

Abstract: Simplifying algebraic extensions

Mark van Hoeij and Andy Novocin, Florida State University

May 8, 2004

Many problems in symbolic computation require the use of an algebraic extension of the rationals, but the extension is not represented with the best (in terms of bit size) possible minimal polynomial. An algorithm was given by Henri Cohen that calculates a new minimal polynomial representing the same field extension. This algorithm often produces a minimal polynomial of small bit size but it uses computation of the ring of algebraic integers, which involves factoring integers. We propose a similar algorithm, but instead of computing the ring of algebraic integers, we use a large subring that is easier to calculate. The input of our algorithm is a list of elements of our number field, the output is a near optimal minimal polynomial and the transformation of the old minimal polynomial in terms of the new one. We add each algebraic number we can find in the problem and add it to our subring until our approximation of the ring of algebraic integers is large.

This has many applications, namely any operation whose output is in terms of an algebraic extension of the rationals. In the following example we find solutions of a system of equations and improve the solution with our algorithm.

When MAPLE solves the following system:

$$215 + 162x + 188y + 531z + 7x^2 + 67xy + 195xz + 36y^2 + 221yz + 338z^2$$

$$194 - 89x + 40y + 527z + 50x^2 - 122xy - 25xz - 15y^2 + 60yz + 364z^2$$

$$15 + 13x - 104y + 137z + 4x^2 - 40xy + 60xz + 100y^2 - 300yz + 225z^2$$

We get a rational solution and the following:

$$y = \frac{50905542013345457244782}{415389067374386774218664204327}\alpha^4 + \frac{307502409246905751748795197879}{415389067374386774218664204327}\alpha^2 +$$
$$\frac{176999401167415594229851760}{415389067374386774218664204327}\alpha^3 + \frac{92612110478302842988413418348200073}{415389067374386774218664204327} +$$
$$\frac{5852317761554448363}{415389067374386774218664204327}\alpha^5 + \frac{680387750120110946270895069925542518}{1058826732737311887483375056829523}\alpha$$
$$x = \frac{9179164288013579679868}{415389067374386774218664204327}\alpha^4 + \frac{52180501417053446687295266273}{415389067374386774218664204327}\alpha^2 +$$

$$\frac{30995221401928532197363156}{415389067374386774218664204327}\alpha^3 + \frac{14652755094293560407487472474805767}{415389067374386774218664204327} +$$

$$\frac{1084381986154211644}{415389067374386774218664204327}\alpha^5 + \frac{111621349705882562664459003881872757}{1058826732737311887483375056829523}\alpha$$

$$z = \frac{1}{2549}\alpha$$

$$\alpha = \text{RootOf}(Z^6 + 10473Z^5 + 45681652Z^4 + 106222031174Z^3 +$$

$$138869253992833Z^2 + 96779995853143649Z + 28089018396122120007)$$

Each of these are algebraic numbers and thus are a multiplication away from being algebraic integers which we can use to approximate our integral basis, so we input each of them into our algorithm to produce the following solution:

$$y = \frac{295}{2549} + \frac{190}{2549}\alpha^3 + \frac{205}{2549}\alpha^4 + \frac{13}{2549}\alpha^2$$

$$x = \frac{-1263}{2549} - \frac{79}{2549}\alpha^3 + \frac{116}{2549}\alpha^4 + \frac{169}{2549}\alpha^2$$

$$z = \frac{-1731}{2549} - \frac{59}{2549}\alpha^2 - \frac{78}{2549}\alpha^3 + \frac{50}{2549}\alpha^4$$

Where our new representative is

$$\alpha = \text{RootOf}(Z^6 - Z^5 + 1)$$

This is clearly an improvement in terms of bit size.

In the next example we take a parametrization which is particularly nasty and compute a nicer reparametrization using the same process. Let:

$$f = -2624 + 27296x + 151520yx^4 + 257040x^3y^2 - 9408y - 72612x^2 + 52796x^3 - 8348x^4 +$$

$$44676x^5 + 95952xy + 528x^2y - 371936x^3y - 468448x^2y^2 + 362752xy^2 - 6256y^2 + 62880xy^4 -$$

$$391664y^3x + 157040y^3x^2 + 187584y^3 - 76608y^4 + 7840y^5$$

MAPLE parametrizes f as $X(t) =$

$$(2322946860161800295940053161t^2 - 355177836316644147839664858562560t -$$

$$398952999326251465506204804132510892032) * (111958974658262258228833464$$

$$633252366728341t^3 + 241218127396230898746354476689066554841504653312t^2 +$$

$$120216160848442302304865507382924194464419866807894016t + 18973244389596$$

$$591039200508646281165042925815057688465244160) /$$

$$(260074748649344881042029603731344399577713658476424351714303185335901t^5 -$$

$$99413365938378956304645871633057077091315545811607852803314554418183782400t^4 -$$

$$446663687414055076077356459261240869180221779147154092331463719947116633254789120t^3 -$$

$$\begin{aligned}
&3081179898447054918665604073843386286508274220117650630677686213454114945467148559 \\
&97440t^2 - 8846228595087639973447972387446409221730087121154033403691086830278244766 \\
&4298474240863109120t - 9564875086568982293923283296673591816902912619227774652575812 \\
&017438876753518118415237972618117120)
\end{aligned}$$

$$Y(t) =$$

$$\begin{aligned}
&-3(2322946860161800295940053161t^2 + 1490691489492566250521403944443904t + \\
&284989871944007641845159360874898522112) * (111958974658262258228833464633 \\
&252366728341t^3 + 274580110500798519502415187814341628088682617856t^2 + 134 \\
&997798586363021381641319157554175228056886593978368t + 206105632319019166 \\
&08689254094480846754620696455848986148864) / \\
&(260074748649344881042029603731344399577713658476424351714303185335901t^5 - \\
&99413365938378956304645871633057077091315545811607852803314554418183782400t^4 - \\
&44666368741405507607735645926124086918022177914715409233146371994711663325 \\
&4789120t^3 - 308117989844705491866560407384338628650827422011765063067768621 \\
&345411494546714855997440t^2 - 8846228595087639973447972387446409221730087121 \\
&1540334036910868302782447664298474240863109120t - 95648750865689822939232832 \\
&96673591816902912619227774652575812017438876753518118415237972618117120)
\end{aligned}$$

In order to improve the parametrization we would like nice values of x and y to occur at nice values of t . So we choose a root of $X(t)$, namely:

$$\begin{aligned}
\alpha = &\text{RootOf}(111958974658262258228833464633252366728341Z^3 + 24121 \\
&8127396230898746354476689066554841504653312Z^2 + 120216160848442302304865507 \\
&382924194464419866807894016Z + 189732443895965910392005086462811650429258150 \\
&57688465244160)
\end{aligned}$$

Substituting this value for t we should get a zero for x and an algebraic number for y . Using α and this algebraic number $X(\alpha)$ we use our process to come up with a better minimal polynomial and the following substitution:

$$\begin{aligned}
\beta = &\text{RootOf}(Z^3 + 2Z + 2) \\
\alpha = &\frac{-53763040707756404736}{48196959034381} + 297984\beta - 297984\beta^2
\end{aligned}$$

We now find a Moebius transform that sends α to β , and this should simplify the entire parametrization while remaining an equivalent parametrization. Once we have done this substitution we obtain our reparametrization:

$$X(t) = \frac{(t^3 + 2t + 2) * (t^2 - 2)}{(t^5 + 2)}$$

$$Y(t) = \frac{(t^3 + 3t + 3) * (t^2 + 2)}{(t^5 + 2)}$$

We have also discovered an algorithm which uses a similar method for reparametrizing a nasty parametrization via a Moebius transform, when we find any linear factors.