introduced because the congruence system degenerates for these primes. For instance $p_1, \ldots, p_k$ may be the prime factors of a certain coefficient, which becomes zero then, which in turn leads to a special solution that does not work for other primes. Guards of the form $p_1 \sim 1 \wedge \cdots \wedge p_k \sim 1$, in contrast, exclude, as a rule, the prime factors of the denominators of the associated solution.

Arriving from an arbitrary variable-free formula over our language, which possibly contains the constant π, at one of the four forms described above is by no means trivial. It requires a large arsenal of sophisticated simplification strategies. The part of our simplifier that is of general interest for quantifier elimination over discretely valued fields has been described in detail in [DS99]. Further special-purpose simplification algorithms have been added for the particular project discussed here.

7 Simultaneous Lifting

With the parametric setup of the previous section it is possible to lift the p-adic solutions simultaneously for finitely many primes p. The crucial tool for this is the well-known *Chinese Remainder Theorem* (CRT) [BWK93].

Theorem 12 (Chinese Remaindering) *Let* $r_1, \ldots, r_k, m_1, \ldots, m_k \in \mathbb{Z}$*, where the* m_i *are relatively prime. We are interested in the system*

$$S = \{\, x \equiv r_i \bmod m_i \mid 1 \leq i \leq k \,\}$$

of congruences. For $1 \leq i \leq k$ *set*

$$n_i = \prod_{\substack{1 \leq j \leq k \\ j \neq i}} m_i.$$

Then $\gcd(n_i, m_i) = 1$*, and the extended Euclidean algorithm yields a linear combination* $1 = s_i n_i + t_i m_i$*. Now*

$$a = \sum_{j=1}^{k} n_j s_j r_j$$

is a solution to the system S*. The set of all solutions is* $a + m\mathbb{Z}$*, where* $m = m_1 \cdots m_k$*.*

7.1 Simultaneous Branch Lifting

Consider now for a congruence system S with symbolic p a solution branch

$$(\gamma, \{x_1 = \tfrac{r_1}{s_1}, \ldots, x_n = \tfrac{r_n}{s_n}\}).$$

Let k be the highest power of p in S, and let $P = \{p_1, \ldots, p_l\}$ be a finite set of primes satisfying γ. We are going to apply the Chinese Remainder Theorem for obtaining an integer solution that is simultaneously correct for all the $p_1, \ldots, p_l$, by solving for each of the r_i/s_i the following system of integer congruences:

$$\begin{aligned} y &\equiv 1 \quad \bmod \quad p_1^k \\ &\;\;\vdots \\ y &\equiv 1 \quad \bmod \quad p_l^k \\ y &\equiv 0 \quad \bmod \quad s_i. \end{aligned}$$

All the k-th powers of the various p_j are obviously pairwise relatively prime, and since the p_j satisfy γ, they are also relatively prime to s_i. The first l congruences allow us to multiply r_i/s_i with our solution a for y without changing its residue class modulo any of the ideals $p^k\mathbb{Z}_p$ for the various p_1, $\ldots$, p_l, and that $a \not\equiv 0$. The last congruence makes sure that a will be a multiple of s_i, such that $r_i a/s_i \in \mathbb{Z}$.

Example 13 For our Example 7 we had obtained a uniform result for $p \notin \{3, 6450196079\}$, which we simultaneously lift:

(i) For the first ten primes $\{2, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$ different from 3, we obtain after 0.01 s a uniform integer solution where $x_1, \ldots, x_6$ have either 93 or 94 digits each.

(ii) For the first 100 primes $\{2, \ldots, 547\}$ different from 3, we obtain after 0.79 s a uniform integer solution where $x_1, \ldots, x_6$ have 2192 digits each.

(iii) For the first 500 primes $\{2, \ldots, 3581\}$ different from 3, we obtain after 31.5 s a uniform integer solution where $x_1, \ldots, x_6$ have either 15228 or 15229 digits each.

7.2 Simultaneous Solution Lifting

Simultaneous branch lifting is applicable only in cases where the list of target primes matches one particular solution branch. This will be in general not be the case as we have demonstrated for our Example 8 concerning, e.g., the primes 2, 3. Nevertheless, we can always find simultaneous integer solutions for a given finite set of primes, provided, of course, the system is solvable for every single prime.

Consider a finite set $P = \{p_1, \ldots, p_l\}$ of primes such that our system S is solvable for each $p \in P$. That is, for each $p_i \in P$ we have a p_i-adic integer solution branch

$$(\gamma^{(i)}, \{x_1^{(i)} = a_1^{(i)'}, \ldots, x_n^{(i)} = a_n^{(i)'}\})$$

with a p_i satisfying $\gamma^{(i)}$, and we can independently lift all the solutions for the various p_i, arriving at corresponding integer solutions

$$\begin{aligned} L_1 &= \{x_1^{(1)} = a_1^{(1)}, \ldots, x_n^{(1)} = a_n^{(1)}\} \\ &\vdots \\ L_l &= \{x_1^{(l)} = a_1^{(l)}, \ldots, x_n^{(l)} = a_n^{(l)}\} \end{aligned}$$

for $p_1, \ldots, p_l$, respectively. It is easy to see that we can equivalently replace all the $a_1^{(1)}, \ldots, a_1^{(l)}$ by the solution a_1 of the following system, where k is the highest power of p in the original system S:

$$\begin{aligned} a_1 &\equiv a_1^{(1)} \mod p_1^k \\ &\vdots \\ a_1 &\equiv a_1^{(l)} \mod p_l^k. \end{aligned}$$

This system is definitely solvable by Chinese remaindering. In the same way, we independently find suitable $a_2, \ldots, a_n$. such that $x_1 = a_1, \ldots, x_n = a_n$ simultaneously solves S for all $p \in P$.

Example 14 We simultaneously lift the result in Example 8 for various finite sets of primes:

(i) For the first ten primes $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$ we obtain after less than 0.01 s the uniform solution $x_1 = 404355827$, $x_2 = 3639202442$.

(ii) For the first 100 primes $\{2, \ldots, 541\}$ we obtain a uniform solution after 0.01 s, where both x_1 and x_2 have 220 digits.

(iii) For the first 500 primes $\{2, \ldots, 3571\}$ we obtain a uniform solution after 0.15 s, where both x_1 and x_2 have 1520 digits.

In general, there will be solution branches that match for several primes $P' \subseteq P$, such that we can lift these branches by simultaneous branch lifting. That is, we combine both our approaches.

7.3 Infinite Sets of Primes

Both our approaches allow us to lift simultaneously only for a finite number of primes. Simultaneous lifting of a non-integer solution for an infinite number of primes is in fact impossible as the following lemma shows.

Lemma 15 *Let r/s be a p-adic integer wrt. an infinite set P of primes. If r/s can be simultaneously lifted to an integer for an infinite subset $P' \subseteq P$, then r/s is already an integer.*

Proof Let the lifting factor $\overline{s} \equiv 1 \bmod p$ for all $p \in P'$. Since P' is infinite, there is $p_0 \in P'$ with $p_0 > \overline{s}$, and from $\overline{s} \equiv 1 \bmod p_0$, i.e., lifting does not change r/s.

8 Arbitrary Moduli

So far we have only considered linear congruence systems modulo powers of one fixed possibly parametric prime modulus. We are now going to extend our ideas to general moduli, where we restrict to the non-parametric case. Consider a system

$$S = \{f_1(\mathbf{x}) \equiv 0 \bmod \mu_1,\ \ldots,\ f_m(\mathbf{x}) \equiv 0 \bmod \mu_m\},$$

where $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ are polynomials that are linear in $x_1, \ldots, x_n$, and $\mu_1, \ldots, \mu_m \in \mathbb{N}$.

The key observation is that each of the $\mu_1, \ldots, \mu_m$ factors into finitely many prime powers, and that $\mathbf{a} \in \mathbb{Z}^n$ satisfies a given congruence modulo a product of prime powers if and only if it does so for all the single prime powers simultaneously:

$$\bigwedge_{i=1}^{l} f(\mathbf{a}) \equiv 0 \bmod p_i^{k_i} \iff f(\mathbf{a}) \equiv 0 \bmod \prod_{i=1}^{l} p_i^{k_i}.$$

So, we have learned all necessary techniques for solving this more general problem already in the previous section. The following algorithm explains how to organize the computation:

Algorithm 16 (Solving with Arbitrary Moduli)
Input: A system

$$S = \{f_1(\mathbf{x}) \equiv 0 \bmod \mu_1, \ \ldots, \ f_m(\mathbf{x}) \equiv 0 \bmod \mu_m\}.$$

of congruences over $\mathbb{Z}$ with $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ linear, $\mu_1, \ldots, \mu_m \in \mathbb{N}$.
Output: "infeasible," or a sample solution $\mathbf{a} \in \mathbb{Z}^n$ for S.

```
BEGIN
   P := the prime factors of μ_1, ..., μ_m
   for each p ∈ P  do
      T := ∅
      k^(p) := 0
      for j := 1 : m  do
         k := the power of p in μ_j
         if k > 0  then
            T := T ∪ {f_j(x) ≡ 0 mod p^k}
            k^(p) := max(k^(p), k)
         fi
      od
      apply Algorithm 3 to T
      if T is feasible  then
         a^(p) := an integer solution for T
      else
         return "infeasible"
      fi
   od
   for i := 1 : n  do
      C := { x_i ≡ a_i^(p) mod p^(k^(p)) | p ∈ P }
```

$a_i :=$ an integer solution for x_i by CRT
od
return $(a_1, \ldots, a_n)$
END

Example 17 We apply our implementation of Algorithm 16 to the following system S of congruences derived from the randomly generated Example 6:

$$\begin{aligned}
70x_1 + 6x_3 + 89x_4 + 7x_6 + 30 &\equiv 0 \quad \text{mod} \quad 280\\
87x_1 + 93x_2 + 78x_3 + 73x_4 + 53 &\equiv 0 \quad \text{mod} \quad 5665\\
87x_2 + 41x_5 + 3 &\equiv 0 \quad \text{mod} \quad 110\\
12x_2 + 37x_3 + 69x_4 + 15x_6 + 53 &\equiv 0 \quad \text{mod} \quad 1545\\
75x_1 + 90x_3 + 65x_4 + 14x_5 + 41 &\equiv 0 \quad \text{mod} \quad 3125\\
91x_5 + 96x_6 + 55 &\equiv 0 \quad \text{mod} \quad 1925.
\end{aligned}$$

The moduli here factorize as follows:

$$\begin{array}{rclcccccccccc}
280 & = & 2^3 & \cdot & & & 5 & \cdot & 7 & & & & \\
5665 & = & & & & & 5 & \cdot & & & 11 & \cdot & 103\\
110 & = & 2 & \cdot & & & 5 & \cdot & & & 11 & & \\
1545 & = & & & 3 & \cdot & 5 & \cdot & & & & & 103\\
3125 & = & & & & & 5^5 & & & & & & \\
1925 & = & & & & & 5^2 & \cdot & 7 & \cdot & 11. & &
\end{array}$$

We obtain after 2.29 s the following solution:

$$\begin{array}{rclrcl}
x_1 & = & 2873631250, & x_2 & = & 3339537828,\\
x_3 & = & 289265341729, & x_4 & = & 422862329737,\\
x_5 & = & 255144121, & x_6 & = & 112853162929.
\end{array}$$

Notice that our algorithm is based on solution lifting in contrast to branch lifting. In extreme special cases a combination with branch lifting might be more efficient. This is the case when there are many prime factors occurring with equal powers in all of the moduli. One would then solve the system parametrically for this distribution of prime powers.

9 Conclusions

Based on an extended quantifier elimination procedure for p-adically valued fields, we have devised algorithms for solving multivariate linear systems of congruences. Our methods generally split into two parts: First, finding solutions in suitable rings of p-adic integers $\mathbb{Z}_p$. Second, lifting these solutions to the integers $\mathbb{Z}$. The first part is computationally hard, while the second one is straightforward and efficient. For the special case, where each modulus is some power of a fixed prime, the computationally hard first part can be performed uniformly for all primes. For this case, we have developed two methods for making the lifting step also as uniform as theoretically possible. These methods can be finally reused for extending our approach to the general case of arbitrary, i.e. not necessarily prime power, moduli. This general case is a considerable generalization of the problem solved by the Chinese Remainder Theorem.

References

[AK66] James Ax and Simon Kochen. Diophantine problems over local fields. *Annals of Mathematics*, 83:437–456, 1966. Part III.

[BWK93] Thomas Becker, Volker Weispfenning, and Heinz Kredel. *Gröbner Bases, a Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer, New York, 1993.

[Coh69] Paul J. Cohen. Decision procedures for real and p-adic fields. *Communications in Pure and Applied Logic*, 25:213–231, 1969.

[DGS98] Andreas Dolzmann, Oliver Gloor, and Thomas Sturm. Approaches to parallel quantifier elimination. In Oliver Gloor, editor, *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (ISSAC 98)*, pages 88–95, Rostock, Germany, August 1998. ACM, ACM Press, New York, 1998.

[DS97a] Andreas Dolzmann and Thomas Sturm. Guarded expressions in practice. In Wolfgang W. Küchlin, editor, *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (ISSAC 97)*, pages 376–383, Maui, HI, July 1997. ACM, ACM Press, New York, 1997.

[DS97b] Andreas Dolzmann and Thomas Sturm. Redlog: Computer algebra meets computer logic. *ACM SIGSAM Bulletin*, 31(2):2–9, June 1997.

[DS99] Andreas Dolzmann and Thomas Sturm. P-adic constraint solving. In Sam Dooley, editor, *Proceedings of the 1999 International*

Symposium on Symbolic and Algebraic Computation (ISSAC 99), Vancouver, BC, pages 151–158. ACM Press, New York, NY, July 1999.

[DSW98] Andreas Dolzmann, Thomas Sturm, and Volker Weispfenning. Real quantifier elimination in practice. In B. H. Matzat, G.-M. Greuel, and G. Hiss, editors, *Algorithmic Algebra and Number Theory*, pages 221–247. Springer, Berlin, 1998.

[Ers65] Juri L. Ershov. On elementary theories of local fields. *Algebra i Logika Sem.*, 4(2):5–30, 1965.

[FR79] Jeanne Ferrante and Charles W. Rackoff. *The Computational Complexity of Logical Theories.* Number 718 in Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1979.

[Mac76] Angus Macintyre. On definable subsets of p-adic fields. *Journal of Symbolic Logic*, 41(3):605–610, September 1976.

[Ost18] Alexander Ostrowski. Über einige Lösungen der Funktionalgleichung $\varphi(x) \cdot \varphi(y) = \varphi(xy)$. *Acta Mathematica*, 41:271–284, 1918.

[Stu99] Thomas Sturm. Reasoning over networks by symbolic methods. *Applicable Algebra in Engineering, Communication and Computing*, 10(1):79–96, September 1999.

[Stu00] Thomas Sturm. Linear problems in valued fields. *Journal of Symbolic Computation*, 30(2):207–219, August 2000.

[Wei84] Volker Weispfenning. Quantifier elimination and decision procedures for valued fields. In G. H. Müller and M. M. Richter, editors, *Models and Sets (Aachen, 1983)*, volume 1103 of *Lecture Notes in Mathematics*, pages 419–472. Springer-Verlag, Berlin, Heidelberg, 1984.

[Wei88] Volker Weispfenning. The complexity of linear problems in fields. *Journal of Symbolic Computation*, 5(1&2):3–27, February–April 1988.