Lecture 5.

Commutative Algebras.

In the class of commutative algebras the algorithmic problems are decidable.

The role of free algebra is played by the algebra of polynomials $F[x_1, \ldots, x_n]$. More precisely:

Let A be an associative commutative algebra generated by elements $a_1, \ldots, a_n$. The mapping $x_i \xrightarrow{\varphi} a_i$, $1 \le i \le n$, extends to a homomorphism $F[x_1, \ldots, x_n] \xrightarrow{\bar{\varphi}} A$. Let $J = \ker \bar{\varphi}$,

$$A \cong F[x_1, \ldots, x_n] / J.$$

By Hilbert's Theorem the ideal J is

finitely generated, so there exists a finite subset $R \subset J$: $J = R\,F[x_1, \ldots, x_n]$, the ideal generated by R. We write

$$A = F\langle x_1, \ldots, x_n \mid R = 0 \rangle.$$

It should be clear from the context if we mean the commutative algebra or the noncommutative algebra $F\langle x_1, \ldots, x_n\rangle / id(R)$.

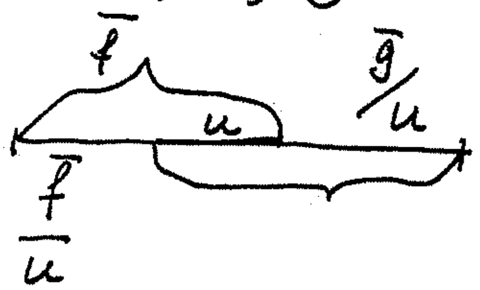
All finitely generated commutative algebras are finitely presented.

Lets introduce the lexicographical order in the set of monomials:

$$x_1 < x_2 < \ldots < x_n.$$

Two (commutative) monomials u, v admit a composition if they are divisible by the same ~~divisible~~ nonidentical monomial.

Choose polynomials $f, g \in F[x_1, \ldots, x_n]$. Suppose that their leading monomials $\bar{f}, \bar{g}$ admit a composition i.e. both are divisible by the same nonidentical monomial u. Let the coefficients at $\bar{f}, \bar{g}$ be $= 1$.



$$, \quad w = \frac{\bar{f}\,\bar{g}}{u}$$

$(f,g)_w = f\,\frac{\bar{g}}{u} - \frac{\bar{f}}{u}\,g$ is the composition of f, g.

If the set of defining relations R is closed with respect to compositions then

$\{$ irreducible words in $a_1, \ldots, a_n\}$ $=$

$\{$ words not divisible by $\bar{f}$, $f \in R\}$ $=$

basis of A.

Let $A = F\langle x_1, \ldots, x_n \mid R = 0 \rangle$, $|R| < \infty$, $R_1 = R$. Then we examine all compositions in R and reduce them. If some do not reduce to 0 then we add them to R_1 and get R_2 and so on,

$$R = R_1 \subseteq R_2 \subseteq \ldots$$

B. Buchberger (with bounds):

this chain stabilizes. In finitely many steps we get a finite system of defining relations that is closed with respect to compositions.

Proof of Buchberger's theorem.

Hilbert Theorem: any set of nonidentical monomials M contains a finite subset $v_1, \dots, v_m \in M$ such that every monomial from M is divisible by one of $v_1, \dots, v_m$. Hence: in every infinite set of monomials there exist distinct ~~ever~~ elements v, w such that v divides w.

Suppose that the chain $R_1 \subseteq R_2 \subseteq \dots$ is infinite. Consider the leading monomials

$\overrightarrow{R_1} \subseteq \overrightarrow{R_2} \subseteq \dots$

Notice that every element $f \in R_{i+1} \setminus R_i$ is irreducible with respect to R_i, hence $\overrightarrow{f}$ is not divisible by any monomial from $\overrightarrow{R_i}$. This is already a contradiction, that completes the proof of the theorem.

<u>Time Complexity.</u>

We will discuss complexity functions for semigroups and groups (later). A proper approach for algebras is not completely clear yet.

Consider a finitely presented semigroup

$$S = \langle x_1, \dots, x_m \mid u_1 = v_1, \dots, u_k = v_k \rangle.$$

Let $\sim$ be the congruence generated by $u_i \times v_i$, $1 \le i \le k$, so $u(x) = v(x)$ in S if and only if $u \sim v$ in X^*.

By Proposition if $u \sim v$ then there exists a sequence of words

$$u = u_1 \to u_2 \to \dots \to u_d = v,$$

each u_{i+1} is obtained from u_i by a substitution $u_i \to v_i$ or $v_i \to u_i$, $1 \le i \le k$) i.e. by a reduction from R.

Of course, there may be more than one such sequence. The length of a shortest such sequence is denoted as $\| u \times v \|$. This is a minimal number of reductions from R needed to reduce u to v.

Define the Dehn function

$$D_X(n) = \max\left(\|u \times v\| \,\middle|\, u \sim v,\ \text{length}(u),\right.$$

$$\left.\text{length}(v) \leq n\right)$$

This function depends on a choice of generators & relations.

Let N denote the set of positive integers, let R_+ denote the set of positive real numbers.

<u>Def.</u> Given two nondecreasing functions $f, g : N \to R_+$ we say that f is <u>asymptotically less or equal to g</u> (denote : $f \preceq g$) if there

exists $C \in N$ such that

$$f(n) \le C\, g(Cn)$$

for all $n \ge 1$.

If $f \preceq g$, $g \preceq f$ then the functions f, g are called <u>asymptotically</u> <u>equivalent</u>.

<u>Lemma I.4.3.</u> Consider two finite presentations of a semigroup S

$$S = \langle \underbrace{x_1, \ldots, x_m}_{X} \mid \underbrace{u_1 = v_1, \ldots, u_p = v_p}_{R} \rangle =$$

$$\langle \underbrace{y_1, \ldots, y_k}_{Y} \mid \underbrace{u_1' = v_1', \ldots, u_q' = v_q'}_{R'} \rangle$$

Then $D_X(n) \sim D_Y(n)$.

Proof. Consider an isomorphism

$$\langle X \mid R\rangle \xrightarrow{\varphi} \langle Y \mid R'\rangle$$

Suppose that all elements $\varphi^{-1}(y_j)$, $1 \le j \le q$, can be written as words in X of length $\le C$.

For any defining relation $u_i(x) = v_i(x)$ the relation $u_i(\varphi(x_1), \ldots, \varphi(x_m)) = v_i(\varphi(x_1), \ldots$ $\ldots, \varphi(x_m))$ follows from R'. Suppose that to get from $u_i(\varphi(x))$ to $v_i(\varphi(x))$ one, $1 \le i \le p$, one needs $\le C$ reductions from R'.

Let a, b be words in Y of length $\le n$, $a(Y) = b(Y)$ in S. Then

$$\varphi^{-1}(a(Y)) = a(\varphi^{-1}(Y)) = b(\varphi^{-1}(Y)) = \varphi^{-1}(b(Y)),$$

and both $a(\varphi^{-1}(Y))$, $b(\varphi^{-1}(Y))$ have length

$\leq Cn$ in X.

Let $a(\varphi^{-1}(Y)) = a_1 \to a_2 \to \cdots \to a_d = b(\varphi^{-1}(Y))$ be a chain of reductions in $\langle X \mid R \rangle$, $d \leq D_X(Cn)$. Applying φ we get

$$a(Y) = \varphi(a_1) \sim \varphi(a_2) \sim \cdots \sim \varphi(a_d) = b(Y)$$

For each $1 \leq j \leq d-1$ the word $\varphi(a_j)$ in Y can be reduced to $\varphi(a_{j+1})$ in $\leq C$ reductions from R'. Hence $u(Y)$ can be reduced to $v(Y)$ in $\leq C D_X(Cn)$ reductions from R';

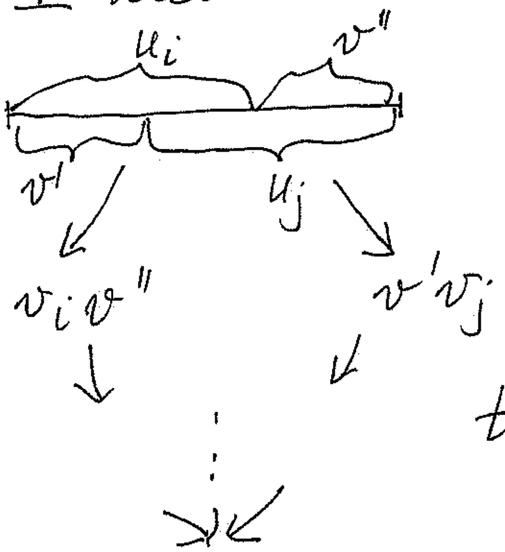
$$D_Y(n) \leq C D_X(Cn), \quad D_Y \preceq D_X$$

Similarly $D_X \preceq D_Y$ and therefore

$D_X \sim D_Y$, which completes the proof of the lemma.

Let $S = \langle X \mid u_1 = v_1, \dots, u_k = v_k \rangle$ be a finitely presented semigroup. Suppose that the set $R = \{u_1 = v_1, \dots, u_k = v_k\}$ of defining relations is closed with respect to compositions (we assume that $X = \{x_1 \dots x_m\}$, $x_1 < x_2 < \dots < x_m$, $u_i > v_i$ lexicographically, $1 \le i \le k$).

I means that for any composition



$v_i v''$ and $v' v_j$ have a common descendant. Then every word reduces to a unique normal form, no matter which reductions we applied (this is known as <u>Newman Lemma</u>). Such reduction system $u_i \to v_i$, $1 \le i \le k$, is called **confluent**.

The final result (normal form) does not depend on which reductions we used, but the # of reductions (time complexity) may depend on this choice.

Let $\|v\|_{min}$, $\|v\|_{max}$ be the minimal and the maximal number of reductions that are needed to reduce v to a normal form.

$$\gamma_{min}(n) = \max(\|v\|_{min} \mid \text{length}(v) \le n),$$

$$\gamma_{max}(n) = \max(\|v\|_{max} \mid \text{length}(v) \le n)$$

These functions are not necessarily asymptotically equivalent.

Example. $\langle x, y \mid yx = xy,\ xy = x^2, yx = x^2 \rangle$

$$\gamma_{min}(n) \sim n$$
$$\gamma_{max}(n) \sim n^2$$

We call a reduction system **uniformly confluent** if $\gamma_{min}(n) \sim \gamma_{max}(n)$.

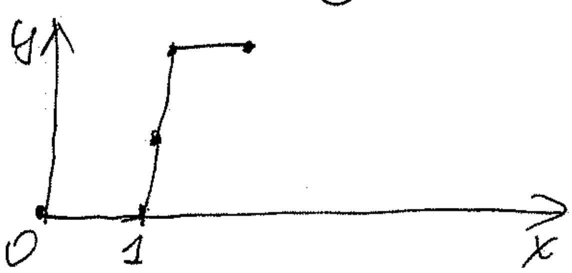
Clearly, $D_X(n) \leq 2\,\gamma_{min}(n)$.

I don't know an example where $D_X(n)$ is strictly asymptotically less than $\gamma_{min}(n)$, though probably it exists.

<u>Example.</u> Let us find the Dehn function of the semigroup $\langle x, y \mid yx = xy \rangle$.
Let $x < y$. Irreducible words: $x^i y^j$

For a word w draw a horisontal segment — for x and the vertical segment | ~~by~~ for y, starting with 0.

For $w = xy^2x$ we draw



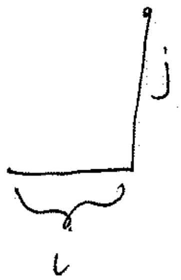
Let Area(w) be the area between this curve and the x-axis, Area$(w) = 2$.

Replacing yx with xy we replace  by , so the area looses one square.

If $w \to w'$ is a reduction (a subword ~~then~~ yx is replaced by xy) then

$$\text{Area}(w') = \text{Area}(w) - 1.$$

$$\text{Area}(x^i y^j) = 0.$$

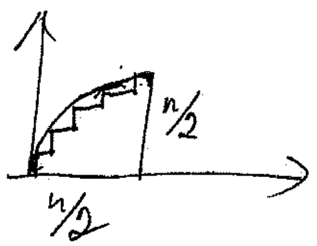


This implies that $\|w\|_{min} =$

$$\|w\|_{max} = \text{Area}(w).$$

$D(n) =$ the maximal area under a curve of length $\leq n \Rightarrow$ ISOPERIMETRIC PROBLEM. The curve should be close to the circle

$$\text{Area} \approx \frac{1}{4}\pi\left(\frac{n}{2}\right)^2 \sim n^2$$



Let us extend this method.

Let $S = \langle X \mid u_i = v_i,\ 1 \le i \le k \rangle$, $|X| < \infty$,

$v_i < u_i$, $R = \{u_i = v_i,\ 1 \le i \le k\}$ is closed with respect to compositions.

Suppose that we found a function

$$\mathrm{Area} : X^* \to R_{\geq 0}$$

with the following properties:

(1) there exist $0 < \varepsilon_1 \le \varepsilon_2$ such that

$$\varepsilon_1 \le \mathrm{Area}(v' u_i v'') - \mathrm{Area}(v' v_i v'') \le \varepsilon_2$$

for any words v', v'';

(2) for any word v in the normal form

$$\mathrm{Area}(v) = 0.$$

Let v_{norm} be the normal form of the word v.

If we apply d reductions to reduce v to v_{norm} then

$$\mathrm{Area}(v) - d\,\varepsilon_2 \le \underset{\substack{\| \\ 0}}{\mathrm{Area}(v_{norm})} \le \mathrm{Area}(v) - d\,\varepsilon_1$$

$$\frac{\mathrm{Area}(v)}{\varepsilon_2} \le d \le \frac{\mathrm{Area}(v)}{\varepsilon_1}$$

this implies that

$$\gamma_{min}(n) \sim \gamma_{max}(n) \sim \max\{\mathrm{Area}(v) \mid \mathrm{length}(v) \le n\}.$$

Let $S = \langle x_1, \dots, x_m \mid x_i \cdot x_j = x_j \cdot x_i;\ 1 \le j < i \le m \rangle$

Let $x_1 < x_2 < \dots < x_m$. For a word $v = x_{i_1} \cdots x_{i_n}$ let

$\mathrm{Area}(v) = \#$ of pairs $1 \le \nu < \mu \le n$ such that ~~$i_\mu > i$~~ $i_\nu > i_\mu$.

It is easy to see that for $i > j$ and any words v', v''

$$\mathrm{Area}\,(v' x_i \cdot x_j\, v'') = \mathrm{Area}\,(v' x_j \cdot x_i \cdot v'') + 1,$$

the conditions for the area function are satisfied,

$$D_X(n) \sim \max\{\mathrm{Area}\,(v) \mid \mathrm{length}(v) \le n\}$$

$$\mathrm{Area}\,(x_{i_1} \cdots x_{i_n}) \le \binom{n}{2} = \frac{n(n-1)}{2}$$

On the other hand

$$\mathrm{Area}\,(x_m^{n/2} \cdot x_1^{n/2}) = \left(\frac{n}{2}\right)^2.$$

This implies $D_X(n) \sim n^2$.