When does $\langle T \rangle$ equal $\mathrm{sat}(T)$?

Wei Pan

joint work with

François Lemaire, Marc Moreno Maza and Yuzhen Xie

MOCAA M^3 workshop
UWO
May 7, 2008

Introduction

- Given a regular chain T, the **saturated ideal** $\mathrm{sat}(T)$ is a fundamental object *attached* to T.
- The questions like
  - Is p an element of $\mathrm{sat}(T)$?
  - Is p a zero-divisor modulo $\mathrm{sat}(T)$?

  can be answered **without** computing a system of generators of $\mathrm{sat}(T)$.
- In some sense, T is a **black box representation** of $\mathrm{sat}(T)$.
- However, in this representation, the **inclusion test** problem
  - Does $\mathrm{sat}(U) \subseteq \mathrm{sat}(T)$ hold?

  is hard.

Introduction

- If a system of generators of U is known, then the inclusion test reduces to the ideal membership problem.
- How to compute a system of generators of $\operatorname{sat}(T)$?
  - The only known general technique is via Gröbner bases.
  - If $\dim(\operatorname{sat}(T)) = 0$, then $\boxed{\operatorname{sat}(T) = \langle T \rangle}$.
- Our objectives are, in **positive** dimension,

(1) characterizing the T's for which $\operatorname{sat}(T) = \langle T \rangle$ holds;

(2) deciding $\operatorname{sat}(T) = \langle T \rangle$ without Gröbner basis computation.

Outline

- Primitivity of polynomials
- Regular chain and saturated ideal
- Primitive regular chain
- Primitivity checking algorithm
- Experimentation and discussion

Primitive polynomials of $A[x]$

- Here A is a unique factorization domain (UFD): $\mathbb{Z}, \mathbb{Q}[x_1, \ldots, x_n]$.
- Let $f \in A[x]$ of degree $d > 0$, and write f as

$$f = a_d x^d + \cdots + a_0.$$

  Then f is called **primitive** if $\gcd(a_d, \ldots, a_0) = 1$.

- Examples:

  (1) $2x + 3 \in \mathbb{Z}[x]$ is primitive;

  (2) $x_1 x_3 + x_2 \in A[x_3]$ is primitive with $A = \mathbb{Q}[x_1, x_2]$;

  (3) $x_1 x_2 \in A[x_2]$ is **not** primitive with $A = \mathbb{Q}[x_1]$.

Saturation operation

- Let R be a commutative ring, $h \in R$ and I be an ideal of R.
- The **saturated ideal** of I by h is

$$I : h^{\infty} = \{f \in R \mid fh^k \in I, \text{for some } k \in \mathbb{Z}_{\geq 0}\}.$$

- One side inclusion $I \subseteq I : h^{\infty}$; it can be strict.
- Examples:

(1) $\langle 12 \rangle : 2^{\infty} = \langle 3 \rangle \iff 12/2^2 = 3$;

(2) $\langle x_1x_3 + x_2 \rangle : x_1^{\infty} = \langle x_1x_3 + x_2 \rangle$;

(3) $\langle x_1x_2 \rangle : x_1^{\infty} = \langle x_2 \rangle$.

- **Proposition**: $f = a_dx^d + \cdots + a_0 \in A[x]$ is primitive iff

$$\langle f \rangle : a_d^{\infty} = \langle f \rangle,$$

where A is a UFD.

Regular chain and saturated ideal

- **Notations**:
  Let $T = \{t_1, \ldots, t_s\}$ be a triangular set in $\Bbbk[x_1 \prec \cdots \prec x_n]$.
  Each $t \in T$ is a univariate polynomial in its **main variable** $\mathrm{mvar}(t)$.
  The leading coefficient of t is called its **initial**, denoted by $\mathrm{init}(t)$.

- The **saturated ideal** $\mathrm{sat}(T)$ of a triangular set T is

$$\mathrm{sat}(T) = \langle T \rangle : h^{\infty},$$

  where h is the product of initials of $t_i{}'s$.

- **Regular chain**:
  (1) if $T = \emptyset$, then it is a regular chain and $\mathrm{sat}(T) = \langle 0 \rangle$;
  (2) if $T = C \cup \{p\}$, then T is a regular chain, iff C is a regular chain and $\mathrm{init}(p)$ is regular modulo $\mathrm{sat}(C)$.

Regular chain and saturated ideal

- For example, in $\mathbb{k}[x \succ y \succ u \succ v]$

$$\begin{aligned} \mathrm{mvar}(uy+v) &= y, & \mathrm{sat}(uy+v) &= \langle uy+v\rangle : u^{\infty} \\ \mathrm{init}(uy+v) &= u, & &= \langle uy+v\rangle. \end{aligned}$$

  Also v is regular modulo $\langle uy+v\rangle$.

- Saturating $\langle T\rangle$ by the product of the initials of T will **kick out** "bad" components.

$$T : \left| \begin{array}{l} vx+u, \\ uy+v, \end{array} \right. \qquad \begin{aligned} \langle T\rangle &= \langle uy+v, xy-1\rangle \cap \langle u, v\rangle, \\ \mathrm{sat}(T) &= \langle uy+v, xy-1\rangle. \end{aligned}$$

  Here $\mathrm{sat}(T)$ is strictly larger than $\langle T\rangle$.

- $\mathrm{sat}(T)$ is **unmixed**: all associated primes of $\mathrm{sat}(T)$ are minimal primes of $\mathrm{sat}(T)$.

The question

- **Proposition**: $f = a_d x^d + \cdots + a_0 \in A[x]$ is primitive iff

$$\langle f \rangle : a_d^\infty = \langle f \rangle,$$

  where A is a UFD.

- This proposition can be re-stated as: For each $f \in \mathbb{k}[x_1, \ldots, x_n]$

$$\mathrm{sat}(f) = \langle f \rangle \iff f \text{ is primitive in its main variable.}$$

- $\boxed{\text{When does } \langle T \rangle \text{ equal } \mathrm{sat}(T)\text{?}}$ **Primitive regular chains**?

A remark

- A strightforward generalization of primitivity is not enough. Consider $T = \{t_1 = uy + v, t_2 = vx + u\}$. Then
  - t_1 is primitive over $\mathbb{k}[u, v]$;
  - t_2 is primitive over $\mathbb{k}[u, v, y]$.

  However, $\mathrm{sat}(T)$ is strictly larger than $\langle T \rangle$.

Primitivity over a commutative ring R

A nonconstant polynomial $p = a_e x^e + a_{e-1}x^{e-1} + \cdots + a_0 \in R[x]$ is **not weakly primitive** if there exists a $\beta \in R$ such that

$$a_e \mid \beta a_0, \; \ldots, \; a_e \mid \beta a_{e-1}, \quad \text{but} \quad a_e \nmid \beta. \tag{1}$$

- For instance, $p = 6x + 3 \in \mathbb{Z}[x]$ is not weakly primitive, since $\beta = 2$ satisfies (1): $6 \mid 2 \cdot 3$ and $6 \nmid 2$.
- The β may be seen as a co-content wrt a_e.
- If R is a UFD, then $\boxed{\text{weakly primitive} = \text{primitive}}$.

Primitive regular chain

- **Definition**:
  Let $T = C \cup \{p\}$ be a regular chain. Then T is **primitive** if C is primitive and p is a weakly primitive polynomial regarded as a univariate polynomial in its main variable over $\mathbb{k}[\mathbf{x}]/\langle C \rangle$.
- This is a proper generalization: If $T = \{p\}$ consists of a single polynomial, then T is primitive iff p is primitive.
- **Theorem**: $\boxed{\text{Regular chain } T \text{ is primitive iff } \langle T \rangle = \mathrm{sat}(T) \text{ holds.}}$

Remark

In the proof of the theorem,

- if T is not primitive, we exhibit a polynomial $p \in \mathrm{sat}(T) \setminus \langle T \rangle$;
- if T is primitive, we express every polynomial of $\mathrm{sat}(T)$ as a linear combination of polynomials in T;
- we rely on a Generalized Gauss Lemma: **Dedekind-Mertens Lemma**.

Primitivity checking algorithm

- **Lemma**:
  Polynomial $p = a_e x^e + \cdots + a_0 \in R[x]$ is **weakly primitive** iff
  (1) a_e is invertible in R; or
  (2) $\mathrm{tail}(p) = p - a_e x^e$ is regular modulo $\langle a_e \rangle$.
- Primitivity test for a regular chain reduces to an **invertibility test** and a **regularity test**.
- Let F be a list of polynomials and $f \in \Bbbk[\mathbf{x}]$. Then
  (1) f is invertible modulo $\langle F \rangle$ iff **Triangularize**$(F \cup \{f\}) = \emptyset$.
  (2) f is regular modulo $\langle F \rangle$ iff f is not contained in any associated prime of $\langle F \rangle$.

  Regularity test (2) is hard for a general ideal.

Primitivity checking algorithm

- **Lemma**:

  Polynomial $p = a_e x^e + \cdots + a_0 \in R[x]$ is **weakly primitive** iff

  (1) a_e is invertible in R; or

  (2) $\mathrm{tail}(p) = p - a_e x^e$ is regular modulo $\langle a_e \rangle$.

- Primitivity test for a regular chain reduces to an **invertibility test** and a **regularity test**.

- Let F be a list of polynomials and $f \in \Bbbk[\mathbf{x}]$. Then

  (1) f is invertible modulo $\langle F \rangle$ iff **Triangularize**$(F \cup \{f\}) = \emptyset$.

  (2) f is regular modulo $\langle F \rangle$ iff f is not contained in any associated prime of $\langle F \rangle$.

  Regularity test (2) is hard for a general ideal.

IsPrimitive algorithm

Input: T, a regular chain of $\mathbb{k}[x_1, \ldots, x_n]$.

Output: *true* if T is primitive, *false* otherwise.

1: **if** $|T| = 1$ **then**
2: $\quad t \leftarrow$ the defining polynomial of T
3: $\quad$ **if** content$(t) \in \mathbb{k}$ **then** *return true* **else** *return false*
4: **else**
5: $\quad$ write T as $T' \cup \{t\}$, where t has the greatest main variable
6: $\quad$ **if not IsPrimitive**(T') **then**
7: $\quad\quad$ *return false*
8: $\quad$ **else**
9: $\quad\quad h \leftarrow \mathrm{init}(t)$, $r \leftarrow \mathrm{tail}(t)$
10: $\quad\quad$ **for** $U \in$ **RegularChains** :− **Triangularize**$(T' \cup \{h\})$ **do**
11: $\quad\quad\quad$ **if** $\mathrm{ires}(r, U) = 0$ **then** *return false*
12: $\quad\quad$ **end for**
13: $\quad\quad$ *return true*
14: $\quad$ **end if**
15: **end if**

Line 10 implies an invertibility test. Line 11 is the regularity test which follows from the following facts.

- Let $I = \langle F \rangle$ and $\mathcal{U}$ be the output of **Triangularize**(F), then

$$\sqrt{I} = \bigcap_{U \in \mathcal{U}} \sqrt{\mathrm{sat}(U)}.$$

- Let T' be primitive regular chain and h be regular modulo $\langle T' \rangle$. Then (T', h) is a regular sequence, consequently $\langle T' \cup \{h\} \rangle$ is an **unmixed ideal** with dimension $n - |T'| - 1$.

- For an unmixed ideal I,

$$\boxed{f \text{ is regular modulo } I \iff f \text{ is regular modulo } \sqrt{I}.}$$

- Finally, $r = \mathrm{tail}(t)$ is regular modulo $\langle T' \cup \{h\} \rangle$

$\iff$ r is regular modulo $\sqrt{\mathrm{sat}(U)}$ for each $U \in \mathcal{U}$

$\iff$ r is regular modulo $\mathrm{sat}(U)$ for each $U \in \mathcal{U}$

$\iff$ the **iterated resultant** $\mathrm{ires}(r, U)$ is not zero.

Experimentation

System	(n, d)	IsPrimitive	Pattern
KdV575	(26, 3)	3.525	[T, T, T, T, T, T, T]
MontesS11	(6, 4)	.001	[T]
MontesS16	(15, 2)	.103	[T, T, T, F, T, T, T]
Wu-Wang2	(13, 3)	0.099	[T, F, T, T, T]
MontesS10	(7, 3)	.145	[F]
Lazard2001	(7, 4)	2.314	[T, T, T, F, T, F]
Lanconelli	(11, 3)	.062	[F, T]
Wang93	(5, 3)	.142	[F]
Leykin-1	(8, 4)	.228	[T, T, T, T, T, T, T, T, F, T, T, T, F, F]
MontesS14	(5, 4)	1.171	[T, F, F]
MontesS15	(12, 2)	.312	[F]
Maclane	(10, 2)	.157	[T, T, F, T, F]
MontesS12	(8, 2)	.042	[F]
Liu-Lorenz	(5, 2)	1.117	[F, T]

In the algorithm the call **Triangularize**$(T' \cup \{h\})$ is **expectedly cheap** since T' is a regular chain and (T', h) is a regular sequence.

Discussion with an example: Montes16

$$F\left\{\begin{array}{l}
w12 + w14, \\
w12 + w13, \\
w12 + w15, \\
w12 + w23 + w25 - w26x + w26, \\
w12 + w25 - w26y + w26, \\
w12 + w23 - w26z + w26, \\
w23 + w34 + xw36, w13 + w34 - w36y + w36, \\
w23 + zw36, w14 + w34 + w45 - w46x + w46, \\
w34 + yw46, \\
w45 + zw56, \\
w15 + w45 - zw56 + w56, \\
-w26 + w26x + xw36 - w46 + w46x + w56x, \\
-w26 + w26y - w36 + w36y + yw46 + w56y, \\
-w26 + w26z + zw36 + w46z - w56 + zw56
\end{array}\right.$$

with $X = [w12, w13, w14, w15, w23, w25, w34, w45, w26, w36, w46, w56, x, y, z]$.

Discussion with an example: Montes16

- The output $\mathcal{T}$ of **Triangularize**

```
[regular_chain,regular_chain,regular_chain,regular_chain,
 regular_chain,regular_chain,regular_chain];
```

- Are they primitive?

```
[true, true, true, false, true, true, true];
```

- Are there any **redundant** regular chains?

- Let $T_i = \mathcal{T}[i]$, for $i = 1, \ldots, 7$. Dimension of regular chains:

$$\dim(T_1) = 3,$$
$$\dim(T_2) = \dim(T_3) = \dim(T_4) = \dim(T_5) = 2,$$
$$\dim(T_6) = \dim(T_7) = 1.$$

- In fact, the following two are the only inclusion relations

$$\underbrace{\mathrm{sat}(T_2) \subseteq \mathrm{sat}(T_6)}_{\text{Can be detected.}} \quad \text{and} \quad \underbrace{\mathrm{sat}(T_4) \subseteq \mathrm{sat}(T_7)}_{\text{Still can not be detected.}} .$$

  Note that a polynomial $\boxed{f \in \mathrm{sat}(T) \iff \mathrm{prem}(f, T) = 0}$.

- An irredundant decomposition for F is

$$\{T_1, T_3, T_5, T_6, T_7\}.$$

- With the notion of primitive regular chain, one can improve the situation for removing redundancy.

- However, a complete Gröbner free algorithm for inclusion test is still **unknown**.

References

(0) J. Arnold and R. Gilmer. On the contents of polynomials. Proc. Amer. Math. Soc., 24:556562, 1970.

(1) A. Corso, W. V. Vasconcelos, and R. H. Villarreal. On the contents of polynomials. J. Pure. Appl. Algebra, 125(1-3):117127, 1998.

(2) P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. J. Symb. Comput., 28(1-2):105124, 1999.

(3) M. Kalkbrener. Algorithmic properties of polynomial rings. J. Symb. Comput., 26(5):525581, 1998.

(4) L. Yang and J. Zhang. Searching dependency between algebraic equations: an algorithm applied to automated reasoning. Technical report IC/91/6, International Atomic Engery Angency, Miramare, Trieste, Italy, 1991.

(5) F. Lemaire, M. Moreno Maza, W. Pan, and Y. Xie. When does $\langle T \rangle$ equal sat(T)? To appear in ISSAC 2008.

Thank you!

Dedekind-Mertens Lemma

Let

$$f = a_0 + a_1 x + \cdots + a_n x^n \text{ and } g = b_0 + \cdots + b_m x^m$$

be polynomials in $R[x]$. Denote by $c(\cdot)$ the ideal generated by the coefficients. Then we have

$$c(f)^{m+1} c(g) = c(f)^m c(fg).$$

As a corollary, for each $h \in R$,

(1) $h \mid fg$ implies $h \mid b_0 a_i^{m+1}$ for $0 \leq i \leq n$,

(2) $h \mid fg$ implies $h \mid b_n a_i^{m+1}$ for $0 \leq i \leq n$.