

Computing small solutions of unit equations in three variables II: Applications to resultant form equations

By István Járási

Dedicated to the memory of Professor Béla Brindza

Abstract. In [7] we described a method to compute small solutions of unit equations in three unknowns. In this paper we apply this method to a type of resultant form equations. We also detail several further improvements of the method. These improvements are essential, because without them it is hopeless to perform the numerical computations in reasonable time.

1. Introduction

Resultant form equations are special, but important decomposable form equations. There are two different types of resultant form equations. To obtain the first type, we fix an irreducible polynomial $P \in \mathbb{Z}[x]$ and a non-zero integer a and we search for a polynomials $Q \in \mathbb{Z}[x]$ such that

$$\text{Res}(P, Q) = a \quad \text{and} \quad 2\deg(Q) < \deg(P) \quad (1)$$

Mathematics Subject Classification: 11Y50, 11D57.

Key words and phrases: resultant form equation, unit equation, small solutions.

The author was supported in part by Grants No. T037367 and N34001 of the Hungarian National Foundation for Scientific Research and by the Netherlands Organization for Scientific Research(NWO)..

where $Res(P, Q)$ denotes the resultant of P and Q . E.Wirsing [10], W.M.Schmidt [9], H.P.Schlickewei [8] and K.Győry [5], [6] obtained finiteness results for equation (1). Recently I.Gaál [2] gave a numerical method to determine the solutions of (1) when P is a given irreducible polynomial with degree at least 3 and the unknown Q -s are monic quadratic polynomials.

In this paper we consider the following problem. Let K be a fixed algebraic number field and $a \in \mathbb{Z}$, $a \neq 0$ is also fixed. Find all polynomials $P, Q \in \mathbb{Z}[x]$ with common splitting field K such that

$$Res(P, Q) = a. \quad (2)$$

It is easy to see that if $(P(x), Q(x))$ is a solution to (2) then for any $b \in \mathbb{Z}$ $(P_1(x), Q_1(x)) = (P(x+b), Q(x+b))$ is also a solution to (2). In this case the pairs $(P(x), Q(x))$ and $(P_1(x), Q_1(x))$ are called \mathbb{Z} -equivalent. This shows that solving (2), one should restrict to some \mathbb{Z} -equivalence classes of polynomials.

It was shown by K.Győry [4] that there exist only finitely many \mathbb{Z} -equivalence classes of polynomials (P, Q) satisfying (2) such that $deg(P) \geq 2$, $deg(Q) \geq 2$, $deg(P) + deg(Q) \geq 5$ and both P and Q has simple roots from a fixed splitting field. He also showed that the same assertion is valid if \mathbb{Z} is replaced by any finitely generated and integrally closed domain over \mathbb{Z} . In [3] Győry gave an explicit upper bound for the degrees of P and Q and for the number of solutions (P, Q) .

The purpose of this paper is to determine the "small" solutions of (2) such that P and Q have roots generating the fixed number fields M_1 and M_2 , respectively. This is a special case of the above problem when P and Q have common splitting field K which is the normal closure of M_1M_2 .

We reduce the problem to unit equations in three unknowns and we use the method of [7] to handle such equations. Since the direct application of that method would require far too much CPU time, we have developed two essential improvements which enables us to perform the computations within feasible CPU time.

2. Resultant form equations

We will solve the following problem:

Let M_1 and M_2 be cubic algebraic number fields. Let $K = M_1M_2$ be the composite of M_1 and M_2 . Assume that the degree of K is 9, and denote by r its unit rank. Our purpose is to determine the "small" solutions of the equation

$$\text{Res}(f_1, f_2) = \pm 1 \quad (3)$$

in monic cubic polynomials f_1, f_2 with integer coefficients, such that a root of f_i generates M_i ($i = 1, 2$). We note that our method can be applied without significant changes to the same problem with a given integer a in place of ± 1 on the right hand side, i.e. to the equation

$$\text{Res}(f_1, f_2) = a.$$

Let $\alpha^{(i)}$ and $\beta^{(i)}$ ($i = 1, 2, 3$) denote the roots of f_1 and f_2 , respectively. Then

$$\text{Res}(f_1, f_2) = \prod_{i=1}^3 \prod_{j=1}^3 (\alpha^{(i)} - \beta^{(j)})$$

holds. For any $\gamma \in K$ denote by $\gamma^{(ij)}$ its conjugate corresponding to $\alpha^{(i)}, \beta^{(j)}$ ($1 \leq i, j \leq 3$). Then we can write

$$\alpha^{(i)} - \beta^{(j)} = \pm \left(\eta_1^{(ij)} \right)^{a_1} \cdots \left(\eta_r^{(ij)} \right)^{a_r}$$

where $\eta_k^{(ij)}$ is a system of fundamental units of K and $a_k \in \mathbb{Z}$ ($k = 1, \dots, r$).

As an analogue of Siegel's identity in our case we have:

$$(\alpha^{(i)} - \beta^{(k)}) + (\alpha^{(j)} - \beta^{(l)}) - (\alpha^{(i)} - \beta^{(l)}) - (\alpha^{(j)} - \beta^{(k)}) = 0.$$

That is

$$\mu^{(ij)} + \mu^{(kl)} - \mu^{(il)} - \mu^{(jk)} = 0 \quad (4)$$

with $\mu^{(mn)} = \alpha^{(m)} - \beta^{(n)}$. Since the $\mu^{(mn)}$ are the conjugates of a suitable unit of \mathbb{Z}_K , (4) is a unit equation in three variables (in homogeneous form) for which we can apply our method described in [7].

3. Our method to compute the small solutions of unit equations in three variables

In the following we summarize how one can apply the method of [7] to compute the "small" solutions of (4) which corresponds to the "small" solutions of (3). As indicated in the Introduction, the direct application is not enough strong to determine the "small" solutions.

We call a solution (f_1, f_2) of (3) "small" if $\max(H(f_1), H(f_2)) \leq H_0$, where $H(f)$ is the maximum of the absolute values of the coefficients of f and H_0 is a given constant. In our numerical example we set $H_0 = 10^{85}$. Clearly, in this case searching directly for the "small" solutions is hopeless.

Let K be an algebraic number field of degree d .

Our purpose is to find all "small" units u in \mathbb{Z}_K such that

$$u^{(1)} + u^{(2)} + u^{(3)} + u^{(4)} = 0 \quad (5)$$

where $u^{(i)}$ is the i -th conjugate of u .

A unit u is called "small" if its exponents corresponding to a given system of fundamental units are "small", that is

$$\max_{1 \leq i \leq r} (|a_i|) \leq A_0, \quad u = \zeta \eta_1^{a_1} \cdots \eta_r^{a_r},$$

where A_0 is a given positive number, η_1, \dots, η_r is a system of fundamental units in K and ζ is a root of unity.

Fix an integer g with $1 \leq g \leq r$ and fix g embeddings of K into \mathbb{C} . Then from each g embedding of (5) equation choose 3 terms. Take one of these embeddings, say i , and consider the equation

$$(u^{(1)})^{(i)} + (u^{(2)})^{(i)} + (u^{(3)})^{(i)} + (u^{(4)})^{(i)} = 0$$

obtained from (5) by using the i -th embedding of K . Then fix $(u^{(1)})^{(i)}, (u^{(2)})^{(i)}, (u^{(3)})^{(i)}$ where $(u^{(j)})^{(i)}$ denotes the image of $u^{(j)}$ under the i -th conjugation. With these 3 terms construct a semi-orbit $\mathfrak{D} \left(\frac{(u^{(1)})^{(i)}}{(u^{(2)})^{(i)}}, \frac{(u^{(3)})^{(i)}}{(u^{(2)})^{(i)}} \right)$ (A semi-orbit $\mathfrak{D}(x, y)$ is defined by $\mathfrak{D}(x, y) = \{x, y, \frac{1}{x}, \frac{1}{y}, -\frac{x}{y}, -\frac{y}{x}\}$ where x, y are nonzero

complex numbers. The semi-orbit is called enumerable if for all $u \in \mathfrak{D}(x, y)$ there is a $v \in \mathfrak{D}(x, y)$ such that $|u+v| \leq 2$ and $\frac{u}{v} \in \mathfrak{D}(x, y)$. In this case it is denoted by \mathfrak{D}^2 . For more details see [7]. Collect the semi-orbits corresponding to different equations into an enumerable set \mathfrak{D} (which is the union of enumerable semi-orbits):

$$\mathfrak{D} = \bigcup_{i=1}^g \mathfrak{D} \left(\frac{(u^{(j_i)})^{(i)}}{(u^{(k_i)})^{(i)}}, \frac{(u^{(l_i)})^{(i)}}{(u^{(k_i)})^{(i)}} \right)$$

This must be done in all the $\binom{4}{3}^g = 4^g$ possible cases.

For each of these 4^g enumerable sets now one can apply the enumeration lemma from [7]:

Lemma 1. *Let S and s be positive numbers with $S > s > 2$. Let \mathfrak{D} be an enumerable set and suppose that for every $u \in \mathfrak{D}$ we have*

$$\frac{1}{S} \leq |u| \leq S.$$

Then

(1) either for all $u \in \mathfrak{D}$

$$\frac{1}{s} \leq |u| \leq s$$

(2) or there is a $u \in \mathfrak{D}$ such that

$$|\log |u|| \leq \frac{2}{s-2}.$$

To apply this lemma one needs an initial bound $S = S_0$. This can be derived using the actual definition of "small" units. Practically we have a bound A_0 on the absolute values of the exponents of the fundamental units representing a "small" unit. Using this bound one can derive the expected S_0 (for details see [7]).

4. Improvements of the method

4.1. Decreasing the number of enumerable sets. First let us see what it means if we fix an enumerable semi-orbit using Corollary 1 of [7].

For this purpose let u be a solution of (5), that is

$$-\frac{u^{(1)}}{u^{(4)}} - \frac{u^{(2)}}{u^{(4)}} - \frac{u^{(3)}}{u^{(4)}} = 1.$$

We apply Corollary 2.2 of [7] to this equation with

$$x_i = -\frac{u^{(i)}}{u^{(4)}} \quad (i = 1, 2, 3).$$

We obtain that one of the four pairs

$$\left(-\frac{u^{(2)}}{u^{(1)}}, -\frac{u^{(3)}}{u^{(1)}}\right), \left(-\frac{u^{(2)}}{u^{(4)}}, -\frac{u^{(3)}}{u^{(4)}}\right), \left(-\frac{u^{(1)}}{u^{(3)}}, -\frac{u^{(4)}}{u^{(3)}}\right), \left(-\frac{u^{(1)}}{u^{(2)}}, -\frac{u^{(4)}}{u^{(2)}}\right)$$

say $\left(-\frac{u^{(2)}}{u^{(1)}}, -\frac{u^{(3)}}{u^{(1)}}\right)$, generates an enumerable semi-orbit. This property is equivalent to

$$\left|-\frac{u^{(1)}}{u^{(3)}}\right| \geq 1, \quad \left|-\frac{u^{(2)}}{u^{(3)}}\right| \geq 1, \quad \left|-\frac{u^{(4)}}{u^{(3)}}\right| \geq 1$$

or

$$\left|u^{(1)}\right| \geq \left|u^{(3)}\right|, \quad \left|u^{(2)}\right| \geq \left|u^{(3)}\right|, \quad \left|u^{(4)}\right| \geq \left|u^{(3)}\right|. \quad (6)$$

In other words, fixing a primitive pair is equivalent to fixing an $u^{(i)}$ with the least absolute value.

In our method we use enumerable sets which are the unions of enumerable semi-orbits corresponding to different conjugates of equation (5). Let \mathfrak{D} be such an enumerable set:

$$\mathfrak{D} = \bigcup_{i=1}^g \mathfrak{D}^2\left(-\frac{u^{(j_i)}}{u^{(k_i)}}, -\frac{u^{(l_i)}}{u^{(k_i)}}\right).$$

By the above formulas, fixing an enumerable set is equivalent to choosing the unit with smallest absolute value from $\{(u^{(1)})^{(i)}, (u^{(2)})^{(i)}, (u^{(3)})^{(i)}, (u^{(4)})^{(i)}\}$ for each $i = 1, \dots, g$. For every fixed conjugation we obtain a system of inequalities similar to (6). After combining these inequalities, we may obtain two conjugates of u -say $u^{(i)}$ and $u^{(j)}$ - appearing in the same equation

$$u^{(i)} + u^{(j)} + u^{(k)} + u^{(l)} = 0. \quad (7)$$

Here

$$|u^{(i)}| \geq |u^{(j)}| \quad \text{and} \quad |u^{(j)}| \geq |u^{(i)}|$$

hold, whence

$$|u^{(i)}| = |u^{(j)}|.$$

Let $\varepsilon = \frac{u^{(i)}}{u^{(j)}}$. Then ε is a unit in $\mathbb{Z}_{\overline{K}}$ (\overline{K} is the normal closure of K) with $|\varepsilon| = 1$, so it is a root of unity. However, this means that (7) can be written as

$$(1 + \varepsilon)u^{(i)} + u^{(k)} + u^{(l)} = 0$$

which is a unit equation in two unknowns (in homogeneous form). When $u^{(i)}$ and $u^{(j)}$ are real units then $\varepsilon = \pm 1$ so (7) reduces either to

$$u^{(k)} + u^{(l)} = 0$$

or to

$$2u^{(j)} + u^{(k)} + u^{(l)} = 0.$$

Hence none of these equations can be a conjugate of (5), so we have a contradiction. This means this \mathfrak{D} can be dropped. In Section 5. we detail a numerical example and there one can see that using this consideration we dropped quarter of the enumerable sets.

4.2. Enumerable sets with small rank. In Section 4 of [7] we defined the rank of an enumerable set. Let \mathfrak{D} be a set containing some nontrivial quotients of the units, that is

$$\mathfrak{D} = \left\{ \frac{u^{(i)}}{u^{(j)}} \mid (i, j) \in \Gamma_{\mathfrak{D}} \right\}$$

where $\Gamma_{\mathfrak{D}} = \{(i_l, j_l) \mid l = 1, \dots, t\}$ is a suitable index set. We shall call $\Gamma_{\mathfrak{D}}$ the index set corresponding to \mathfrak{D} .

Definition 1. Let \mathfrak{D} be an enumerable set with corresponding index set $\Gamma_{\mathfrak{D}} = \{(i_l, j_l) \mid l = 1, \dots, t\}$. By the rank of \mathfrak{D} we mean the dimension of the vector space spanned by the vectors

$$\underline{e}_k = \begin{pmatrix} \log \left| \frac{\varepsilon_k^{(i_1)}}{\varepsilon_k^{(j_1)}} \right| \\ \vdots \\ \log \left| \frac{\varepsilon_k^{(i_t)}}{\varepsilon_k^{(j_t)}} \right| \end{pmatrix} \quad (k = 1, \dots, r).$$

In that paper the numerical example illustrated what can be expected: the smaller the rank is, the longer the running time is.

In the following we show how one can substitute a given enumerable set with four new enumerable sets of rank which is greater than or equal to the original one's rank. If all of the four new enumerable sets have greater ranks then there is a better chance to enumerate the possible solutions in them in reasonable time.

Lemma 2. *Let u be a solution to (5). Using the first $d_1 < d$ conjugates of (5) construct the 4^{d_1} enumerable sets as in Theorem 4.2 in [7]. Let \mathfrak{D} be one of them. Then there are enumerable sets $\mathfrak{D}_1, \mathfrak{D}_2, \mathfrak{D}_3, \mathfrak{D}_4$ such that*

$$\mathfrak{D} \subset \bigcup_{i=1}^4 \mathfrak{D}_i$$

and \mathfrak{D}_i has rank greater than or equal to the rank of \mathfrak{D} for $i = 1, \dots, 4$.

PROOF. Construct the four enumerable semi-orbits by the help of one of the remaining $d - d_1$ conjugates of equation (5) using Theorem 4.2 of [7] for a $g \in \{d_1 + 1, \dots, d\}$. Let these semi-orbits be

$$\mathfrak{D}_1^2, \mathfrak{D}_2^2, \mathfrak{D}_3^2, \mathfrak{D}_4^2.$$

Then put

$$\mathfrak{D}_1 = \mathfrak{D} \cup \mathfrak{D}_1^2, \quad \mathfrak{D}_2 = \mathfrak{D} \cup \mathfrak{D}_2^2, \quad \mathfrak{D}_3 = \mathfrak{D} \cup \mathfrak{D}_3^2, \quad \mathfrak{D}_4 = \mathfrak{D} \cup \mathfrak{D}_4^2.$$

It is easy to see that

$$\mathfrak{D} \subset \bigcup_{i=1}^4 \mathfrak{D}_i.$$

Since in each \mathfrak{D}_i there are more elements than in \mathfrak{D} so their ranks are greater than or equal to the rank of \mathfrak{D} . \square

5. A numerical example

We take M_1 to be generated by a root of $x^3 - x^2 - 6x + 5$ and M_2 to be generated by a root of $x^3 - 9x + 6$. One can check that M_1 and M_2 are totally real cubic fields, so their unit rank $r = 8$.

Using the improvements of the method, we computed the "small" solutions of the equation

$$Res(f_1, f_2) = \pm 1$$

where the f_i -s are monic polynomials with integer coefficients such that a root of f_i generates M_i ($i = 1, 2$), and

$$\max(H(f_1), H(f_2)) \leq 10^{85}. \tag{8}$$

As we explained in Section 2, our problem can be reduced to finding the "small" solutions of the equation

$$\mu^{(ij)} + \mu^{(kl)} - \mu^{(il)} - \mu^{(jk)} = 0$$

with $\mu^{(mn)} = \alpha^{(m)} - \beta^{(n)} \in (M_1)^{(m)}(M_2)^{(n)}$. Since the $\mu^{(mn)}$ are conjugates of a suitable unit from \mathbb{Z}_K , this equation is a unit equation in three variables (in homogeneous form). Thus we obtain

$$\alpha^{(i)} - \beta^{(j)} = \pm \left(\eta_1^{(ij)}\right)^{a_1} \cdots \left(\eta_8^{(ij)}\right)^{a_8}$$

where $\eta_k^{(ij)}$ is a system of fundamental units of K and $a_k \in \mathbb{Z}$ ($k = 1, \dots, 8$). Using standard tools from (8) one can get a bound A_0 such that

$$\max_{i=1, \dots, 8} (|a_i|) \leq A_0.$$

In this case we have $A_0 = 200$ which is a typical bound in the case of unit equations in two variables obtained by the help of Baker's theory and LLL-reduction due to de Weger. For details see [1].

Now we apply the method as described in Section 3. We take four conjugates of the unit equation. This yields 256 enumerable set. In the following table we summarize the number of enumerable sets without the

recent improvements (second row), applying the first improvement (Section 4.1, third row) and applying both improvements of this paper (Section 4.1 and 4.2, fourth row).

	# of e. s. of rank 8 (18 m)	# of e. s. of rank 7 (36 m)	# of e. s. of rank 6 (23 h 20 m)	# of e. s. of rank 5 (∞)	Total # of e.s.	Total CPU Time
none	30	145	74	7	256	∞
4.1	12	109	68	7	196	∞
4.1 + 4.2	12	125	70	0	207	72 days

In the first row in the brackets one can find the average CPU time on a 700 MHz Xeon processor of a single enumerable set of the corresponding rank (∞ stands for too much CPU time), and "e.s." stands for enumerable sets.

In the second row one can find the number of enumerable sets using the method of [7] of the corresponding rank. In the third row one can find the number of enumerable sets using our first improvement (Section 4.1). The last row contains the number of enumerable sets using both new improvements (Sections 4.1 and 4.2). It is clear from the table that our improvements are really essential.

We have found two solutions: $(f(x), g(x)) = (x^3 + x^2 - 6x - 5, x^3 - 9x + 6)$ and $(x^3 + 2x^2 - 9x + 5, x^3 - 9x + 6)$.

References

- [1] I.Gaál, *Diophantine equations and power integral bases*, Birkhäuser Boston, 2002.
- [2] I.Gaál, *On the resolution of resultant type equations*, J.Symbolic Comput. **34** (2002), no. 2, 137–144.
- [3] K.Györy, *On the number of pairs of polynomials with given resultant or given semi-resultant*, Acta Sci. Math. **57** (1993), 169–180.
- [4] K.Györy, *On arithmetic graphs associated with integral domains*, in: A tribute to Paul Erdős, Cambridge University Press, 1990. pp. 207–222.
- [5] K.Györy, *Some applications of decomposable form equations to resultant form equations*, Colloq. Math. **65** (1993), 267–275.

- [6] K.Györy, *On the irreducibility of neighbouring polynomials*, Acta Arith. **67** (1994), 283–294.
- [7] I.Járasi, *Computing small solutions of unit equations in three variables I: Application to norm form equations*, submitted.
- [8] H.P.Schlickewei, *Inequalities for decomposable form equations*, Astérisque **41-42** (1977), 267–271.
- [9] W.M.Schmidt, *Inequalities for resultants and for decomposable forms*, in: Diophantine Approximation and its applications, Academic Press, New York 1973, pp. 235–253.
- [10] E.Wirsing, *On approximations of algebraic numbers by algebraic numbers of bounded degree*, in: Proc. Symp. Pure Math. 20, Amer. Math. Soc., Providence 1971, pp. 213–247.

DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
UNIVERSITY OF DEBRECEN
H-4010 DEBRECEN, P.O.B. 12
HUNGARY

E-mail: ijarasi@math.klte.hu