ELIMINATION VIA SATURATION

MOHAMED BARAKAT, MARKUS LANGE-HEGERMANN, AND SEBASTIAN POSUR

ABSTRACT. This short paper presents saturation-based algorithms for homogenization and elimination. Saturation can be computed using syzygies, hence the Gröbner-bases-driven algorithms work with respect to any monomial order, in particular, they do not require the use of block-elimination orders. The used saturation is a translation of the geometric fact that the projective closure of an affine scheme has no components in the hyperplane at infinity.

1. INTRODUCTION

Elimination has many applications, for example solving systems of equations, computing primary decompositions, and computing Zariski closures of images of morphisms of varieties. Furthermore, using elimination, one can compute ideal quotients and saturations of ideals, either by iterating ideal quotients or using “Rabinowitch’s trick”. This leads us to our first question:

Q1. Is the converse true, i.e., can one use saturation to eliminate?

Eisenbud writes in [Eis95, Chapter 15]: “The kinds of problems that can be attacked with Gröbner bases can be very roughly divided into two groups: constructive module theory and elimination theory.” This motivates our second question:

Q2. Is constructive elimination theory a special case of constructive module theory?

In elimination theory one computes Gröbner bases w.r.t. a block-elimination order. For the module theoretic applications any global order can be used, e.g., the degree-reverse-lexicographic order. So the second question can be reformulated as follows:

Q2’. Can one use the degree-reverse-lexicographic order for elimination?

This paper answers the above questions affirmatively.

Geometrically speaking, we are interested in the Zariski closure of the image of an affine subscheme $X \subset \mathbb{A}_B^n$ (over a base ring $B$) under the affine projection morphism $\pi : \mathbb{A}_B^n \to \text{Spec } B$. The idea employed in this paper is to factor $\pi$ over $\mathbb{P}_B^n$ and to use the fact that the projective closure $\overline{X}$ (of $X$ in $\mathbb{P}_B^n$) has no components in the hyperplane at infinity $H := \mathbb{P}_B^n \setminus \mathbb{A}_B^n$ in order to represent $\overline{X}$ (non-canonically) as the Zariski...
Algebraically speaking, our approach to elimination of ideals (or submodules) in polynomial rings uses a certain homogenization thereof. Homogenizing an ideal $I = \mathcal{I}(X)$ in the relative case ($B$ not a field) usually relies on computing a Gröbner basis w.r.t. a block-elimination order (cf., e.g., [Eis95, Prop. 15.31]), and it is precisely this order which we want to offer an alternative to. Instead, the homogenized ideal $I^h$ can be computed by homogenizing any generating set of $I$ followed by a saturation w.r.t. the new homogenizing indeterminate. The original elimination of the ideal $I$ can now be computed by evaluating certain indeterminates to zero in a generating set of $I^h$.

More formally, let $R := B[x_1, \ldots, x_n]$ be a polynomial ring over the commutative ring $B$. We show how to compute the intersection $I \cap B$ for an ideal $I \subseteq R$ given by a generating set $G \subseteq I$, i.e., how to eliminate the indeterminates $x_1, \ldots, x_n$, without using a block-elimination order. We base the alternative algorithm on the observation that $I \cap B$ is equal to the intersection of $B$ with the homogenization of $I$. More precisely, for $f \in R$ denote by $f^h \in S := B[x_0, x_1, \ldots, x_n]$ the homogenization of $f$ w.r.t. the new indeterminate $x_0$. The above mentioned equality reads $I \cap B = I^h \cap B$ (Lemma 2.7), where $I^h = \langle f^h \mid f \in I \rangle \subseteq S$ denotes the homogenization of $I$. The homogenization $I^h$ can be computed using the equality $I^h = \langle g^h \mid g \in G \rangle : x_0^\infty$ (Proposition 2.4). Finally, we obtain a generating set of the elimination ideal $I \cap B = I^h \cap B \subseteq B$ by simply evaluating $x_0, \ldots, x_n$ to zero in a generating set of $I^h$ (Corollary 2.9).

Using homogenization to transfer a given computational task to an easier one is a common principle (see, e.g., [KR05, Tutorial 51]). Instead of dehomogenizing the result of a homogeneous computation, we take global sections by simply evaluating indeterminates to zero.

The above statements are proved in Section 2 with no further assumption on the unital base ring $B$ other than being commutative. In Appendix A we give alternative, more conceptual proofs of Proposition 2.4 and Lemma 2.7.

Algorithmically speaking, the only computationally non-trivial step in the above sketched algorithm is the saturation w.r.t. $x_0$. It is well-known that saturations can be computed by iterating ideal quotients, each of which can be computed using syzygies, for certain classes of base rings\footnote{for which the iterated ideal quotients stabilizes after finitely many steps.} $B$ (cf. [AL94, §3.8] or [Eis95, §15.10.6]):

In case $B = k[b_1, \ldots, b_m]$ is a polynomial ring over a computable field $k$ we can use any term order of $S = k[b_1, \ldots, b_m, x_0, x_1, \ldots, x_n]$ to compute syzygies. This very convenient setting allows performing computations in one big ring, as $B$ receives no special treatment in the Gröbner basis algorithm. Similarly, if $B = k[b_1, \ldots, b_m]/L$ we can simply add any set of generators of $L$ to $I$ and proceed as above.

For the computability of syzygies over the ring $S = B[x_0, \ldots, x_n]$ it suffices to assume that $B$ has effective coset representatives [AL94, Theorem 4.3.15]. A ring $B$ is said to have effective coset representatives if for every ideal $L \subseteq B$ we can algorithmically find a set $T$ of coset representatives of $B/L$, such that for every $b \in B$ we can compute the unique $t \in T$ with $b + L = t + L$. It is immediate that computable fields and the ring of integers $\mathbb{Z}$ have effective coset representatives. Furthermore, if $B$ has effective coset representatives then also its residue class rings and polynomial rings there over.
We do not claim that our saturation-based algorithm can outperform the direct use of block-elimination orders. In fact, our straightforward implementation in homalg [hom17] was significantly slower than direct elimination using a block-elimination order, where the Gröbner bases computations in both cases were delegated to SINGULAR [DGPS16]. However, our implementation relies on SINGULAR’s general procedures to compute syzygies, which are a priori not optimized for saturation with respect to a single indeterminate.

2. Correctness of the Algorithm

Let $B$ be a unital commutative ring, $R := B[x_1, \ldots, x_n]$ and $S := B[x_0, x_1, \ldots, x_n]$ polynomial rings over $B$, We view $S$ as a graded ring over $B$ equipped with its standard grading, i.e., $\deg(x_i) = 1$ for all $i = 0, \ldots, n$, and $\deg(b) = 0$ for all $b \in B \setminus \{0\}$.

2.1. Homogenization. For $f \in R$ denote by $f^h$ the homogenization of $f$ in $S$ w.r.t. the indeterminate $x_0$:

$$f^h := x_0^{\deg f} f \left( \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0} \right) \in S.$$ 

Note that possible different degrees of the summands or cancelation of leading terms prevent the homogenization $f \mapsto f^h$ from being additive. However, as a direct consequence of the definition one gets

**Remark 2.1 (Generalized additivity).** Let $f = \sum_i f_i \in R$ and $m := \max_i \{\deg f_i\}$. Then

$$x_0^{m-\deg f} f^h = \sum_i x_0^{m-\deg f_i} f_i^h.$$  

If $B$ is a domain then the homogenization is multiplicative; more generally:

**Remark 2.2 (Generalized multiplicativity).** Let $f, g \in R$. Then

$$x_0^k (fg)^h = f^h g^h \quad \text{with} \quad k := \deg f + \deg g - \deg(fg) \geq 0.$$  

If $B$ is a domain then $k = 0$, trivially.

On the other hand the dehomogenization

$$\varphi : S \rightarrow R, \begin{cases} x_0 \mapsto 1, \\ x_i \mapsto x_i & i \neq 0 \end{cases}$$

is an epimorphism of $B$-algebras with kernel $\langle x_0 - 1 \rangle$. Moreover, $\varphi(r^h) = r$ for all $r \in R$ and $\varphi(s)^h = s$ for all homogeneous $s \in S$ with $s \notin \langle x_0 \rangle$.

The homogenization of an ideal $I \unlhd R$ is the homogeneous ideal $I^h := \langle f^h \mid f \in I \rangle \unlhd S$, generated by the homogenization of all elements of $I$. We now show that homogenized ideals are saturated w.r.t. $x_0$. In Proposition 2.4 we show the converse, namely that $I^h$ can be computed by such a saturation.

**Lemma 2.3.** The homogenization $I^h \unlhd S$ of an ideal $I \unlhd R$ is saturated w.r.t. $x_0$, i.e.,

$$I^h = I^h : x_0^{\infty} := \{ f \in S \mid \exists k \in \mathbb{N}_0 : x_0^k f \in I^h \}.$$  

---

5We do not need that $B$ is a polynomial ring to prove correctness.

6This follows from $\deg(fg) = \deg(f) + \deg(g)$ if $B$ is a domain. If $B$ is not a domain then $\deg(fg) \leq \deg(f) + \deg(g)$: consider, e.g., the square of $2x + 1$ in $(\mathbb{Z}/4\mathbb{Z})[x]$. 


This statement is the manifestation of the geometric fact that the closure \( V(I^h) \subset \mathbb{P}_B^n \) of the vanishing set \( V(I) \subset \mathbb{A}_B^n \subset \mathbb{P}_B^n \) does not include components in the hyperplane \( V(x_0) \subset \mathbb{P}_B^n \) at infinity.

**Proof.** It suffices to prove the inclusion \( I^h \supseteq I^h : x_0^\infty \). Let \( f \in I^h : x_0^\infty \) homogeneous. We can assume that \( f \notin \langle x_0 \rangle \), since such elements generate \( I^h : x_0^\infty \). Then there exists a nonnegative integer \( k \) such that \( x_0^k f \in I^h \), i.e., there exist \( f_i \in I \) and homogeneous \( s_i \in S \) such that \( x_0^k f = \sum_i s_i f_i^h \). Applying the dehomogenization \( \varphi \) yields \( \varphi(f) = \varphi(x_0^k f) = \sum_i \varphi(s_i) f_i \in I \). As \( \varphi(f) \in I \) we finally have \( f = \varphi(f)^h \in I^h \), where the last equality holds since \( f \notin \langle x_0 \rangle \) by the assumption. \( \square \)

Homogenizing a generating set of an ideal does not generally yield a generating set of the homogenized ideal (cf. Example 2.5). However, the necessary saturatedness condition from Lemma 2.3 suffices in the following sense:

**Proposition 2.4.** Let \( G \) be a generating set of an ideal \( I \subseteq R \). Then

\[
I^h = J : x_0^\infty
\]

for the homogeneous ideal \( J := \langle g^h \mid g \in G \rangle \subset I^h \subseteq S \) generated by the homogenized elements of \( G \).

Geometrically speaking, the vanishing set \( V(J) \) (of the homogenization of a generating set of \( I \)) coincides with \( V(I^h) \) up to possible extra components of \( V(J) \) which are contained in the hyperplane \( V(x_0) \) at infinity (see Example 2.5).

**Proof.** The inclusion \( I^h \supseteq J : x_0^\infty \) follows from the inclusion \( I^h \supseteq J \) and Lemma 2.3.

We now prove the reverse inclusion. Consider an element \( f^h \) for \( f \in I \) (by definition \( I^h \) is generated by elements of this form). Since \( G \) is a generating set of \( I \) we can write \( f = \sum_{g \in G'} r_g g \) for some \( r_g \in R \) and a finite subset \( G' \subseteq G \). Set \( m := \max\{\deg r_g + \deg g \mid g \in G'\} \). Then homogenizing the above \( R \)-linear combination of \( f \) yields the \( S \)-linear combination

\[
x_0^{m-\deg f} f^h = \sum_{g \in G'} x_0^{m-\deg(r_g g)} (r_g g)^h \tag{Remark 2.1}
= \sum_{g \in G'} x_0^{m-(\deg r_g + \deg g)} r_g^h g^h \in J \tag{Remark 2.2}.
\]

Hence, \( f^h \in J : x_0^\infty \). \( \square \)

Note that if our base ring \( B \) is a field, proofs of Lemma 2.3 and Proposition 2.4 are given in [KR05, Corollary 4.3.7, Corollary 4.3.8.a]. See also [Eis95, Exer. 15.40].

2.2. **Examples.** If \( B = k[b_1, \ldots, b_m] \) is a polynomial ring over a field \( k \), then the above saturation can be computed by Gröbner bases algorithms with respect to any monomial order.

Homogenizing a Gröbner basis of the ideal \( I \subset R \) w.r.t. the block-elimination order \( b_i \prec x_j \) already yields a generating set of \( I^h \subseteq S \), i.e., there is no need for subsequent saturation (cf. [Eis95, Prop. 15.31] or [AL94, Exer. 1.6.19]).

However, in our alternative approach to homogenization using saturation (Proposition 2.4) we are free in choosing a monomial order. One could proceed as follows: Use the degree-reverse lexicographical order (degrevlex) in \( S \) to compute the saturation, as it is the fastest
order on average. We even suggest to start in Proposition 2.4 with a Gröbner basis \( G \) of \( I \)
 w.r.t. degrevlex in \( R \) (since then for \( B = k \) no subsequent saturation is required\(^3\)).

**Example 2.5.** Consider \( B = k = \mathbb{Q} \), \( R = \mathbb{Q}[x_1, x_2] \), \( G := \{ x_1^2, x_2 - x_1^2 \} \subset R \), and \( I = (G) \). Then \( J : = (G^\infty) = \langle x_1^2, x_0x_2 - x_1^2 \rangle = \langle x_1^2, x_0x_2 \rangle \subseteq \langle x_1^2, x_2 \rangle = I^h \). However, the
 saturation \( J : = x_0^\infty = I^h \), complying with Proposition 2.4. If we would have started with the
 Gröbner basis \( G' : = \{ x_1^2, x_2 \} \) of \( I \) the saturation step would’ve been obsolete.

Unless \( B = k \), the next example shows that homogenizing a Gröbner basis of \( I \) w.r.t.
degrevlex (contrary to the above mentioned block-elimination order) does not generally
yield a generating set of \( I^h \) and a subsequent saturation is necessary.

**Example 2.6.** Consider \( B = \mathbb{Q}[b_1, b_2, b_3], R = B[t] \), and \( I = \langle b_i - t^i \mid i = 1, 2, 3 \rangle \triangleleft R \)
the ideal defining the twisted cubic. A Gröbner basis of \( I \) w.r.t. degrevlex is \( G := \{ b_1 - t, t^2 - b_2, b_2t - b_3, b_3^2 - b_3t \} \). Then \( J : = \langle b_1s - t, t^2 - b_2s^2, b_2t - b_3s, b_3^2s - b_3t \rangle \triangleleft S = B[s, t] \) and for obvious
degree reasons \( J \) cannot contain elements of degree 0 in \( s \) and \( t \), i.e., \( J \cap B = \{ 0 \} \).
This example shows that homogenizing a Gröbner basis of \( I \) w.r.t. the degrevlex does not
generally yield a generating set of \( I^h = J : = \langle s \rangle^\infty = \langle b_1s - t, b_1b_2 - b_3, b_1^2 - b_2 \rangle \).

2.3. **Elimination via homogenization.** Homogenizing an ideal \( I \triangleleft R \) does not add additional
elements from \( B \) to the ideal, allowing us to use homogenization for elimination,
which is our main goal:

**Lemma 2.7.** For an ideal \( I \triangleleft R \) we have \( I^h \cap B = I \cap B \).

*Proof.* The homogeneity of elements of \( B \) yields the inclusion \( I^h \cap B \subset I \cap B \). So we
only need to show the inclusion \( I^h \cap B \subseteq I \cap B \). To this end let \( b \in I^h \cap B \). As \( b \in I^h \) there
exist finitely many \( f_i \in I \) and homogeneous \( s_i \in S \) such that \( b = \sum_i s_i f_i^h \). Applying the
dehomogenization \( \varphi \) yields \( b = \varphi(b) = \sum_i \varphi(s_i) \varphi(f_i) = \sum_i \varphi(s_i) f_i \in I \).

Since \( B \) is the degree zero part of \( S \), this intersection \( I^h \cap B \) is just the degree zero part of
\( I^h \). We shortly explain on how to read off this degree zero part of any homogeneous ideal:

**Remark 2.8.** Let \( H \triangleleft S \) be a homogeneous ideal. By definition, a polynomial is contained
in \( H \) iff all of its homogeneous parts are. Hence, given a generating set \( G \) of \( H \), the set
\( G' := \{ p_i \mid p_i \in G, i \in \mathbb{Z}_{\geq 0} \} \) of the homogeneous parts of \( G \) is also a generating set of
\( H \). Removing a polynomial \( p \in G' \) of degree \( d \) from \( G' \) does not affect the parts of degree
smaller than \( d \), i.e., \( H \) is equal to \( (G' \setminus \{ p \}) \triangleleft S \) in all degrees smaller \( d \). In particular,
\( G_0' : = \{ p \in H' \mid \deg(p) = 0 \} = \{ p_{|x_0=0, \ldots, x_n=0} \mid p \in G \} \) is a generating set of the degree 0
part \( H \cap B \).

**Corollary 2.9.** Let \( I \triangleleft R \) be an ideal. Evaluating the indeterminates \( x_0, \ldots, x_n \) to zero
in a generating set of \( I^h \triangleleft S \) yields a generating set of \( I \cap B = I \cap B \).

Proposition 2.4 gives an algorithm to compute a generating set for \( I^h \) as a Gröbner basis
of \( J : = x_0^\infty \) by saturating \( J \) w.r.t. the indeterminate \( x_0 \). We again emphasize that we do not
need any elimination order, as a saturation can be computed by iterated syzygies w.r.t. any
order. By Lemma 2.7 and Corollary 2.9 we can then compute the elimination \( I \cap B \) by
evaluating the \( x_i \) to zero in \( I^h \).

**Example 2.10.** Continuing Example 2.6 we get \( I \cap B = I^h \cap B = \langle b_1b_2 - b_3, b_1^2 - b_2, b_2^2 - b_1b_3 \rangle \cap B \)
(with Gröbner basis \( \{ b_1b_2 - b_3, b_1^2 - b_2, b_2^2 - b_1b_3 \} \)).

\(^3\)This is [CLO92, Theorem 8.4.4 and Exer. 8.4.5], a special case of [Eis95, Prop. 15.31].
2.4. Generalization to submodules. All statements and above proofs easily generalize to the case of submodules of finite rank free modules. For \( \ell \in \mathbb{N}_0 \) let \( I \subseteq R^\ell \) be an \( R \)-submodule generated by the finite set \( G \subseteq R^\ell \). For \( f = (f_1, \ldots, f_\ell) \in R^\ell \) define \( f^h = (f_1^h, \ldots, f_\ell^h) := (x_0^{\deg(f_1)}, \ldots, x_0^{\deg(f_\ell)}) \), where \( i_j \) is determined by the equality \( i_j + \deg(f_j) = \deg(x_0^{i_j}) \). The homogenization of \( I \) is the graded \( S \)-submodule \( I^h = \{ f^h \mid f \in I \} \subseteq S^\ell \) and the saturation of \( J := \{ f^h \mid f \in G \} \) by \( x_0 \) is \( J : x_0^\infty = \{ f \in S^\ell \mid \exists k \in \mathbb{N}_0 : x_0^k f \in J \} \). Elimination now means computing the intersection \( I \cap B^\ell = I^h \cap B^\ell \) with \( B^\ell := \{ (r_1, \ldots, r_\ell) \mid r_i \in B \} \subseteq R^\ell \), which reduces to evaluating the indeterminates \( x_0, \ldots, x_n \) to zero in a generating set of \( I^h \).

APPENDIX A. ALTERNATIVE PROOFS

In this section we give some alternative, more conceptual proofs of Proposition 2.4 and Lemma 2.7.

Alternative proof of Proposition 2.4. Define the \( B \)-algebra homomorphisms

\[
\begin{array}{ccc}
R & \xrightarrow{\alpha} & S_{x_0} \\
x_i & \mapsto & \frac{x_i}{x_0} \\
\beta & \xleftarrow{} & S \\
\frac{x_i}{x_0} & \mapsto & x_i
\end{array}
\]

We write \( \alpha_* \) and \( \beta_* \) for the operators that send an ideal to its extension with respect to \( \alpha \) and \( \beta \), respectively. Now, given any subset of elements \( F \subseteq R \), we have

\[
\beta^{-1} \alpha_*(\langle f \mid f \in F \rangle_R) = \beta^{-1}(\langle f \left( \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0} \right) \mid f \in F \rangle_{S_{x_0}})
\]

\[
= \beta^{-1}(\langle f^h \mid f \in F \rangle_{S_{x_0}})
\]

\[
= \beta^{-1} \beta_*(\langle f^h \mid f \in F \rangle_S)
\]

\[
= \langle f^h \mid f \in F \rangle_S : x_0^\infty.
\]

On the one hand, setting \( F = I \) yields

\[
\beta^{-1} \alpha_*(I) = I^h : x_0^\infty = I^h,
\]

(Lemma 2.3)

and on the other hand, setting \( F = G \) gives us

\[
\beta^{-1} \alpha_*(I) = \langle g^h \mid g \in G \rangle : x_0^\infty = J : x_0^\infty.
\]

Remark A.1. Let \( B \) be a commutative ring and let \( \overline{R}, \overline{S} \) be \( B \)-algebras with structure morphisms \( \rho : B \to \overline{R}, \) \( b \mapsto b \cdot 1_{\overline{R}} \) and \( \sigma : B \to \overline{S}, \) \( b \mapsto b \cdot 1_{\overline{S}} \). Assume that there exists a \( B \)-algebra homomorphism \( \varphi : \overline{S} \to \overline{R} \). Then

\[
\ker \sigma \subseteq \ker \rho.
\]

Proof. The statement that \( \varphi \) is a morphism of \( B \)-algebras means that \( \varphi \circ \sigma = \rho \) and hence \( \ker(\varphi \circ \sigma) = \ker \rho \). This implies the claim.

The categorical formulation would be...
to construct the mono $\iota$ as the unique lift of $\kappa_{\sigma}$ along the kernel embedding $\kappa_{\rho}$, which exists since $\rho \circ \kappa_{\sigma} = 0$ by the commutativity of the right square. Since $\kappa_{\rho} \circ \iota = \kappa_{\sigma}$ is a mono it follows that $\iota$ is itself a mono. \hfill \Box

**Alternative proof of Lemma 2.7.** We define the $B$-algebras $\overline{R} := R/I$ and $\overline{S} := S/I^h$, and denote their structure morphisms by $\rho$, $\sigma$, respectively. Their kernels are given by $I \cap B$ and $I^h \cap B$, respectively, and the inclusion $I^h \cap B \supset I \cap B$ was the easy inclusion in the first proof of Lemma 2.7. Furthermore, the dehomogenization $\varphi : S \to R$ induces a $B$-algebra homomorphism $\overline{\varphi} : \overline{S} \to \overline{R}$. We can now apply Remark A.1 which completes the proof. \hfill \Box

**REFERENCES**

[AL94] William W. Adams and Philippe Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994. MR 1287608 (95g:13025) 1, 2, 4

[CLO92] D. Cox, J. Little, and D. O’Shea, *Ideals, varieties, and algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. An introduction to computational algebraic geometry and commutative algebra. MR MR1189133 (93j:13031) 5

[DGPS16] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, *SINGULAR 4-1-0 — A computer algebra system for polynomial computations*, http://www.singular.uni-kl.de, 2016. 3

[Eis95] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995. MR MR1322960 (97a:13001) 1, 2, 4, 5

[hom17] homalg project authors, *The homalg project — Algorithmic Homological Algebra*, (http://homalg-project.github.io), 2003–2017. 3

[KR05] Martin Kreuzer and Lorenzo Robbiano, *Computational commutative algebra. 2*, Springer-Verlag, Berlin, 2005. MR MR2159476 (2006h:13036) 2, 4