Computation of unirational fields

Jaime Gutierrez[1], David Sevilla[1]

[1]Faculty of Science, University of Cantabria, E-39071 Santander, Spain

Abstract

In this paper we present an algorithm for computing all algebraic intermediate subfields in a separably generated unirational field extension (which in particular includes the zero characteristic case). One of the main tools is Gröbner bases theory, see [BW93]. Our algorithm also requires computing computing primitive elements and factoring over algebraic extensions. Moreover, the method can be extended to finitely generated $\mathbb{K}$-algebras.

1 Introduction

The goal of this paper is to study the problem of computing intermediate fields between a rational function field and a given subfield of it. This computational problem has many applications, not only in other areas of mathematics like Algebraic Geometry, but also in Computer Aided Geometric Design. The question of the structure of the lattice of such intermediate fields is of theoretical interest by itself; we will focus on the computational aspects, like deciding if there are proper intermediate fields and computing them in the affirmative case.

In the univariate case, the problem can be stated as follows: given $f_1, \ldots, f_m \in \mathbb{K}(t)$, find a field $\mathbb{F}$ such that $\mathbb{K}(f_1, \ldots, f_m) \subsetneq \mathbb{F} \subsetneq \mathbb{K}(t)$. By Lüroth's Theorem this is equivalent to the problem of decomposing the rational functions. Algorithms for decomposition of univariate rational functions can be found in [Zip91] and [AGR95].

In the multivariate case, the problem can be stated as:

Problem 1 *Let $\mathbb{K}$ be a field and $\mathbb{K}(x_1, \ldots, x_n) = \mathbb{K}(\mathbf{x})$ be the rational function field in the variables $\mathbf{x} = (x_1, \ldots, x_n)$. Given rational functions $f_1, \ldots, f_m \in \mathbb{K}(\mathbf{x})$, compute a proper unirational field $\mathbb{F}$ between $\mathbb{K}(f_1, \ldots, f_m)$ and $\mathbb{K}(\mathbf{x})$, if it exists.*

Any unirational field is finitely generated over $\mathbb{K}$ (see [Nag93]). Thus, by computing an intermediate field we mean that such a finite set of generators is to be calculated. Regarding algorithms for this problem, see [MQS99], where the authors generalize the method of [AGR95] to several variables, by converting this problem into the calculation of a primary ideal decomposition. Primary ideal decomposition can be computed by Gröbner Bases. The

book [BW93] by T. Becker and Volker Weispfenning is an excellent reference guide to this important theory and their application.

It is not difficult to realize that the solution of the problem is trivial and uninteresting for most choices of $f_1, \ldots, f_m$, since it is easy to construct infinitely many intermediate fields when the transcendence degree of $\mathbb{K}(f_1, \ldots, f_m)$ over $\mathbb{K}$ is smaller than n. Due to this, we will focus on the following version of the problem.

Problem 2 *Given functions $f_1, \ldots, f_m \in \mathbb{K}(\mathbf{x})$, find all the fields $\mathbb{F}$ between $\mathbb{K}(f_1, \ldots, f_m)$ and $\mathbb{K}(\mathbf{x})$ that are algebraic over $\mathbb{K}(f_1, \ldots, f_m)$.*

There are finitely many algebraic intermediate fields if the original extension is separable.

The special case of Problem 2 when the transcendence degree of $\mathbb{K}(f_1, \ldots, f_m)/\mathbb{K}$ is 1 has been treated in [GRS01]. In this case a generalization of Lüroth's Theorem applies so the problem is equivalent to the so-called uni-multivariate decomposition. The paper [GRS02] provides a very efficient constructive proof of the theorem mentioned above and it also contains different decomposition algorithms for multivariate rational functions. In some sense, Problem 2 can be seen as a generalization of the univariate rational function decomposition problem.

In this paper we will combine several techniques of Computational Algebra to create an algorithm that finds all the intermediate fields that are algebraic over the smaller field. Moreover, our method can be extended to finitely generated $\mathbb{K}$-algebras, that is, the case where the ambient field is $\mathbb{K}(z_1, \ldots, z_n) = \mathbb{K}(\mathbf{z})$ for some $z_1, \ldots, z_n$ transcendental over $\mathbb{K}$ that need not be algebraically independent, and $\mathbb{K}(\mathbf{z})$ is the quotient field of a polynomial ring, so that we have

$$\mathbb{K}(\mathbf{z}) = QF\left(\mathbb{K}[x_1, \ldots, x_n]/I\right)$$

for some prime ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ that will be given explicitly by means of a finite system of generators. Unsurprisingly, the algorithm will be much simpler when $\mathbb{K}(\mathbf{x})$ is rational, that is, when $I = (0)$.

2 Main Results

First, we can use Gröbner bases to compute and manipulate various elements in our extensions, see [Swe93] and [BW93]. We can compute transcendence and algebraic degrees of unirational fields, decide whether an element is transcendental or algebraic over a field, compute its minimum polynomial in the latter case, and decide membership. Moreover, we can compute bases in the separable case without using, properly, Gröbner bases, see [Ste00].

The next step is solving the problem when the given extension is algebraic. We can rewrite the fields in the following way:

- There exist rational functions $\hat{\alpha}_1,\ldots,\hat{\alpha}_n$ such that $\mathbb{K}(\hat{\alpha}_1,\ldots,\hat{\alpha}_n)/\mathbb{K}$ is a purely transcendental extension, with

$$\mathbb{K}(\hat{\alpha}_1,\ldots,\hat{\alpha}_n) \subset \mathbb{K}(f_1,\ldots,f_m) \subset \mathbb{K}(x_1,\ldots,x_n).$$

- There exist $\hat{\alpha}_{n+1}$, f algebraic over $\mathbb{K}(\hat{\alpha}_1,\ldots,\hat{\alpha}_n)$ such that

$$\begin{array}{ll} \mathbb{K}(f_1,\ldots,f_m) = & \mathbb{K}(\hat{\alpha}_1,\ldots,\hat{\alpha}_n,\hat{\alpha}_{n+1}), \\ \mathbb{K}(x_1,\ldots,x_n) = & \mathbb{K}(\hat{\alpha}_1,\ldots,\hat{\alpha}_n,f). \end{array}$$

Also, for any intermediate field in the extension there is h algebraic over $\mathbb{K}(\hat{\alpha}_1,\ldots,\hat{\alpha}_n)$ such that

$$\mathbb{F} = \mathbb{K}(\hat{\alpha}_1,\ldots,\hat{\alpha}_n,h).$$

Thus, we can work in an algebraic simple extension. Let $\mathbb{E} = \mathbb{K}(t_1,\ldots,t_n)$ be a purely transcendental field over $\mathbb{K}$, $\mathbb{E}[\alpha]/\mathbb{E}$ an algebraic separable extension. Then, there exists a bijection between the set of intermediate fields of $\mathbb{E} \subset \mathbb{E}[\alpha]$ and the set of subgroups of the Galois group G that contain G_α. Moreover, if $\mathbb{E}[\beta],\mathbb{E}[\gamma] \subset \mathbb{E}[\alpha]$ are intermediate fields, we can decide if $\mathbb{E}[\beta] \subset \mathbb{E}[\gamma]$.

It turns out that by factoring the minimal polynomial of α over $\mathbb{E}[\alpha]$, we can compute the intermediate fields of the extension $\mathbb{E}[\alpha]/\mathbb{E}$. This is accomplished by means of using decomposition blocks and, from the computational point of view, factorization of polynomials in algebraic extensions, see [Tra76], [YNT89], [Rub01] and [LM85].

Algorithm 1
[A] Factor $p_\alpha(z)$ in $E[\alpha]$.
[B.1] If $p_\alpha(z)$ has more than one linear factor:

$$p_\alpha(z) = (z-\alpha)(z-p_2(\alpha))\cdots(z-p_r(\alpha))p_{r+1}(z,\alpha)\cdots p_{r'}(z,\alpha)$$

- Compute a minimal subgroup G_ψ of $< \{\sigma_2 : \alpha \mapsto p_i(\alpha)\} >$.
- Consider $h(z) = \prod_{\sigma\in G_\psi}(z-\sigma(\alpha)) = a_u x^u + \cdots + a_0$.
- Take a_i such that $\mathbb{E}[a_i]$ is a proper subfield of $\mathbb{E} \subset \mathbb{E}[\alpha]$.

[B.2] If $p_\alpha(z) = (z-\alpha)p_2(z,\alpha)\cdots p_{r'}(z,\alpha)$, with p_i non-linear.
- Consider a factor $P_2(z) = h(z,\alpha)(z-\alpha)$ of $p_\alpha(z)$.

$$P_2 = (z-\alpha)h(z,\alpha) = a_u x^u + \cdots + a_0.$$

- If $\mathbb{E}[a_i] = \mathbb{E}[\alpha]$ for all i, then take another factor.

In order to solve the general problem, we will compute the algebraic closure of the given field in the ambient field. We will look for the minimum field $\mathbb{F}_0$ that contains all the intermediate algebraic fields over the given one. We adapt our data according to the algorithm in [BV93] and [Vas98].

- Let h be the minimum common denominator of the rational functions $f_i \in \mathbb{K}(\mathbf{x})$.
- Let $\Phi : \mathbb{K}[y_1,\ldots,y_m] \to \mathbb{K}[x_1,\ldots,x_n,1/h]$, defined as $\Phi(y_i) = f_i$ for each $i = 1,\ldots,m$.
- Let $\mathbb{D}_1 = \Phi(\mathbb{K}[y_1,\ldots,y_m]) = \mathbb{K}[f_1,\ldots,f_m]$. We have that $\mathbb{D}_1 = \mathbb{K}[y_1,...,y_m]/\operatorname{Ker}(\Phi)$ is a finitely generated $\mathbb{K}$-algebra. Also, the field of fractions of $\mathbb{D}_1$ is $\mathbb{K}(f_1,...,f_m)$.
- Let $\mathbb{D}_2 = \mathbb{D}_1[x_1,\ldots,x_n] = \mathbb{K}[x_1,\ldots,x_n,1/h]$. The field of fractions of $\mathbb{D}_2$ is $\mathbb{K}(\mathbf{x})$.
- Let t be a new variable and $\mathbb{D} = \mathbb{D}_1[t,x_1,\ldots,x_n] \subset \mathbb{D}_2[t]$, it is a birational monomorphism. Compute the integral closure $\overline{\mathbb{D}}$ of the extension $\mathbb{D} \subset \mathbb{D}_2[t]$ according to [Vas98]. The integral closure of the extension $\mathbb{D}_1 \subset \mathbb{D}_2$ is $\mathbb{D}_0 = \overline{\mathbb{D}} \cap \mathbb{D}_2$.
- Then $\mathbb{F}_0$ is the field of fractions of $\mathbb{D}_0$.

Summarizing the results we have presented, we have the following algorithm to find intermediate unirational fields over a given field, if the extension is separable.

Algorithm 2

INPUT: $f_1,\ldots,f_m \in \mathbb{K}(\mathbf{x})$.

OUTPUT: rational functions $h_1,\ldots,h_r$ such that

$$\mathbb{K}(f_1,\ldots,f_m) \subsetneq \mathbb{K}(h_1,\ldots,h_r) \subsetneq \mathbb{K}(\mathbf{x}).$$

A. Compute the algebraic closure of $\mathbb{K}(f_1,\ldots,f_m)$ relative to $\mathbb{K}(\mathbf{x})$.

B. Find a separating basis of $\mathbb{K}(f_1,\ldots,f_m)$.

C. Rewrite the fields to obtain a simple algebraic extension.

D. Factor the minimum polynomial obtained in the algebraic extension.

E. Compute the decomposition blocks that correspond to the factors found before.

F. If such a block exists, compute an intermediate field.

G. Recover the generators of the intermediate field in terms of the variables $\mathbf{x}$.

Something that is worth mentioning is the fact that all the computations can also be performed if the ambient field is not a rational field but one of type $QF(\mathbb{K}[x_1,\ldots,x_n]/I)$ for some prime ideal I, the given extension being separable. However, the theoretical and practical efficiency increases greatly, since the representations of the elements are larger and all the checks of type $f = 0$ become $f \in \mathscr{B}_{\mathbb{K}(\mathbf{x})/\mathbb{K}}$.

3 Conclusions

We have presented algorithms for resolving several issues related to rational function field. Our approach has combined useful computational algebra tools. We also unresolved many interesting questions. Unfortunately, we do not know if the computed intermediate field is rational or not, the reason is that the algorithm produce an intermediate field generated always by the transcendence degree plus one elements. Should be interesting to investigate under which circumstances our algorithm can display an intermediate subfield generated by as many elements as the transcendence degree. From a more practical point of view, we would like to have either a good algorithm or a good implementation to compute a factorization of a polynomial over an algebraic extension. Concerning applications, we regard the future interrelation of our techniques to the factorization of morphisms and regular maps between affine and projective algebraic sets.

References

[AGR95] C. Alonso, J. Gutierrez, and T. Recio. A rational function decomposition algorithm by near-separated polynomials. *J. Symbolic. Comput.*, 19(6):527–544, 1995.

[BV93] J. Brennan and W. Vasconcelos. Effective computation of the integral closure of a morphism. *J. Pure Appl. Algebra*, 86(2):125–134, 1993.

[BW93] T. Becker and V. Weispfenning. *Groebner bases. A computational approach to commutative algebra. Graduate Texts in Mathematics, 141*. Springer-Verlag, New York, 1993.

[GRS01] J. Gutiérrez, R. Rubio, and D. Sevilla. Unirational fields of transcendence degree one and functional decomposition. pages 167–174, 2001.

[GRS02] J. Gutiérrez, R. Rubio, and D. Sevilla. On multivariate rational function decomposition. *Computer algebra (London, ON, 2001). J. Symbolic Comput.*, 33(545–562):5, 2002.

[LM85] S. Landau and G. L. Miller. Solvability by radicals is in polynomial time. *J. Comput. System Sci.*, 30(2):179–208, 1985.

[MQS99] J. Müller-Quade and R. Steinwandt. Basic algorithms for rational function fields. *J. Symbolic Comput.*, 27(2):143–170, 1999.

[Nag93] M. Nagata. *Theory of commutative fields*. Translations of Mathematical Monographs, 125. American Mathematical Society, Providence, RI, 1993.

[Rub01] R. Rubio. *Unirational fields. Theorems, algorithms and applications*. PhD. Thesis. Dep. of Mathematics, University of Cantabria, 2001.

[Ste00] R. Steinwandt. On computing a separating transcendence basis. *SIGSAM Bulletin*, 34(4):3–6, 2000.

[Swe93] M. Sweedler. Using gröbner bases to determine the algebraic and transcendental nature of field extensions: return of the killer tag variables. *Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., Springer*, 673:66–75, 1993.

[Tra76] B. Trager. Algebraic factoring and rational function integration. pages 219–228, 1976.

[Vas98] W. Vasconcelos. *Computational Methods in Commutative Algebra and Algebraic Geometry. Vol. 2 of Algorithms and Computation in Mathematics*. Springer-Verlag, 1998.

[YNT89] K. Yokoyama, M. Noro, and T. Takeshima. Computing primitive elements of extensions fields. *J. Symbolic Comput.*, 8(6):553–580, 1989.

[Zip91] R. Zippel. Rational function decomposition. pages 1–6, 1991.

Jaime Gutierrez is an an Associate Professor of Mathematics at the University of Cantabria, Spain, since 1991. His main interests are Computational Algebra, Coding Theory and Cryptography.

jaime.gutierrez@unican.eshttp://personales.unican.es/gutierrj/

David Sevilla is a Ph. D. in Mathematics since March 2004 and is currently researching Functional Decomposition and other topics of Computational Algebra in University of Cantabria, Spain.

david.sevilla@unican.eshttp://personales.unican.es/sevillad/