THIS IS `rag_class.pdf`
This document was created by Sal Barone during the class
of Saugata Basu in Spring '10.

1 January 12, Day 1

This is Real Algebraic Geometry with Prof. Saugata Basu. The references for the course are:

1. Real Algebraic Geometry, Bochnak, Coste, Roy, [2]
2. Positive polynomials and sums of squares, Marshall, [3]
3. Algorithms in Real Algebraic Geometry, Basu, Pollack, Roy. [1]

Why study RAG? A polynomial with complex coefficients $F \in \mathbb{C}[X]$ with degree $\deg F = d$ will always have exactly d roots in $\mathbb{C}$. Of course, a polynomial in one variable over $\mathbb{R}$, $F \in \mathbb{R}[X]$ might have no real roots. So we would like some kind of statement which tells you something about the number of *real roots*. Similarly, over the complex numbers a polynomial in n variables will have a zero set which is a complex hypersurface of dimension $n-1$. This is not true over $\mathbb{R}$. Originally, algebraic geometry started with the complex numbers because of this added simplicity over the algebraically closed field $\mathbb{C}$. However, we are most often concerned with the *real solutions*.

Here is an elementary theorem, the *Descartes rule of sign*, which says that a real polynomial $F = a_{\alpha_1}X^{\alpha_1} + a_{\alpha_2}X^{\alpha_2} + \cdots + a_{\alpha_m}X^{\alpha_m}$, $0 \leq \alpha_1 < \alpha_2 < \cdots < \alpha_m$, $\alpha_i \in \mathbb{R}$. Then the number of real positive roots is at most the number of sign changes of the coefficients, or the *variance* of the polynomial. A corollary to this theorem is that there are at most $2m-1$ real roots of a polynomial with m terms, independent of the degree of the polynomial!

It is an open problem to formulate and prove Descartes rule of sign in two polynomials in two variables. The following is known for two polynomials in X, Y with m monomials in the system. If we look for the isolated common zeros of the two polynomials, then there is an exponential bound (like 2^{m^2}) for the number of isolated common zeros which is most likely not tight; the bound grows very fast with large number of monomials. A polynomial bound (say of the form m^2) would be a big improvement.

The point here is that real algebraic geometry (RAG) has problems which have no counterpart in the study of complex algebraic geometry.

There are two main motivations which we will look at.

1. Hilbert's 16^{th} and 17^{th} problems.
2. Model theory, Tarski.

It turns out that Hilbert's 16^{th} problem has more to do with differential equations and things, and not so much RAG. We will first look instead at Hilbert's 17^{th} problem.

1.1 Hilbert's 17^{th} Problem

Let $F \in \mathbb{R}[X_1, \ldots, X_n]$ such that $F(X_1, \ldots, X_n) \geq 0$ for all $(X_1, \ldots, X_n) \in \mathbb{R}^n$. Is it true that F is a sum of squares (SOS)?

Example 1. In the case where $n = 1$. If $F(X) \geq 0$ for all $X \in \mathbb{R}$, then $F = h^2 + g^2$ for some $h, g \in \mathbb{R}[X]$.

Proof. We can decompose F into linear and quadratic factors. Write

$$\begin{aligned} F &= a\prod_{i\in I}(x-a_i)^{k_i} \cdot \prod_{j\in J}(x-(c_j+d_ji))(x-(c_j+d_ji)) \\ &= a\prod_{i\in I}(x-a_i)^{k_i}\prod_{j\in J}((x-c_j)^2+d_j^2)^{\ell_j} \end{aligned}$$

1. If $F \geq 0$, then $a \geq 0$ and all k_i's are even.

2. We use that for complex numbers $z_1, z_2 \in \mathbb{C}$ we have $|z_1 z_2|^2 = |z_1|^2 \cdot |z_2|^2$. So $|(a+bi)(c+di)|^2 = |a+bi|^2|c+di|^2 = (a^2+b^2)(c^2+d^2)$. But the LHS is $(ac-bd)^2 + (ad+bc)^2$. This finishes the fact that f is a sum of squares since $(ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2)$ we can write the product of the sum of two squares as the sum of squares.

So, in the case $n = 1$ the answer to the problem is YES for any d.

Example 2. In the case $d = 2$, then it is true for any n. Finally, the case $n = 2$ and $d = 4$ the answer is also YES. However, there is a counterexample (called the Motzkin polynomial) for the case $n = 2$ and $d = 6$; once you have a counterexample you can extend it to higher degree and more variables. So Hilbert knew that the answer to this question was NO in general.

Theorem 1 (Hilbert's 17^{th} problem)**.** *If F is a non-negative polynomial in n variables of degree d, then $F = \frac{\sum g_i^2}{h^2}$ for some polynomials g_i, h. That is, every non-negative polynomial is a sum of squares of* RATIONAL *functions.*

1.2 Tarski-Seidenberg principle

From high school math, we know that $(\exists x)(x^2 + 2bx + c) = 0$ is equivalent to the discriminant $b^2 - c \geq 0$. The first formula is QUANTIFIED, since it has an existential quantifier, while the second is QUANTIFIER FREE. It turns out that for any real closed field (like $\mathbb{R}$), there is an algorithm for getting rid of quantifiers. As a corollary to this fact, if there is a quantified formula which has coefficients in a real closed field R, then if it is true in some real closed extension $R' \supset R$, then it is also true in R.

1.3 Preliminary definitions, Real algebra

Definition 1.1 (Ordered field)**.** An ordered field $(F, \leq)$ is a field with a total order which satisfies

1. $x \geq y$ then $x + z \geq y + z$

2. $x \geq 0,\ y \geq 0$ implies $xy \geq 0$.

We will call elements x of F which are $x > 0$ to be *positive*.

Example 3. The fields $\mathbb{Q}$, $\mathbb{R}$ are ordered fields.

Example 4. The field $F = \mathbb{R}(x)$ of rational functions has many possible orderings that make it into an ordered field.

Proposition 2. *There is a unique order on F in which $x > 0$ but smaller than all positive elements of $\mathbb{R}$.*

This makes F into a non-archimedean field, since the element $\frac{1}{x}$ would be a bigger element than any element of $\mathbb{R}$.

Proof of prop. We just say what the positive elements are, and it is left to the reader to check that the two properties of ordered field are satisfied. Say $p(x) = a_n x^n + \cdots + a_\ell x^\ell > 0$ if and only if $a_\ell > 0$ (here $n > \ell \geq 0$. Say $\frac{p(x)}{q(x)} > 0$ if and only if $p(x)q(x) \geq 0$. It is also left to the reader that this is the only way to define the positive elements so that x is infinitesimal.

□

Corresponding to the ordered field $(\mathbb{R}(X), \leq)$ there is a dedekind cut (I, J), $I = \{x \in \mathbb{R} |\ x < X\}$ and $J = \{x \in \mathbb{R} |\ x > X\}$. We define

- $(\emptyset, \mathbb{R}) = -\infty$,
- $((-\infty, a), [a, \infty)) = a_-$,
- $((-\infty, a], (a, \infty)) = a_+$,
- $(\mathbb{R}, \emptyset) = \infty$.

If we set $Y = X - a$ then $R(X) = R(Y)$ and by uniqueness of the order which makes X infinitesimal we see that the *cuts* and the *orderings* are in one-to-one correspondence.

It is interesting that we get back the real closed elements by taking the different orderings.

Definition 1.2. Let F be a field. A subset $P \subset F$ is called a *cone* (or *preorder*) if it satisfies

(i) $x, y \in P \implies x + y \in P$,

(ii) $x, y \in P \implies xy \in P$,

(iii) $\forall x \in F,\ x^2 \in P$,

and the cone is called proper if in addition

(iv) $-1 \notin P$.

Example 5. The set $\sum F^2 = \{x_1^2 + \dots x_n^2 |\ x_1, \dots, x_n \in F\}$ is a cone contained in every other cone.

Proposition 3. *Let $(F, \leq)$ be an ordered field. Then its positive elements P form a proper cone satisfying*

(v) *$P \cup -P = F$.*

Conversely, any proper cone satisfying (v) is the cone of positive elements of an ordering F.

Remark 4. Not all fields have an ordering. In particular, $\mathbb{C}$ can not be ordered. We make this precise in the following theorem.

Theorem 5. *The following are equivalent for a field F.*

1. *F can be ordered.*

2. *F has a proper cone.*

3. *$-1 \notin \sum F^2$.*

4. *If $x_1^2 + \dots + x_n^2 = 0$ then $x_1 = \dots = x_n = 0$.*

Any field satisfying one of these equivalent definitions is called a *real field*. Before we prove this theorem we should prove a small lemma from which the proof will follow. Unfortunately, the proof of the following lemma requires Zorn's lemma, and this is where some of the NONCONSTRUCTIVE problems with Artin's proof arise.

Lemma 1. *Suppose F is a field and P is a proper cone and $-a \notin P$. Then*

(i) *$P[a] = \{x + ya |\ x, y \in P\}$ is a proper cone containing a,*

(ii) *P is contained in the positive cone of a total order on F.*

Proof. For part (i), the only non-trivial part is showing that $-1 \notin P[a]$. Suppose, seeking contradiction, that $-1 \in P[a]$. Then $-1 = x + ay$ for some $x, y \in P$. We have two cases to consider. If $y = 0$ then $-1 \in P$ is a contradiction with the fact that P was a proper cone. If $y \neq 0$, then $-a = \frac{1}{y}(1 + x) \in P$ since $(\frac{1}{y})^2 y(1 + x) \in P$.

For part (ii), there is a maximal proper Q cone containing P by Zorn's Lemma. We expect this maximal cone to be the positive cone of a total order on F. Since Q is a proper cone, we only need to show that $Q \cup -Q = F$. Suppose $a \notin Q$. By (i), we have that $Q[-a]$ is a proper cone which contains Q as well as $-a$, which by maximality of Q implies that $Q[-a] = Q$. So if $a \notin Q$ then $-a \in Q$, which means that $Q \cup -Q = F$. So Q is a positive cone of a total order by Proposition 3. □

2 January 14, day 2

Last time, we were characterizing real fields.

Theorem 5. *The following are equivalent for a field F.*

1. *F can be ordered.*
2. *F has a proper cone.*
3. *$-1 \notin \sum F^2$.*
4. *If $x_1^2 + \cdots + x_n^2 = 0$ then $x_1 = \cdots = x_n = 0$.*

Proof. (1) $\implies$ (2) $\implies$ (3) ✓ are easy. For (3) $\implies$ (4) suppose that $x_1^2 + x_2^2 + \cdots + x_n^2 = 0$ and $n \geq 2$ or else $x_1^2 = 0$ means $x_1 = 0$. We may assume that $x_i \neq 0$ for $i = 1, \ldots, n$. So dividing by x_1^2 we have $-1 = \frac{x_2^2 + \cdots + x_n^2}{x_1^2}$ is a sum of squares ✓. For finishing the proof, we use that (4) $\implies$ (3) $\implies$ (2) is easy and (2) $\implies$ (1) is from yesterday's Lemma.

□

Any field R which satisfies one of the equivalent properties of the Theorem 5 is called a *real field*.

Definition 2.1. A field R is a *real closed* field if R is real and R does not have any proper real algebraic extension.

The definition of a real closed field has many equivalent definitions.

Theorem 6. *The following are equivalent for a field R.*

1. *R is a real closed field.*
2. *R is an ordered field with a unique ordering whose positive elements are the sums of squares, and every polynomial of odd degree has a root in R.*
3. *The ring $R[i] = \frac{R[x]}{(x^2+1)}$ is algebraically closed.*

Proof. We first show (1) $\implies$ (2). Suppose, seeking a contradiction, that $a \in R$ is such that $a > 0$ but a is not a square in R. If a is not a square in R, we can look at the algebraic extension $R[\sqrt{a}]$ which is a field and a proper algebraic extension of R. Since it is a proper algebraic extension, then it must NOT be a real field by (1). So $-1 = \sum_i (x_i + y_i\sqrt{a})^2$ for some $x_i, y_i \in R$. So $-1 = \sum_i (x_i^2 + y_i^2 a) + \sqrt{a} \sum_i 2x_i y_i = \sum_i x_i^2 + a \sum_i y_i^2$, but this is impossible since the RHS is positive since a is positive, but this is a contradiction with the fact that -1 is negative in R.

This finishes the first part of (1) $\implies$ (2) since any proper cone contains $\sum F^2$ but we just showed the other containment, that is, $\sum F^2$ is the ONLY proper cone of R, and this means there can only be one ordering. We still need to show that all polynomials of odd degree have roots in R to finish (1) $\implies$ (2).

We induct on the degree d of the polynomial. Clearly, a polynomial of degree $d = 1$ has a root in R. Suppose every odd degree polynomial of degree less than d has a root in R for some odd d. Let f be a polynomial of degree d and we want to show that f has a root. If f is NOT irreducible then we're done by the induction hypothesis. So we can assume f is irreducible and look at $F = \frac{R[x]}{(f)}$, which is a proper algebraic extension of R and hence not real by (1). So $-1 \in \sum F^2$. So there exists polynomials $h_1, \ldots, h_m \in R[x]$ of degree strictly smaller than d and

$$-1 = \sum_i h_i^2 + f \cdot g \qquad (*)$$

for some $g \in R[x]$. Now the highest power of x occurring among all the h_i's can not cancel since the leading coefficients of h_i^2 are squares of R. So $\sum_i h_i^2$ is a polynomial of EVEN degree $\deg(\sum_i h_i^2) \leq 2(d-1)$. Looking now at $f \cdot g$, we see that $\deg(g)$ is odd and $\deg(g) \leq d-2$. Now, by induction hypothesis, there exists $\alpha \in R$ such that $g(\alpha) = 0$. Substitution of $x = \alpha$ in Equation $(*)$ we get a contradiction $-1 = \sum_i (h_i(\alpha))^2$. So f could not have been irreducible.

We next prove (2) $\implies$ (3). First, $R[i] = \frac{R[x]}{x^2+1}$ is a field since $x^2 + 1$ is irreducible in R since -1 is not a square in R. To show that $R[i]$ is algebraically closed, we first show that every polynomial with coefficients in R has a root in $R[i]$, and from there it is easy to finish the desired implication.

Let $f \in R[x]$, $\deg(f) \geq 1$, and we want to show that f has a root in $R[i]$. The proof is by induction on the biggest power of 2 dividing the degree of f. Let $d = \deg(f) = 2^m \cdot n$ where n is odd, and we induct on m. If m is zero, then $d = n$ is odd, so by hypothesis the polynomial f has a root in $R \subseteq R[i]$. For the induction step, assume the implication holds for polynomials of degree having at most a power of 2 less than m dividing the degree of the polynomial.

Let K be an algebraic closure of R and $y_1, \ldots, y_d \in K$ be roots of f. For an integer $h \in \mathbb{Z}$, consider the polynomial $g_h = \prod_{1 \leq i < j \leq d}(x - y_i - y_j - h y_i y_j)$, which *a priori* has coefficients in K, but since it is symmetric it actually has coefficients in R (any permutation of the roots does not change the coefficients of the polynomial). The polynomial g_h has degree $\deg(g_h) = \binom{d}{2} = \frac{1}{2} \cdot d(d-1) = \frac{1}{2} \cdot 2^m \cdot n \cdot (2^m n - 1) = 2^{m-1} \cdot (odd)$, so by induction g_h has a root in $R[i]$. This means that there is a pair $i < j$ such that $y_i + y_j + h y_i y_j \in R[i]$. Since there are infinitely many h's and only finitely many terms in the product defining g_h, at least one pair needs to satisfy $y_i + y_j + h y_i y_j, y_i + y_j + h' y_i y_j \in R[i]$ for $h \neq h'$. This means $y_i + y_j, y_i y_j \in R[i]$, and note that y_i, y_j are the roots of the quadratic equation $x^2 - (y_i + y_j)x + y_i y_j = 0$. We finish the implication by the next claim.

Claim Every quadratic polynomial in $R[i][x]$ has both roots in $R[i]$.

Write $x^2 + 2bx + c = 0$ with $b, c \in R[i]$, and then rewrite as $(x + b)^2 - (b^2 - c) = 0$ and now we just need to see that a square root of an element in $R[i]$ is an element of $R[i]$. Note that $a + bi \in R[i]$ has a square root since if we write $(a + bi) = (c + di)^2 = (c^2 - d^2) + 2cdi$ and solve for c, d where

$$\begin{aligned} c^2 - d^2 &= a \\ 2cd &= b \end{aligned}$$

So $d = \frac{b}{2c}$ and $c^2 - \frac{b^2}{4c^2} = a$. The second equation yields $4c^2 - 4ac^2 - b^2 = 0$ which rewrites to $(2c^2 - a)^2 = a^2 + b^2 > 0$ in R, so the LHS has a square-root. We solve for c to get $c = \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}$ and $d = \frac{b}{2c}$ (in the calculation we need to use $|a| < \sqrt{a^2 + b^2}$).

We're ready to finish the implication. Given $f \in R[i][x]$, say $f = a_0 + a_1 x + \cdots + a_n x^n$ and let $g = f \cdot \bar{f}$ where $\bar{f} = \bar{a_0} + \bar{a_1} x + \cdots + \bar{a_n} x^n$. Hence $g \in R[x]$ and hence g has a root (say α) in $R[i]$. So $g(\alpha) = f(\alpha) \cdot \bar{f}(\alpha) = 0$. So either $f(\alpha) = 0$ or $\bar{f}(\alpha) = 0$, and in the first case we're done, f has α as a root, and in the second case f has $\bar{\alpha}$ as a root.

For the last implication (3) $\implies$ (1), we have $R[i]$ is algebraically closed field and we want to see that this implies that R is a real field that has no proper real algebraic extension. Since $R[i] = \frac{R[x]}{x^2+1}$ is a field, -1 is not a square in R (since x^2+1 is irreducible in R iff $R[i]$ is a field).

Claim Every sum of two squares a^2+b^2 is already a square of R

Since $R[i]$ is algebraically closed, $(a+bi) = (c+di)^2$ for some $c, d \in R$. Then note that $(a-bi) = (c-di)^2$ and multiplying together these two equations we get $a^2+b^2 = (c^2+d^2)^2$.

□

Note that the implication (2) $\implies$ (3) is an algebraic proof of the Fundamental Theorem of Algebra.

Definition 2.2. Let $(F, \leq)$ be an ordered field. A real closure of F is an algebraic extension of F that is real closed and whose unique order extends the order of F.

Example 6. We give several examples of real closed fields. The field $\mathbb{R}$ is the prototypical example of a real closed field. Every odd degree polynomial has a root in $\mathbb{R}$. The real closure of $\mathbb{Q}$ is $\mathbb{R}_{alg}$ which are all the elements of $\mathbb{R}$ which are zeros of polynomials with integer coefficients. We denote $\mathbb{R}_{alg}[i] = \overline{\mathbb{Q}}$. The field $\mathbb{R}(x) \subseteq \mathbb{R}\langle\langle x\rangle\rangle = \{\sum_{i \geq i_0} a_i x^{\frac{i}{q}} \mid q \in \mathbb{Z}_{>0}\} = \cup_{q>0}\mathbb{R}[[x^{\frac{1}{q}}]]$, called the field of Puiseux series, is real closed. The Newton Puiseux Theorem says that if C is algebraically closed then $C\langle\langle x\rangle\rangle$ is also algebraically closed. For us, this says that $R\langle\langle x\rangle\rangle[i] = R[i]\langle\langle x\rangle\rangle$ is algebraically closed, so $R\langle\langle x\rangle\rangle$ is real closed. WARNING: the real closure of $R(x)$ is denoted $R\langle x\rangle$ which is a proper subfield of $R\langle\langle x\rangle\rangle$.

3 Jan 19, Day 3

Last time we proved the theorem which gives equivalent formulations of what it means for R to be real closed.

Theorem 6. *The following are equivalent.*

1. *R is a real closed field (by definition, no proper algebraic extension of R is real).*
2. *R is a real field with a unique ordering in which the positive cone consists of squares and every polynomial of odd degree has a root in R.*
3. *$R[i] = \frac{R[x]}{(x^2+1)}$ is an algebraically closed field.*

The examples that come to mind are $\mathbb{R}$, $\mathbb{R}_{alg}$, and $R\langle\langle x\rangle\rangle = \{\sum_{i \geq i_0} a_i x^{\frac{i}{q}} \mid a_i \in R\}$. The last is an example of a non-archimedian real closed field since $\frac{1}{x} > n$ for every $n \in \mathbb{N}$. The field of real numbers have a metric completeness property, but $\mathbb{R}_{alg}$ is completely disconnected.

We can do some calculus on real closed fields since we have the intermediate value property.

Proposition 7. *Let R be a real closed field and $P \in R[x]$ and $a < b \in R$. Suppose that $P(a)P(b) < 0$, then there exists c with $a < c < b$ such that $P(c) = 0$.*

Proof. Since $R[i]$ is algebraically closed, the roots of P occur in conjugate pairs. That is, $P(x)$ factors into linear and quadratic factors. The quadratic factors are of the form $(x-(c+di))(x-(c-di)) = ((x-c)^2+d^2)$, which is a sum of squares, hence no quadratic factor can change signs (they are either non-negative or non-positive). If $P(x)$ changes sign then there is a linear factor which is changing sign over (a, b), hence the linear factor has a zero $c \in (a, b)$.

□

Theorem 8 (Rolle's Theorem)**.** *Let $P \in R[x]$, $a < b$, and suppose $P(a) = P(b) = 0$. Then there exists a c, $a < c < b$ such that $P'(c) = 0$.*

Proof. We may as well assume that $P(c) \neq 0$ for all $c \in (a,b)$; that is, assume that a, b are consecutive roots of P and hence P maintains sign over the interval $[a,b]$.

Write $P(x) = (x-a)^m(x-b)^n P_1$ where $P_1(a) \neq 0$ and $P_1(b) \neq 0$. Then $P'(x) = (x-a)^{m-1}(x-b)^{n-1}P_2$ where $P_2 = m(x-b)P_1 + n(x-a)P_1 + (x-a)(x-b)P_1'$. Considering P_2, substitution of $x = a$ yields $P_2(a) = m(a-b)P_1(a) \neq 0$, and substitution of $x = b$ yields $P_2(b) = m(b-a)P_1(b)$. Using the first remark of the proof, we have $P_2(a)P_2(b) < 0$, and using Proposition 7, the intermediate value property gives us $\exists c$, $a < c < b$ such that $P_2(c) = 0$, and hence $P'(c) = 0$.

□

Recall the definition from the last section.

Definition 2.2. If $(F, \leq)$ ordered field, then a real closure of F is a real closed algebraic extension whose order extends the order of F.

Theorem 9. *Let $(F, \leq)$ be an ordered field. Then there exists a real closure R of F. Moreover, if R' is another real closure of F, then there exists a unique F-isomorphism $\varphi : R \to R'$.*

We remark that the isomorphism is an isomorphism of *ordered fields*. In the category of ordered fields, this is how a homomorphism should perform.

Proof of Theorem 9. Fix an algebraic closure $\overline{F} \supset F$. Consider the family of ordered sub-extensions $(F, \leq) \subset (K, \leq)$ where $F \subset K \subset \overline{F}$. By Zorn's lemma , there exists a maximal ordered sub-extension $(F, \leq) \subset (R, \leq)$.

Claim R is real closed.

There are several steps.

(1) First we prove that the positive elements of R are precisely the squares: If $a \in R$ and $a > 0$ then a is a square. Suppose not, and consider $R_1 = R[\sqrt{a}]$. Consider the cone

$$P = \{\sum_i a_i(b_i + c_i\sqrt{a})^2 |\ a_i > 0, b_i, c_i \in R\}.$$

Clearly, the set P is a cone; it is closed under sums and products. Furthermore, P is a proper cone since if $-1 \in P$ then $-1 = \sum_i a_i(b_i + c_i\sqrt{a})^2$ implies $-1 = \sum_i a_i(b_i^2 + c_i^2 a)$ is positive in R, which is a contradiction. So, if a is not a square of R then R_1 can be ordered extending the order of R, which contradicts the maximality of R. So a must be a square of R.

(2) Now, since every positive element of R is a square, this means that there is only one possible ordering of R: the positive cone of which is $\sum R^2$. Now, R can not have a proper algebraic ordered extension. If it did have such an extension, then this extension must extend the *unique* order of R, which extends the order of F. Hence, this algebraic ordered extension would be an algebraic ordered extension of $(F, \leq)$, contradicting the maximality of $(R, \leq)$.

Since R can not have a proper algebraic ordered extension, by definition R is real closed.

We must wait to prove the uniqueness of R to a later date.

□

3.1 Tarski-Seidenberg transfer theorem

In order to complete Artin's proof of Hilbert's 17^{th} problem, we need the existence of real closed extensions (which we have seen is non-constructive, it uses Zorn's Lemma), and the Tarski-Seidenberg transfer theorem which we next introduce.

Suppose D is an integral domain contained in an ordered field K (*e.g.*, $D = \mathbb{Z}$, $K = \mathbb{Q}$). In the language of ordered domains, a quantifier free formula with coefficients in D is defined as follows.

1. If $P \in D[x_1, \ldots, x_k]$, then $P = 0,\ P < 0, P > 0$ are formulas with free variables $x_1, \ldots, x_k$.

2. If $\phi,\ \psi$ are formulas, then $\phi \wedge \psi$, $\phi \vee \psi$ are formulas whose free variables are any free variables of ϕ or ψ, and $\neg\phi$ is also a formula with the same free variables as ϕ.

In general, a formula with coefficients in D may be *quantified*, and is defined as follows.

1. ϕ is a quantifier free formula.

2. $\exists \bar{y}\phi(\bar{x}, \bar{y})$ or $\forall \bar{y}\phi(\bar{x}, \bar{y})$ when ϕ is a formula with free variables $\bar{x}, \bar{y}$ and the free variables of $\exists \bar{y}\phi(\bar{x}, \bar{y}),\ \forall \phi(\bar{x}, \bar{y})$ is $\bar{x}$.

Definition 3.1. Let $\phi(x_1, \ldots, x_k)$ be a formula with free variables $x_1, \ldots, x_k$ and let $(F, \leq)$ be an ordered extension of the ordered field $(K, \leq)$ containing D. Let $\mathcal{R}(\phi, F^k) = \{(a_1, \ldots, a_k) \in F^k |\ \phi(a_1, \ldots, a_k)\}$.

Theorem 10. *[Tarski-Seidenberg] Let $\phi(x_1, \ldots, x_k)$ be a formula with coefficients in D contained in an ordered field K. Then there exists a quantifier free formula $\psi(x_1, \ldots, x_k)$, such that for any real closed ordered extension R of K, we have $\mathcal{R}(\phi, R^k) = \mathcal{R}(\psi, R^k)$.*

Remark 11. If ϕ has no free variables, then ψ is a sentence which is either true or false, and the realization is either a point of R^k or possibly the empty set (if the sentence is false, like $0 = 1$).

Example 7. Let $D = \mathbb{Z}$ and $K = (\mathbb{Q}, \leq)$ under the usual ordering, and

$$\phi :\ (\exists x)(x^2 + 2bx + c = 0).$$

Then $\psi(b, c)$ is the quantifier free formula

$$\psi :\ (b^2 - c > 0) \wedge (b^2 - c = 0).$$

Then ψ satisfies the property: For any real closed extension of $\mathbb{Q}$ (say $\mathbb{R}, \mathbb{R}_{alg}$, etc.) whenever ϕ is true for particular b, c, then ψ is true as well.

Example 8. We can consider a similar formula for a quartic polynomial. If

$$\phi :\ (\exists x)(x^4 + ax^2 + bx + c = 0),$$

then what is the formula ψ which is equivalent to ϕ but is quantifier free? This is harder to write down, and the next goal will be to develop a method for finding the quantifier free ψ which is equivalent to ϕ.

Definition 3.2 (Semi-algebraic set)**.** A *semi-algebraic set* is a set which is the realization of a quantifier free formula in R.

The geometric formulation of the Tarksi-Seidenberg theorem is seen as follows. If $\phi(x_1, \ldots, x_k, y_1, \ldots, y_\ell)$ is a formula with coefficients in R, then $\mathcal{R}(\phi, R^k \times R^\ell)$ is a semi-algebraic subset of $R^k \times R^\ell$. In particular,

$$\phi_1 : (\exists y_1) \ldots (\exists y_\ell)\phi(x_1, \ldots, x_k)$$

is equivalent to a quantifier free $\psi(x_1, \ldots, x_k)$. Notice that $\mathcal{R}(\psi, R^k)$ is a semi-algebraic subset of R^k. What is the relationship between $\mathcal{R}(\phi, R^k \times R^\ell)$ and $\mathcal{R}(\psi, R^k)$? If we denote $\pi_y : R^k \times R^\ell \to R^k$ the projection along the y-coordinates, then we see that $\mathcal{R}(\psi, R^k) = \pi_y(\mathcal{R}(\phi, R^k \times R^\ell))$. So, a geometric formulation of the Tarski-Seidenberg theorem is that the projection of a semi-algebraic set is again semi-algebraic. This also gives the first idea of the correspondence between projections and quantifier elimination.

4 Jan 21, Day 4

Our next goal will be to prove the Tarki-Siedenberg transfer principle, Theorem 17. We need the notion of Sturm sequences.

4.1 Sturm sequences

Suppose $P, Q \in R[x]$, with R a real closed field. We define

$$P_0 = PP_1 = Q$$
$$P_{i+1} = -Rem(P_{i-1}, P_i) \text{ for } i \geq 1.$$

The notation $Rem(P, Q)$ is for the remainder after Euclidean division.

Definition 4.1. We let $SremS(P, Q)$ denote the sequence $SremS(P, Q) := (P_0, P_1, \ldots, P_i, \ldots, P_N)$, called the *signed remainder sequence*.

Example 9. If $P = x^2 + 2bx + c$, then set $Q = 2x + 2b$. Then $P_0 = P$ and $P_1 = Q$, and $P_2 = -(c - b^2)$. Note that $\deg(P_i) > \deg(P_{i+1})$ for $i \geq 1$.

Definition 4.2. Given $x \in R$, we define the *variation at* x $V(P, Q)$ of P and Q to be

$$V(P, Q)(x) := Var(sign(SremS(P, Q)(x))).$$

Example 10. From our last example, when $x = \infty$ we have $V(P, Q)(\infty) = 0$ if $b^2 - c \geq 0$ and $V(P, Q)(\infty) = 1$ in the other case.

Definition 4.3. We next define the *index* of P, Q to be

$$Ind(\tfrac{Q}{P}; a, b) := \#\text{ of jumps from } -\infty \text{ to } \infty \text{ of } \tfrac{Q}{P} \text{ in } (a, b)$$
$$-\#\text{ of jumps from } \infty \text{ to } -\infty \text{ of } \tfrac{Q}{P} \text{ in } (a, b)$$

Example 11. Consider the function $\frac{x-2}{(x-1)(x-3)(x-4)}$. Graphing the function or looking at sided limits at $a = 1, 3, 4$, we see that $Ind(\frac{x-2}{(x-1)(x-3)(x-4)}; 0, 5) = -1$.

Note that $\frac{Q}{P}$ makes a jump at x if and only if the multiplicity $\mu_P(x)$ of the root x of P is strictly larger than the multiplicity $\mu_Q(x)$ of the root x of Q (if x is not a root, then the multiplicity is zero). Note that $\frac{Q}{P}$ jumps from $-\infty$ to ∞ if and only if $(\mu_P(x) - \mu_Q(x)) > 0$ and odd, and $PQ > 0$ at x^+. Similarly, the jump from ∞ to $-\infty$ happens if and only if $(\mu_P(x) - \mu_Q(x)) > 0$ and odd, and $PQ < 0$ at x^+.

Now let us consider $Ind(\frac{P'Q}{P}; a, b)$. If $P = (X - x)^{\mu_P(x)} \cdot P_1$ with $P_1(x) \neq 0$, then $P' = \mu_P(x)(X - x)^{\mu_P - 1} \cdot P_1 + (X - x)^{\mu_P(x)} \cdot P_1' = (X - x)^{\mu_P(x)-1}(\mu_P(x)P_1 + (X - x)P_1')$. We can deduce that $\frac{P'Q}{P}$ jumps from $-\infty$ to ∞ at x if and only if $P(x) = 0$ and $Q(x) > 0$, and $\frac{P'Q}{P}$ jumps from ∞ to $-\infty$ at x if and only if $P(x) = 0$ and $Q(x) < 0$.

So

$$Ind(\frac{P'Q}{P}; a, b) = \#\text{ of roots of } P \text{ at which } Q > 0$$
$$-\#\text{ of roots of } P \text{ at which } Q < 0.$$

In particular, when $Q \equiv 1$, the index just counts the number of roots of P between a and b.

Theorem 12. *Let $P, Q \in R[x]$, $a < b$ and suppose that a, b are not roots of P. Then*

$$Ind(\frac{Q}{P}; a, b) = V(P, Q)(a) - V(P, Q)(b).$$

Proof. The proof is elementary and by induction on the length of the signed remainder sequence $SremS(P, Q)$. Step 1: Suppose furthermore that a, b are not roots of any of the polynomials in the signed remainder sequence $SremS(P, Q)$. Let $R = Rem(P, Q)$, and for any $x \in R$ let $\sigma(x) = \text{sign}P(x)Q(x)$ and we prove:

1. $Ind(\frac{Q}{P}; a, b) = \begin{cases} Ind(\frac{-R}{Q}; a, b) & \text{if } \sigma(a)\sigma(b) = +1, \textit{and} \\ Ind(\frac{-R}{Q}; a, b) + \sigma(b) & \text{if } \sigma(a)\sigma(b) = -1. \end{cases}$

2. $TarQ(P,Q;a,b) = \begin{cases} TarQ(Q,-R;a,b) & \text{if } \sigma(a)\sigma(b) = +1, \textit{and} \\ TarQ(Q,-R;a,b) + \sigma(b) & \text{if } \sigma(a)\sigma(b) = -1. \end{cases}$

There are several cases to consider, but it is all very easy to check.

STEP 2: If a, b are roots of some polynomials in $SRemS(P,Q)$, then we can pick $a < a' < b' < b$ such that no polynomial in $SRem(P,Q)$ have a root in $(a,a']$, $[b',b)$. We claim that $TarQ(P,Q;a,b) = TarQ(P,Q;a',b')$. Since a, b are not roots of P or Q, they are necessarily not roots of $gcd(P,Q)$. This means that if $P_i(a) = 0$ then necessarily $P_{i-1}(a)P_{i+1}(a) < 0$, using the fact that $P_{i+1} = -Rem(P_{i-1}, P_i)$. So for any three consecutive Sturm polynomials, P_{i-1}, P_i, P_{i+1}, if $P_i(a) = 0$ then the number of sign variations of the triple (P_{i-1}, P_i, P_{i+1}) is constant from a to a'. Since there is no change in the sign variations of any triple from a to a', there is no change in the variation.

Checking the base case and finishing the many possible cases not checked here are exercises.

□

Suppose $S \subset R^k$ is a semi-algebraic set, meaning S is defined by a formula involving polynomial inequalities and inequalities. Our goal is to prove that the projection of S after forgetting one variable is again a semi-algebraic set. Since S is defined by a formula, and any formula has a *disjunctive normal form*, we can assume that S is the union of sets defined by a simple formula of the form

$$(P_1 = \cdots = P_\ell = 0 \wedge P_{\ell+1} > 0 \wedge \ldots P_s > 0),$$

and we call a set defined by such a formula a *basic* semi-algebraic set. In particular, we can replace the conjunction $P_1 = \cdots = P_\ell = 0$ with the single atom $Q = \sum_{i=1}^{\ell} P_i^2 = 0$.

We show directly that for a basic semi-algebraic set and the projection which forgets one variable, the projection of the basic semi-algebraic set is again semi-algebraic. This would complete the Theorem 17.

Theorem 13. *Let S be a basic semi-algebraic set defined by $(Q = 0, P_1 > 0, \ldots, P_s > 0)$, and let $\pi : R^k \to R^{k-1}$. Then $\pi(S)$ is a semi algebraic subset of R^{k-1}.*

Proposition 14. *Let V be a basic algebraic set defined by $P = 0$, and $\pi : R^k \to R^{k-1}$ the projection. Then $\pi(V)$ is semi-algebraic.*

Proof. Think of $P \in R[x_1, \ldots, x_{k-1}][x_k]$. Then $x \in \pi(V)$ if and only if $P(x, X_k)$ has a real root (a value for X_k for which $P(x, X_k) = 0$).

FINISH NEXT TIME

5 January 26, Day 5

We combine the information from last time.

Theorem 15 (Sturm Theorem)**.** *Let $P, Q \in R[x]$, $a < b$, and suppose $P(a)P(b) \neq 0$. Then*

(i) $Var(sign(SremS(P,Q)))(a) - Var(sign(SremS(P,Q)))(b) = Ind(\frac{Q}{P}; a, b)$,

(ii) $Var(sign(SremS(P,P'Q)))(a) - Var(sign(SremS(P,P'Q)))(b) = \begin{array}{l}(\#\textit{ of roots of } P \textit{ at which } Q > 0) - \\ (\#\textit{ of roots of } P \textit{ at which } Q < 0)\end{array}$,

and

(iii) *By substituting Q by 1, we have $V(sign(SremS(P,P')))(a) - V(sign(SremS(P,P')))(b) =$ $\#$ of roots of P in (a,b).*

Definition 5.1. Let $P, Q \in D[x]$ for D a domain. Write

$$P = a_p X^p + \cdots + a_0$$
$$Q = b_q X^q + \cdots + b_0,\ b_q \neq 0.$$

The Pseudo-remainder $Prem(P,Q) = rem(b_q^d P, Q)$ where d is the smallest EVEN number greater than or equal to $p - q$. Observe that $sign(Prem(P,Q))(a) = sign(rem(P,Q))(a)$ for all $a \in R$.

Definition 5.2. We define the *tree of possible signed pseudo-remainder sequences.* Each leaf L of the tree corresponds to a formula ϕ_L. PICTURE HERE?

1. Each $y \in R^\ell$ satisfies at most one of the formulas ϕ_L.
2. Suppose $\phi_L(y)$ is true. Then for every $x \in R$, $sign(SremS(P_y, Q_y)(x)) = sign(P_L(x))$ where $P_L(x)$ is the unique PATH ending at leaf L and P_y, Q_y are the polynomials $P(y_1, \ldots, y_\ell, X),\ Q(y_1, \ldots, y_\ell, X) \in R[X]$.

Theorem 16. *Let $Q \in R[X_1, \ldots, X_k]$ and let $Z(Q, R^k) = \{x \in R^k |\ Q(x) = 0\}$, and let $\pi : R^k \to R^{k-1}$ be the projection along X_k. Then, $\pi(Z(Q, R^k))$ is a semi-algebraic subset of R^{k-1}.*

Proof. Consider $\pi(Z(Q, R^k)) = \{(x_1, \ldots, x_{k-1}) \in R^{k-1} |\ Q(x_1, \ldots, x_{k-1}, X_k)$ has a real root$\}$. We know how to compute the real roots of a real polynomial: we can use Sturm sequences. Thinking of $x_1, \ldots, x_{k-1}$ as parameters, consider the tree of possible signed pseudo-remainder sequences for the polynomials $Q, \frac{\partial Q}{\partial X_k}$ which we are thinking of as *one-variable* polynomials with k parameters. The various leaves L of this tree have corresponding ϕ_L formulas, and for each leaf L we have a path starting at $P_0 = P$ and ending at L and denote the path $P_L = (P_0, P_1, \ldots, P_m, 0)$. Let $(Q_0, Q_1, \ldots, Q_m, 0)$ be the sequence of leading coefficients of P_L, so $Q_i \in R[x_1, \ldots, x_{k-1}]$. Let ψ_L be the formula that expresses $Var(sign(Q_0, \ldots, Q_m))(-\infty) - Var(sign(Q_0, \ldots, Q_m))(+\infty) > 0$ given specialization of the parameters from the condition that we are on the leaf L. Then ψ_L has atoms of the form $Q_i = 0, Q_i < 0, Q_i > 0$. Finally, we consider the formula

$$\Phi : \bigvee_{L \text{ leaf}} \phi_L \wedge \psi_L.$$

The formula Φ defines $\pi(Z(Q, R^k))$, and hence $\pi(Z(Q, R^k))$ is a semi-algebraic set.

□

Notation 1. Denote by $Ind(\frac{Q}{P}) := V(P,Q)(-\infty) - V(P,Q)(+\infty)$.

We need to modify the above proof to deal with the case where Z is just a semi-algebraic set. In particular, we need Sturm sequences to deal with finding roots of P subject to some additional $Q_1 > 0$. Recall, we have

$$\begin{aligned}
Ind(\frac{P'}{P}) = &\quad count(P=0, Q=0) + count(P=0, Q>0) &+ count(P=0, Q<0)\\
Ind(\frac{P'Q}{P}) = &\quad count(P=0, Q>0) &- count(P=0, Q<0)\\
Ind(\frac{P'Q^2}{P}) = &\quad count(P=0, Q>0) &+ count(P=0, Q<0)
\end{aligned}$$

which we can write as a system of linear equations as follows.

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} ct(P=0, Q=0) \\ ct(P=0, Q>0) \\ ct(P=0, Q<0) \end{bmatrix} = \begin{bmatrix} Ind(\frac{P'}{P}) \\ Ind(\frac{P'Q}{P}) \\ Ind(\frac{P'Q^2}{P}) \end{bmatrix}$$

In the above, we define

$$M_1 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix}$$

For two polynomials, we get a similar system with a matrix M_2.

$$\begin{array}{c} \\ 1\cdot 1 \\ 1\cdot Q_2 \\ 1\cdot Q_2^2 \\ Q_1\cdot 1 \\ Q_1Q_2 \\ Q_1Q_2^2 \\ Q_1^2\cdot 1 \\ Q_1^2Q_2 \\ Q_1^2Q_2^2 \\ \\ \end{array} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{array}{c} \\ 00 \\ 0+ \\ 0- \\ +0 \\ ++ \\ +- \\ -0 \\ -+ \\ -- \end{array} \begin{bmatrix} ct(P=0,Q_1=0,Q_2=0) \\ ct(P=0,Q_1=0,Q_2>0) \\ ct(P=0,Q_1=0,Q_2<0) \\ ct(P=0,Q_1>0,Q_2=0) \\ ct(P=0,Q_1>0,Q_2>0) \\ ct(P=0,Q_1>0,Q_2<0) \\ ct(P=0,Q_1<0,Q_2=0) \\ ct(P=0,Q_1<0,Q_2>0) \\ ct(P=0,Q_1<0,Q_2<0) \end{bmatrix} = \begin{bmatrix} Ind(\frac{P'\cdot 1}{P}) \\ Ind(\frac{P'Q_2}{P}) \\ Ind(\frac{P'Q_2^2}{P}) \\ Ind(\frac{P'Q_1}{P}) \\ Ind(\frac{P'Q_1Q_2}{P}) \\ Ind(\frac{P'Q_1Q_2^2}{P}) \\ Ind(\frac{P'Q_1^2}{P}) \\ Ind(\frac{P'Q_1^2Q_2}{P}) \\ Ind(\frac{P'Q_1^2Q_2^2}{P}) \end{bmatrix}$$

EXERCISE 1. Show that $M_2 = M_1 \otimes M_1 = [m_{ij}M_1]$ where $M_1 = [m_{ij}]$. In particular, show M_2 is invertible.

6 January 28, day 6

Here is what we have shown.

Theorem 17 (Tarski-Seidenberg theorem)**.** *Let D be an ordered domain contained in a real closed field R and let*

$$\phi(X_1,\ldots,X_k) := (\mathcal{Q}_1 Y^1)(\mathcal{Q}_2 Y^2)\ldots(\mathcal{Q}_\omega Y^\omega)\tilde{\phi}(X, Y^1,\ldots,Y^\omega)$$

be a first order formula with coefficients in D where each $\mathcal{Q}_i$ is either a universal $\forall$ or existential $\exists$ quantifier, and $\tilde{\phi}$ is a quantifier free formula. Then, there exists a quantifier-free first order formula $\psi(X_1,\ldots,X_k)$ with coefficients in D such that ϕ is equivalent to ψ, and in particular $\mathcal{R}(\varphi, R^k) = \mathcal{R}(\psi, R^k)$ the semi-algebraic sets they define (as their realizations) are the same.

The most important application of this Theorem for the time being is the following so-called Transfer principle.

Corollary 18 (Transfer theorem)**.** *If ϕ is a sentence with coefficients in D and R_1 is any real closed field containing D, then ϕ is true/satisfied over R_1 if and only if ϕ is satisfied over R.*

We mention that in order to prove the Theorem above, we constructed an effective algorithm for quantifier elimination. We might ask about the complexity of ψ that occurs as a result of the complexity of ϕ. For example, what are the degrees of the polynomials in ψ and how many polynomials do you need based on the number and degrees of the polynomials appearing in ϕ. As another corollary to the Theorem, then, we can speak of the complexity of ψ in this way.

Corollary 19. *There exists a uniform bound (which depends only on the number of polynomials in ϕ, their degrees, and the number of variables but* NOT *on the coefficients of the polynomials) on the size of ψ in terms of the size of ϕ.*

The proof we gave is, more or less, Tarski's [Artin's?] original proof. However, the bound in this case is not elementary primitive recursive: the tower of exponents increases with the number of variables. Much tighter bounds are known, however.

Example 12 (An application of quantifier elimination). Let $R = \mathbb{R}$ and $S \subseteq R^k$ a semi-algebraic set. Then the closure $cl(S)$, interior $int(S)$, and frontier/boundary $\partial(S)$ are also semi-algebraic. Suppose that $S = \mathcal{R}(\phi, R^k)$ is defined by the quantifier free formula ϕ. Then $cl(S)$ is defined by the formula with quantifiers

$$\psi(X): \ (\forall \varepsilon)(\varepsilon > 0 \implies (\exists y)(|x-y|^2 < \varepsilon \wedge \phi(y))).$$

By Tarski-Seidenberg there exists a quantifier free θ which is equivalent to ψ. Similar formulas can be written for $int(S)$ and $\partial(S)$.

Remark 20. Note that the closure $cl(S)$ is NOT necessarily formed by just relaxing any strict inequalities appearing in the representation of S to non-strict inequalities. For example, consider $\phi(X): \ x^2(x-1) > 0$ and the relaxation $\psi(X): \ x^2(x-1) \geq 0$. The set $\mathcal{R}(\phi, R) = (1, \infty)$ the open interval and $\mathcal{R}(\psi, R) = \{0\} \cup [1, \infty)$ has two connected components. In general, if you have a polynomial $P(X_1, \ldots, X_k)$ of degree d in k variables, and you perform quantifier elimination on the formula $(\exists X)P(X) > 0$ you get polynomials of degree d^{4k}.

Definition 6.1. A quantifier free first order formula ϕ is "*open*" if it has no negations and all atoms are of the form $P > 0, \ P < 0$. Clearly, an open formula ϕ defines an open semi-algebraic set $\mathcal{R}(\phi, R^k)$. The converse is actually TRUE, but difficult to prove.

Theorem 21 (To be proved at a later date)**.** *A semi-algebraic set $S \subseteq R^k$ is open if and only if it has a description as $S = \mathcal{R}(\phi, R^k)$ for some open formula ϕ.*

The next question which naturally arises from this theorem is the following. Given an open semi-algebraic set S defined by ψ which is not assumed to be an open formula, find a ϕ open formula which describes the set S and bounds on the number and degrees of the polynomials appearing in ϕ depending on the number and degrees of the polynomials appearing in ψ.

6.1 Hilbert's 17th problem

Example 13 (Robinson's example). Consider the polynomial $P(X,Y) = 1 - 3X^2Y^2 + X^4Y^2 + X^2Y^4$. Note that $P(X,Y) \geq 0$ over R^2 as a consequence of the arithmetic mean begin larger than the geometric mean. The geometric mean of $1, X^4Y^2, X^2Y^4$ is X^2Y^2. However, the polynomial P is NOT a sum of squares. To see this fact, suppose to the contrary that $P(X,Y) = \sum_i h_i^2(X,Y)$ is a sum of squares. Notice this means $\deg h_i \leq 3$. The possible monomials of h_i are thus among $\mathcal{M} = \{1, X, Y, X^2, Y^2, X^3, Y^3, XY, X^2Y, XY^2\}$. Note that X^3 can not be a monomial of any h_i since otherwise X^6 would appear in $P(X,Y)$. Similarly, Y^3 can not occur as a monomial of any h_i. We can then conclude that X^2 does not occur since X^4 is not a monomial of $P(X,Y)$. Similarly, Y^2 can not occur. Continuing in this vein, X and Y can not occur. To finish the argument, the coefficient of X^2Y^2 must be a sum of squares since the only way to get the monomial X^2Y^2 with the monomials of $\mathcal{M}$ which we have not excluded is with XY, but this is a contradiction since -3 is not a sum of squares.

Example 14 (Robinson polynomial as a rational sum of squares). The Robinson polynomial can be written as

$$P(X,Y) = \frac{X^2Y^2(X^2+Y^2+1)(X^2+Y^2-2)^2 + (x^2-Y^2)^2}{(X^2+Y^2)^2}$$

and note that this allows the numerator to have higher degree than $P(X,Y)$. The number of squares needed in this case is 4.

We are now ready to give Artin's proof of Hilbert's 17^{th} problem.

Artin's proof of Hilbert's 17^{th} problem. Suppose that $P \in R[X_1, \ldots, X_n]$ is non-negative and suppose that P is not a sum of squares of rational functions. Then $P \notin \sum F^2$ where $F = R(X_1, \ldots, X_n)$. The field F can be ordered, and hence it is a real field. In particular, the cone $\sum F^2$ is proper. Using [a previous??] Lemma,

$$\sum F^2[-P] = \{a - bP | \ a, b \in \sum F^2\}$$

is a proper cone. So this proper cone belongs to the positive cone of an ordering $\leq_P$ of F. Since P is not in this cone, $P <_P 0$ must be negative in this ordering $\leq_P$ of F. Now, consider the real closure R_1 of the ordered field $(F, \leq_P)$. Write $P = \sum a_\alpha X^\alpha$ with $a_\alpha \in R$ (and X^α means $X_1^{\alpha_1} \dots X_k^{\alpha_k}$). Consider the first order formula

$$(\exists T_1)(\exists T_2) \dots (\exists T_n) \sum a_\alpha T^\alpha < 0.$$

The formula ϕ has coefficients in R, we have

$$(R, \leq) \hookrightarrow (F, \leq_P) \hookrightarrow (R_1, \leq)$$

and ϕ is satisfied over R_1 since with $T_i = X_i \in F$ we have $P = \sum a_\alpha X^\alpha <_P 0$. By Tarski-Seidenberg transfer theorem, ϕ is satisfied in R. So P is not non-negative over R, which is a contradiction with the original assumption.

□

7 February 2, Day 7

Homework Assignment #1 assigned today. Due in 2 WEEKS.

Today we formulate and the real analogue of the Nullstellensatz. We first formulate the statement over an algebraically closed field.

Theorem 22 (Complex Nullstellensatz)**.** *If C is an algebraically closed field and let $I \subseteq C[X_1, \dots, X_n]$ an ideal, then $V_C(I) = \{x \in C^n |\ (\forall P)(P \in I \implies P(x) = 0)\}$ satisfies $\mathcal{I}(V_C(I)) = \sqrt{I}$, where $\sqrt{I} = \{f \in C[X_1, \dots, X_n] |\ f^n \in I$ for some $n > 0\}$. Equivalently, $V_C(I)$ satisfies $V_C(I) = \emptyset \iff 1 \in I$.*

Proof. We prove one direction of the inclusion in the first statement. Let $f \in \mathcal{I}(V_C(I))$ and consider the polynomial $fY - 1 \in C[X_1, \dots, X_n, Y]$. Let $I = (P_1, \dots, P_s)$, then the variety $V(fY - 1, P_1, \dots, P_s) = \emptyset$. By the second statement we have the polynomial identity $1 = g(fY - 1) + g_1 P_1 + \dots + g_s P_s$ where $g, g_1, \dots, g_s \in C[X_1, \dots, X_n, Y]$. The this identity, substitute $Y = \frac{1}{f}$ and clear denominators to get an expression of the form $1 = \frac{P}{f^n}$ where $P \in I$.

□

This theorem requires the field to be algebraically closed. Indeed, the ideal $I = (x^2 + 1)$ over $\mathbb{R}$ does not contain the element $1 \notin I$, but of course $V_{\mathbb{R}}(I) = \emptyset$ since this polynomial is strictly positive.

Definition 7.1 (Real ideals)**.** Let A be a commutative ring and $I \subseteq A$ an ideal. The ideal I is said to be a *real ideal* if it satisfies $\forall a_1, \dots, a_p \in A$ if $a_1^2 + \dots + a_p^2 \in I$, then $a_i \in I$ for all $1 \leq i \leq p$.

Definition 7.2 (The real radical of an ideal)**.** Given $I \subseteq A = R[X_1, \dots, X_n]$, we define the *real radical* of I as

$$\sqrt[R]{I} = \{a \in A |\ \exists m > 0,\ b_1, \dots, b_p \in A \text{ s.t. } a^{2m} + b_1^2 + \dots + b_p^2 \in I\}.$$

Theorem 23 (Real Nullstellensatz)**.** *Let R be a real closed field, and I an ideal of $R[X_1, \dots, X_n]$. Then $I = \mathcal{I}(V_R(I))$ if and only if I is a real ideal.*

Lemma 2. *If $I \subseteq A$ is a real ideal then I is radical. Moreover, if A is Noetherian then all minimal prime ideals containing A are real.*

Proof. Let $a^n \in I$ with I a real ideal. If n is even, then $a^{\frac{n}{2}} \in I$, and if n is odd, then $a^{\frac{n+1}{2}} \in I$. In either case, we have reduced the power of a, so continuing inductively we obtain $a \in I$.

Now suppose A is Noetherian and let $P_1, \dots, P_m$ be the finitely many minimal primes containing I. Suppose, seeking a contradiction, that P_1 is not a real ideal. Then there exists $a_1, \dots, a_p \notin P_1$ such that

$a_1^2 + \cdots + a_p^2 \in P_1$. Choose, for each $i = 2, \ldots, m$, an element $b_i \in P_i$–P_1 and let $b = b_2 \cdots b_m$. Now, P_1 was prime, and so $b \in \cap_{i=2}^m P_i$ and $b \notin P_1$. Finally, consider the sum of squares $(a_1 b)^2 + \cdots + (a_p b)^2 = (a_1^2 + \cdots + a_p^2) b^2 \in \cap_{i=1}^m P_i = I$, since I is real and hence radical. In particular, $a_1 b \in I$ implies that $a_1 b \in P_1$, but $a_1, b \notin P_1$ is a contradiction.

□

Lemma 3. *A prime ideal $P \subseteq A$ is real if and only if the field of fractions $\frac{A}{P}$ is a real field.*

Proof. Just use the characterization that F is a real field if and only if $\sum_{i=1}^p a_i^2 = 0$ for $a_i \in F$ implies $a_i = 0$ for all $i = 1, \ldots, p$.

□

We now prove the Real Nullstellensatz.

Proof of Theorem 23. One inclusion is always true, $I \subseteq \mathcal{I}(V_R(I))$. We first prove the easier, forward direction. Let $f_1^2 + \cdots + f_p^2 \in I$. Then for every $x \in V_R(I)$ we have $f_1^2(x) + \cdots + f_p^2(x) = 0$, which implies $f_i(x) = 0$ for all $x \in V_R(I)$ and $i = 1, \ldots, p$. Therefore, $f_i \in \mathcal{I}(V_R(I)) = I$, which implies that I is real.

Now, assume that I is real and we show that $I \supseteq \mathcal{I}(V_R(I))$. Let $f \in A$–I, and we show that $f \notin \mathcal{I}(V_R(I))$. We will need to use Tarski-Seidenberg to show this fact. Since I is real, we have that I is the intersection of all minimal primes which contain I. Write $I = \cap_{i=1}^m P_i$ where $P_1, \ldots, P_m$ are all the minimal primes containing I. Without loss of generality, suppose $f \in A$–P_1. Let K be the field of fractions of $\frac{A}{P_1}$ which is a real field by Lemma 3. We have the following natural inclusion, where the order $\leq$ on R is extended to K by looking at the proper cone which is the image of the natural surjection $A \twoheadrightarrow \frac{A}{P_1}$ of the sums of squares of A.

$$(R, \leq) \subseteq (K, \leq)$$

Let R_1 be a real closure of $(K, \leq)$. Let $I = (P_1, \ldots, P_s)$ and consider the first order formula ϕ below.

$$\phi : \ (\exists T_1, \ldots, T_n)(f(T_1, \ldots, T_n) \neq 0 \wedge \bigwedge_{i=1}^m P_i(T_1, \ldots, T_n) = 0)$$

Consider $T_i = \overline{X_i} \in K$ the image in K of X_i under the natural surjection. The formula ϕ is thus true in R_1, and hence by Tarski-Seidenberg transfer principle, Corollary 18, we have that the formula is true over R as well. Hence, $f \notin \mathcal{I}(V_R(I))$.

□

Theorem 24. *Let A be a Noetherian ring and $I \subseteq A$ any ideal. Then the real radical $\sqrt[R]{I} = \{a \in A | \ \exists m > 0, \ b_1, \ldots, b_p \in A, \ a^{2m} + b_1^2 + \cdots + b_p^2 \in I\}$ is the smallest real ideal which contains I, and $\sqrt[R]{I}$ is the intersection of all real prime ideals containing I.*

Proof. We show that, assuming that $\sqrt[R]{I}$ is an ideal, that this ideal is real. Let $a_1^2 + \cdots + a_p^2 \in \sqrt[R]{I}$. Then $(a_1^2 + \cdots + a_p^2)^{2m} + b_1^2 + \cdots + b_l^2 \in I$ and thus $a_1^{4m} + s.o.s. \in I$ and hence by definition $a_1 \in \sqrt[R]{I}$, so this ideal is real. We now show that $\sqrt[R]{I}$ is an ideal. The hard part is showing that $a_1, a_2 \in \sqrt[R]{I}$ implies $a_1 + a_2 \in \sqrt[R]{I}$. Let $a_1, a_2 \in \sqrt[R]{I}$. Then $a_1^{2m} + b_1^2 + \cdots + b_p^2 \in I$, and also $a_2^{2m'} + c_1^2 + \cdots + c_q^2 \in I$. Consider the expression

$$(a_1 + a_2)^{2(m+m')} + (a_1 - a_2)^{2(m+m')} = a_1^{2m} \cdot (s.o.s.) + a_2^{2m'} \cdot (s.o.s.). \tag{1}$$

For some elements $x, y \in I$ we have $a_1^{2m} = x - (s.o.s.)$ and $a_2^{2m'} = y - (s.o.s.)$. Substitution into Eqn. 1 yields

$$(a_1 + a_2)^{2(m+m')} + (a_1 - a_2)^{2(m+m')} = (x - s.o.s.)(s.o.s.) + (y - s.o.s.)(s.o.s.)$$

which implies that $(a_1 + a_2)^{2(m+m')} + (a_1 - a_2)^{2(m+m')} + s.o.s. \in I$. Hence we have $a_1 + a_2 \in I$.

Now, let $J \supseteq I$ be a real ideal containing I. Let $a \in \sqrt[R]{I}$. Then $a^{2m} + s.o.s. \in I \subseteq J$. Since J is real, it is radical and so $a \in J$. Hence, $\sqrt[R]{I}$ is the smallest real ideal containing I.

8 February 4, Day 8

We proved the Real Nullstellensatz, which says that if $I \subseteq R[X_1, \ldots, X_n]$ is an ideal with R real closed, then $\mathcal{I}(V_R(I)) = I$ if and only if I is a real ideal. Furthermore, we showed that if A is a commutative ring and $I \subseteq A$ is an ideal, then the real radical $\sqrt[R]{I} := \{a \in A |\ \exists m > 0,\ b_1, \ldots, b_p \in A \text{ s.t. } a^{2m} + b_1^2 + \cdots + b_p^2 \in I\}$ is the smallest real ideal containing I. We still need to show that the real radical $\sqrt[R]{I}$ is the intersection of all real prime ideals containing I or equal to A if there are no real prime ideals containing I.

Theorem 24. *Let A be a Noetherian ring and $I \subseteq A$ any ideal. Then the real radical $\sqrt[R]{I} = \{a \in A |\ \exists m > 0,\ b_1, \ldots, b_p \in A,\ a^{2m} + b_1^2 + \cdots + b_p^2 \in I\}$ is the smallest real ideal which contains I, and $\sqrt[R]{I}$ is the intersection of all real prime ideals containing I.*

Proof. Finishing the proof from last time, it only remains to show the last statement. We have that

$$\mathcal{J} := \bigcap_{\substack{J \text{ real prime} \\ J \supset I}} J \supset \sqrt[R]{I}.$$

Suppose that $a \in A - \sqrt[R]{I}$. By Zorn's Lemma, there exists a real ideal J which is maximal with respect to the property that J is a real ideal, contains I, and does not contain the element $a \notin J$. We claim that J is prime, in which case we are done since this verifies that $a \notin \mathcal{J}$. Suppose, seeking a contradiction, that J is not prime. Then there exist $b, b' \in A$ such that $b, b' \notin J$ but $bb' \in J$. Consider the ideals $J_1 := J + (b),\ J_2 := J + (b')$ which strictly contain J. The ideal J was real, so $J = \sqrt[R]{J}$, and hence $\sqrt[R]{J_1} \supsetneq J$ and $\sqrt[R]{J_2} \subsetneq J$. By maximality of J, we have $a \in J_1 \cap J_2$. Write

$$\begin{aligned} a^{2m} + s.o.s. &= j + cb \ j \in J, c \in A \\ a^{2m'} + s.o.s. &= j' + c'b \ j' \in J, c' \in A \\ \implies \qquad a^{2(m+m')} + s.o.s. &= jj' + jc'b' + j'cb + cc'bb' \in J. \end{aligned}$$

So $a \in \sqrt[R]{J} = J$, which is a contradiction.

□

We obtain the following Corollary, which provides a certificate of a statement of the form: $P \in R[X_1, \ldots, X_n]$ vanishes at all the common zeros of $P_1, \ldots, P_s$.

Theorem 25. *Let R be real closed and $I \subseteq R[X_1, \ldots, X_n]$ an ideal. Then, $\mathcal{I}(V_R(I))$ is the smallest real ideal containing I, and hence $\mathcal{I}(V_R(I)) = \sqrt[R]{I}$. In particular, if $P \in \mathcal{I}(V_R(I))$ there exists $m > 0, Q_1, \ldots, Q_p \in R[X_1, \ldots, X_n]$ such that $P^{2m} + Q_1^2 + \cdots + Q_p^2 \in I$.*

Proof. It suffices to show that $\mathcal{I}(V_R(I))$ is the smallest real ideal which contains I. Let $I' = \mathcal{I}(V_R(I))$. Then we have $V_R(I') = V_R(I)$, and hence $\mathcal{I}(V_R(I')) = \mathcal{I}(V_R(I)) = I'$ and I' is real. It is also clear that $I' \supset I$. Now suppose I'' is another real ideal which contains I. Hence, $I''' := I' \cap I'' \supset I$, and I''' is a real ideal. Now, $V_R(I''') = V_R(I') = V_R(I)$ is verified by

$$\begin{aligned} & I' \supset I' \cap I'' \supset I \\ \implies & V_R(I') \subset V_R(I' \cap I'') \subset V_R(I) \end{aligned}$$

and $V_R(I') = V_R(I)$, and so

$$I''' = \mathcal{I}(V_R(I''')) = \mathcal{I}(V_R(I') = I',$$

and hence $I' \subset I''$ as desired.

□

Definition 8.1 (The cone $\sum A^2[(F_j)_{j\in J}$, multiplicative monoid)**.** For a family of polynomials $(F_j)_{j\in J} \subset R[X_1,\dots,X_n]$, we define the *cone generated by the family* $(F_j)_{j\in J}$ to be

$$P = \sum A^2[(F_j)_{j\in J}] := \{F_j + (s.o.s.)F_{j_1}\cdots F_{j_m} |\ j_1,\dots,j_m \in J\}.$$

We define the *multiplicative monoid generated by the family* $(G_k)_{k\in K}$ to be

$$M = \{G_{k_1}\cdots G_{k_m} |\ k_1,\dots,k_m \in K\}.$$

Theorem 26. *Let $S \subseteq R^n$ be defined by the conditions $(F_j \geq 0)_{j\in J}, (G_k \neq 0)_{k\in K}, (H_\ell = 0)_{\ell\in L}$ for the families of polynomials $(F_j)_{j\in J}, (G_k)_{k\in K}, (H_\ell)_{\ell\in L} \subseteq R[X_1,\dots,X_n]$. Let $P = \sum A^2[(F_j)_{j\in J}]$ the cone generated by the family $(F_j)_{j\in J}$, let M be the multiplicative monoid generated by $(G_k)_{k\in K}$, and let $I = (H_\ell |\ \ell \in L)$ be the ideal generated by the family $(H_\ell)_{\ell\in L}$. Then S is empty if and only if there exists $p \in P, m \in M, i \in I$ such that $p + m^2 + i = 0$.*

Before we can prove the theorem, we need some to do some preliminary work.

Definition 8.2 (Cone of a ring)**.** Let A be a commutative ring. A subset $P \subseteq A$ is called a cone if it satisfies

1. $a, b \in P \implies a + b \in P$,
2. $a, b \in P \implies ab \in P$,
3. $a^2 \in P$ for all $a \in A$,

and furthermore P is called proper if in addition

4. $-1 \notin P$.

Example 15. The cone $\sum A^2$ is contained in every cone of A.

Example 16. Let $A = R[X_1,\dots,X_n]$ with R real closed and let $S \subset R^n$. Define

$$W(S) = \{P \in R[X_1,\dots,X_n] |\ P(x) \geq 0,\ \forall x \in S\}$$

which is a proper cone.

Definition 8.3. Let $P \subset A$ a cone and $I \subseteq A$ an ideal. We say that I is *P-convex* if it satisfies $P_1, P_2 \in P$ and $P_1 + P_2 \in I$ implies $P_1, P_2 \in I$. The ideal I is called *P-radical* if $a^2 + p \in I, p \in P$ implies $a \in I$.

Lemma 4. *An ideal I is P-radical if and only if I is radical and P-convex.*

Proof. If I is P-radical, then I is radical. If $P_1 + P_2 \in I$ and $P_1, P_2 \in P$. Then $P_1^2 + \underbrace{P_1P_2}_{\in P} \in I$, which implies that $P_1 \in I$ and hence I is P-convex.

If I is radical and P-convex, suppose $a^2 + p \in I$ and $p \in P$. Then, by virtue of I being P-convex and $a^2 \in P$ we have $a^2 \in I$. Thus, by virtue of I being radical we have $a \in I$ as desired.

□

Definition 8.4 (Prime cone)**.** A cone $P \subset A$ is called a *prime cone* if $ab \in P$ implies either $a \in P$ or $-b \in P$.

Example 17. If $A = F$ is a field, then every cone P which is the positive cone of an order is a prime cone. That is, if $ab > 0$ then either $a > 0$ or $b < 0$. Also, notice that in this case we have $P \cup -P = A$ and $P \cap -P = \{0\}$. These facts hold in some generality, and the specific properties are listed below.

Lemma 5. *Let $P \subseteq A$ be a prime cone. Then*

1. *$P \cup -P = A$, and*

2. *$P \cap -P$ is a prime ideal.*

Proof. We have $a^2 \in P$ which means that $a \in P$ or $-a \in P$ for all $a \in P$. To show the second statement, we only show that $P \cap -P$ is a prime ideal, and we leave as an easy exercise to check that $P \cap -P$ is an ideal. Suppose that $ab \in P \cap -P$ and that $a \notin P \cap -P$. We want to show that $b \in P \cap -P$. We have two cases to consider. Note that since $ab \in P \cap -P = -(P \cap -P)$ we have $-(ab) \in P \cap -P$.

Case $ab \in P$ **and** $a \notin P$**:** We have $-b \in P$ by virtue of P being a prime cone. Similarly, $a(-b) \in P$ and $a \notin P$ implies $b \in P$. So $b \in P \cap -P$.

Case $ab \in P$ **and** $a \notin -P$**:** We have $b \in P$ by virtue of $-a \notin P$, $-(ab) \in P$ and P being a prime cone. Similarly, $ab \in P$ means $(-a)(-b) \in P$ and $-a \notin P$, so $-b \in P$. Hence, $b \in P \cap -P$.

In all cases, $b \in P \cap -P$ and so this ideal is prime.

□

Definition 8.5. If P is a prime cone, then the prime ideal $P \cap -P$ is called the *support of* P, and we write $supp(P) = P \cap -P$.

9 February 9, Day 9

The following theorem is a direct consequence of the Tarski-Seidenberg theorem. We state the version that we will make use of the most often.

Theorem 27 (Artin-Lang Homomorphism Theorem)**.** *Let R be a real closed field and A a finitely generated R-algebra and let $R_1 \supset R$ be a real closed extension of R. Then if there exists a homomorphism $\varphi : A \to R_1$ of rings, then there also exists a homomorphism $\psi : A \to R$.*

Proof. Write $A = \frac{R[X_1,\ldots,X_n]}{I}$, with $I = (P_1, \ldots, P_s)$. Let $b_i = \varphi(\overline{X_i}) \in R_1$. Then the sentence

$$\Phi : (\exists T_1) \ldots (\exists T_n) \left(\bigwedge_{j=1}^{s} P_j(T_1, \ldots, T_n) = 0 \right)$$

is satisfied by $T_i = b_i$ in R_1. By Tarski-Seidenberg, Φ is already satisfied in R. Hence, $\exists c_i \in R$, $1 \leq i \leq n$, such that $P_1(c_1, \ldots, c_n) = \cdots = P_s(c_1, \ldots, c_n) = 0$. Just define ψ by $\psi(\overline{X_i}) = c_i$.

□

Theorem 28. *Suppose A is a commutative ring and $P \subset A$ a cone, and let $I \subset A$ be an ideal. Then define (the P-radical of I to be) $\sqrt[P]{I} = \{a \in A |\ a^{2m} + p \in I$ for some $m > 0$ and $p \in P\}$ which is the smallest P-radical ideal containing I and $\sqrt[P]{I}$ is the intersection of all P-convex prime ideals containing I.*

Recall: A prime cone $P \subseteq A$ is a proper cone satisfying the property that $ab \in P$ implies $a \in P$ or $-b \in P$. We saw that if P is a prime cone, then $P \cup -P = A$ and $supp(P) = P \cap -P$ is a prime ideal. We will denote by $K(supp(P))$ to be the field of fractions of the domain $\frac{A}{supp(P)}$.

Example 18. If $(F, \leq)$ is an ordered field and P is the positive cone of the ordering, then P is a prime cone.

Example 19. If $\varphi : A \to F$ is a ring homomorphism where F is an ordered field and P is the positive cone of F, then $\varphi^{-1}(P)$ is a prime cone of A. We'll show later that every prime cone P of A is a pull back of the positive cone of $K(supp(P))$.

Example 20. Let R be a real closed field and let $A = R[X]$. Let's look at some cones of A. For example, the sums of squares form a cone of A. We have seen in this number of variables that $\sum A^2$ consists exactly of the non-negative polynomials, and is a proper cone. However, this cone $\sum A^2$ is NOT a prime cone since $(\sum A^2) \cup -(\sum A^2) \neq A$. In particular, any polynomial which takes both positive and negative values is neither in $\sum A^2$ nor $-\sum A^2$.

Let $P = \{f \in A |\ f(0) \geq 0\} \subseteq A$. Note that P is a proper cone, and furthermore it is prime. Note that $supp(P) = P \cap -P = \{f \in A |\ f(0) = 0\}$, and so this is the maximal ideal (X). Note that (X) is $\sum A^2$-convex. There is something special going on here which we will investigate soon.

Let $Q = \{f \in A |\ \exists \varepsilon > 0 \text{ s.t. } f(x) \geq 0 \text{ for all } x \in [0, \varepsilon]\}$. It can be seen that Q is a prime, proper cone of A. The support $supp(Q) = (0)$ is the zero ideal.

Theorem 29. *Let $P \subseteq A$ be a prime cone and let $\phi : A \to K(supp(P))$ the canonical homomorphism. Then there exists an ordering of $K(supp(P))$ such that P is the pre-image of the positive cone.*

Proof. We need to find $\bar{P} \subseteq K(supp(P))$ which is the positive cone of an ordering of $K(supp(P))$ with the desired properties. Define $\bar{P}$ to be the elements of $K(supp(P))$ having a representation $\frac{\bar{b}}{\bar{c}}$ where $b, c \in A$, bar denotes the image under ϕ the canonical homomorphism, and $bc \in P$. We leave it as an exercise that $\bar{P}$ defined this way is (1) a proper cone and that (2) $\varphi^{-1}(\bar{P}) = P$ as desired.

□

We have important types of cones in a commutative ring. The important relationship to remember is detailed in the following theorem.

Theorem 30. *Let A be a commutative ring. The following are equivalent:*

1. *A has a proper cone.*
2. *A has a prime cone.*
3. *There exists a homomorphism $\phi : A \to R$ where R is a real closed field.*
4. *A has a real prime ideal.*
5. *$-1 \notin \sum A^2$*

Proof. The implications have been put in the order which makes them obvious to see. Only (1) $\implies$ (2) takes any proof, but just use Zorn's lemma on the family of proper cones of A containing P. The maximal cone Q with this property can be shown to be prime. Seeking a contradiction, suppose that $ab \in Q$, $a \notin Q$, $-b \notin Q$. We observe that $Q[a], Q[-b]$ are both cones containing A, so they must not be proper by the maximality of Q. Write $-1 = p_1 + q_1 a = p_2 - q_2 b$ where $p_1, p_2, q_1, q_2 \in Q$. From these equations we observe that

$$\begin{aligned} 1 + p_1 &= -q_1 a \\ 1 + p_2 &= q_2 b \\ 1 + p_1 + p_2 + p_1 p_2 &= -q_1 q_2 ab \\ -1 &= p_1 + p_2 + p_1 p_2 + q_1 q_2 ab \in Q, \qquad \lightning \end{aligned}$$

□

Theorem 31. *Let $P \subset A$ be a cone and I a P-convex prime ideal. Then there exists a prime cone Q containing P such that $I = supp(Q)$.*

Before proving the Theorem, we state and prove a useful Corollary. Note that by the assumptions above we have that P is a proper cone.

Corollary 32. *Let $P \subset A$ be a prime cone. Then the correspondence $Q \leftrightarrow supp(Q)$ is a bijection between prime cones of A containing P and P-convex prime ideals of A.*

Proof. We only need to show the correspondence is injective since the correspondence is surjective by the result of the Theorem. To see the correspondence is injective we show that $supp(Q)$ determines Q. In fact, we claim that $Q = P \cup supp(Q)$. If this is true, then of course $supp(Q_1) = supp(Q_2) \implies Q_1 = Q_2$. Let $x \in Q$ and $x \notin supp(Q)$. Then $x \notin -Q$, so $-x \notin Q \supset P$ and hence $-x \notin P$. The cone P is prime, so $-x \in -P$ and hence $x \in P$. The other inclusion holds since $Q \supset P$ and $Q \supset supp(Q)$.

□

We now prove the Theorem.

Proof of Theorem. Let Q be a maximal proper cone containing P such that I is Q-convex. We claim that Q is a prime cone and $I = Q \cap -Q$. We first show that $I = Q \cap -Q$. Let $a \in supp(Q) = Q \cap -Q$, then $a - a = 0 \in I$ and $a, -a \in Q$ implies $a \in I$. The harder direction is to show $I \subseteq Q \cap -Q$.

The property of being Q-convex and I prime means that I is Q-radical (since I prime implies I radical). Let $a \in I$ and we want to show that $a \in Q$. Suppose not, then $Q[a]$ is larger than Q and thus I is NOT $Q[a]$-convex (or $Q[a]$-radical). Therefore, there exists $b \notin I$ with $b^2 + p + qa \in I$, and thus $b^2 + b \in I$, and finally $b \in I$ since I is Q-radical $\lightning$. Therefore, $a \in Q$. A similar argument shows $-a \in Q$ and thus $I = Q \cap -Q$.

The rest of the proof, namely, the proof that the maximal Q proper cone is in fact a prime cone.

□

10 February 11, Day 10

We now finish the proof from last time.

Theorem 31. *Let $P \subset A$ a cone and I a prime P-convex ideal. Then there exists Q a prime cone containing P and such that $I = supp(Q)$.*

Proof. We chose Q to be a maximal cone with the property that it is proper, it contains P, and I is Q-convex. We showed that $I = Q \cap -Q$. It only remains to show that Q is prime. Suppose $ab \in Q$ and $a \notin Q$. Since $Q[a]$ is strictly larger than Q, I is not $Q[a]$-convex and hence not $Q[a]$-radical. Therefore, there exists $c \in A,\ c \notin I$ but $c^2 + p + qa \in I$ for some $p, q \in Q$. Suppose $-b \notin Q$. Then, similarly I is not $Q[-b]$-radical such that there exists $c' \notin I$ and $c'^2 + p' - q'b \in I$ for some $p'q' \in Q$. Consider the sum

$$\begin{aligned} d &= (c^2 + p + qa)(c'^2 + p' + q'b) + (c^2 + p - qa)(c'^2 + p' - q'b) \\ &= 2c^2c'^2 + 2c^2p' + 2c'^2p + 2pp' + 2qq'ab. \end{aligned}$$

Note $d \in I$ and all the terms of d are in Q, and since I is Q-convex we have $c^2c'^2 \in I$. But I is prime (and hence radical), this implies that $c \in I$ $\lightning$

□

Theorem 33. *[Abstract Positivstellensatz] Let A be any commutative ring and $(a_j)_{j\in J}$, $(b_k)_{k\in K}$, $(c_\ell)_{\ell\in L}$ are finite families of elements of A. Let $P = \sum A^2[(a_j)_{j\in J}]$, M the multiplicative monoid generated by $(b_k)_{k\in K}$, and $I = (c_\ell |\ \ell \in L)$ the ideal generated by $(c_\ell)_{\ell\in L}$. Then the following are equivalent.*

1. *There is no prime cone $Q \subset A$ having the property that $a_j \in Q$, $b_k \notin supp(Q)$, $c_\ell \in supp(Q)$ for all $j \in J,\ k \in K, \ell \in L$.*

2. *There is no ring homomorphism $\varphi : A \to R$, with R real closed such that $\varphi(a_j) \geq 0$, $\varphi(b_k) \neq 0$, $\varphi(c_\ell) = 0$ for all $j \in J,\ k \in K, \ell \in L$.*

3. *There exists $p \in P$, $m \in M$, and $i \in I$ such that $p + m^2 + i = 0$.*

Proof. We have already seen, in some detail, that (1) $\iff$ (2): this just combines the results from some of the previous Theorems in this context. The easy direction amounts to proving Theorem 26 and is that (3) $\implies$ (2). Suppose $\varphi : A \to R$ is a homomorphism such that $\varphi(a_j) \geq 0$, $\varphi(b_k) \neq 0$ and $\varphi(c_\ell) = 0$ as in the statement of the Theorem. Then $0 = \varphi(p + m^2 + i) = \varphi(p) + (\varphi(m))^2 + \varphi(i) > 0$ is a contradiction. Now, we prove the existence of a certificate, (2) $\implies$ (3).

Let $A_1 = \frac{A}{I}$, $A_2 = \overline{M}^{-1}A_1$, $A_3 = \frac{A_2[(T_j)_{j\in K}]}{(T_j^2 - a_j \mid j\in J)}$. These objects do the job of making anything in I to be zero, anything in M to be invertible (non-zero), and anything in P to be positive. If there was a ring homomorphism out of A_3 into a real closed field, then this would give a ring homomorphism out of A, since there are natural maps $A \to A_1 \to A_2 \to A_3$. By the assumption that there is no ring homomorphism $\varphi : A \to R$ with the above properties, there can be no ring homomorphism $\widetilde{\varphi} : A_3 \to R$ with R real closed: if such $\widetilde{\varphi} : A_3 \to R$ existed, then the induced $\varphi : A \to A_3 \to R$ which is just composition by natural maps would have the properties $\varphi(c_\ell) = 0$, $\varphi(b_k) \neq 0$, and $\varphi(a_j)$ are squares and hence $\varphi(a_j) \geq 0$. The only technicality here is to check that for $a \in A$ that we can define $\varphi(a) = \widetilde{\varphi}\left(\frac{\overline{a}}{\overline{1}}\right)$ and that this is a well defined mapping. Now, using Theorem **??**, $-1 \in \sum A_3^2$.

We must now unravel what it means $-1 \in \sum A_3^2$ to obtain the certificate. We first examine more closely the elements of A_3. We see that every element in A_3 has a unique representation as a sum of terms with exponents at most one. In symbols, let

$$-1 = \delta_1^2 + \cdots + \delta_N^2,\ \delta_i \in A_3$$

and write

$$\delta_i = \sum_{J' \subset J} \frac{\bar{\gamma}_{J',i}}{\bar{\beta}_{J',i}} \overline{T}^{J'},$$

where the notation $T^{J'} = \prod_{j\in J'} T_j$ and $\bar{\gamma}_{J',i} \in A_1$ and $\bar{\beta}_{J',i} \in \overline{M}$. Now, in the expression for -1, when we square δ_i^2 we can again replace any occurrence T_j^2 by a_j. We have

$$-1 = \sum_i \delta_i^2 = \sum_i \sum_{J'\subset J} \left(\frac{\bar{\gamma}_{J',i}^2}{\bar{\beta}_{J',i}^2} \cdot \prod_{J'\in J} \overline{a_j} \right), \tag{2}$$

since any cross terms which still had a T_j (after substitution $T_j^2 = a_j$) must have a coefficient of zero. Note that $\prod_{j\in J'} a_j \in P$ and hence the numerator of the last expression 2 is in P (without bars).

Now, take $m_0 = \prod_{J',i} \beta_{J',i} \in M$ and by clearing denominators in Equation 2 we obtain the identity $\overline{m_0}^2 + \overline{p_0} = 0$ in A_2 where $p_0 \in P$. Hence, in A_1 we have $\overline{m_1}^2(\overline{m_0}^2 + \overline{p_0}) = 0$ for some $m_1 \in M$, and hence we have that that $m_1^2(m_0^2 + p_0) \in I$ in A. Set $m = m_1^2 m_0 \in M$ and $p = m_1^2 p_0 \in P$, and since $m + p \in I$ we have that $i := -(m + p) \in I$, and we have found the certificate $m^2 + p + i = 0$.

□

Corollary 34. *Let $V \subset R^n$ be a real variety and let $g_1, \ldots, g_s \in \frac{R[X_1,\ldots,X_n]}{I(V)}$ and let $W = \{x \in V \mid g_1(x) \geq 0, \ldots, g_s(x) \geq 0\}$. Then,*

(i) *$\forall x \in W$, $f(x) \geq 0$ if and only if $\exists m > 0$, $g, h \in P[g_1, \ldots, g_s]$ such that $fg = f^{2m} + h$,*

(ii) *$\forall x \in W$, $f(x) > 0$ if and only if $\exists g, h \in P[g_1, \ldots, g_s]$ such that $fg = 1 + h$, and*

(iii) *$\forall x \in W$, $f(x) = 0$ if and only if $\exists m > 0$, $h \in P[g_1, \ldots, g_s]$ such that $f^{2m} + h = 0$.*

Proof. We show (i) writing $I = (u_1, \ldots, u_r)$ and by applying the Positivstellensatz to

$$\underbrace{g_1 \geq 0, \ldots, g_s \geq 0, -f \geq 0}_{a_j\text{'s}}, \quad \underbrace{f \neq 0}_{b_k\text{'s}}, \quad \underbrace{u_1 = \cdots = u_r = 0}_{c_\ell\text{'s}}.$$

For (ii), use

$$\underbrace{g_1 \geq 0, \ldots, g_s \geq 0, -f \geq 0}_{a_j\text{'s}}, \quad \underbrace{u_1 = \cdots = u_r = 0}_{a_j\text{'s}}.$$

We leave (iii) for an exercise.

□

11 February 23, Day 11

Homework #1 DUE today. The next assignment, Homework #2, is due in ONE WEEK.

For today, we'll start with a few words on the Positivstellensatz. For the version that we've proved, we just proved for R a real closed fields. We did not assume $R = \mathbb{R}$. There are other types of certificates which only work over an archimedean field.

WARNING! The natural number N in the next statement depends on the coefficients of the polynomial, and hence the theorem holds only over archimedean real closed fields. For example, the real closure $(R(\varepsilon), \leq)$ where $0 < \varepsilon < a$ for all $a \in R$ is non-archimedean since no natural number is larger than the element $\frac{1}{\varepsilon}$.

Theorem 35. *Let $F \in \mathbb{R}[X_1, \ldots, X_n]$ be a homogeneous polynomial, then $F > 0$ on $\mathbb{R}^n_+$ if and only if there exists a natural number $N > 0$ such that $(X_1 + X_2 + \cdots + X_n)^N \cdot F$ has only positive coefficients.*

Proof. One direction is obvious. The other direction will be an exercise in an upcoming assignment.

□

The next statement is a corollary of the Positivstellensatz.

Corollary 36. *Suppose $S \subset R^n$ is a semi-algebraic set defined by $g_1, \ldots, g_s \geq 0$ and $f > 0$ on S. Then there exists $g, h \in P[g_1, \ldots, g_s]$ such that $fg = 1 + h$.*

This is another example of a certificate. However, the proof of the corollary above is *non-constructive*. In particular, there exist bounds on the degrees of h, g (although in the above statement there is no such reference), but even with this information is it generally very hard to actually find the expressions of h, g in terms of sums and products of the polynomials $g_1, \ldots, g_s$.

This problem is addressed in the next theorem, but first we need a definition which is a relaxation on the definition of *cone*.

Definition 11.1 (Quadratic module)**.** A subset $Q \subset A$ is called a quadratic module if

1. $1 \in Q$
2. $Q + Q \subset Q$
3. $(\sum A^2)Q \subset Q$

and is called proper if in addition

4. $-1 \notin Q$.

Definition 11.2 (Quadratic module generated by $G = \{g_1, \ldots, g_s\}$)**.** The quadratic module generated by $G = \{g_1, \ldots, g_s\}$ is defined to be

$$Q(G) := \{q_0 + q_1 g_1 + \cdots + q_s g_s |\ q_0, q_1, \ldots, q_s \in \sum A^2\}.$$

Compare this to the definition of *cone generated* by G as $P(G) = \{\sum_\alpha q_\alpha g_1^{\alpha_1} \cdots g_s^{\alpha_s}$, and we're ready to state the better version of the corollary.

Theorem 37. *[Putinar Positivstellensatz] Let $G = \{g_1, \ldots, g_s\} \subset \mathbb{R}[X_1, \ldots, X_n]$ and let $K_G = \{x \in \mathbb{R}^n |\ g_1(x) \geq 0, \ldots, g_s(x) \geq 0\}$. Suppose $Q(G)$ satisfies $(*)$, then for all $f \in \mathbb{R}[X_1, \ldots, X_n]$, $f > 0$ on K_G implies $f \in Q(G)$. In the above statement, property $(*)$ is given by*

$$\exists u \in Q(G) \quad s.t. \quad \{x \in \mathbb{R}^n |\ u(x) \geq 0\} \quad \text{is compact.} \tag{$*$}$$

Suppose K_G is contained in a ball of radius R, then set $G' = G \cup \{R^2 - X_1^2 - \cdots - X_n^2\}$ and note that $K_{G'} = K_{G \cup \{R^2 - X_1^2 - \cdots - X_n^2\}} = K_G$ and $Q(G')$ satisfies the property $(*)$.

Definition 11.3. A quadratic module $Q \subset A$ is called archimedean if for each $a \in A$ there exists a natural number n such that $n \pm a \in Q$. *We always assume rings to contain the integers, i.e., all rings are characteristic zero.*

Example 21. Let $K \subset \mathbb{R}^N$ and $A = \mathbb{R}[X_1, \ldots, X_n]$. Then $Q = \{f \in A |\ f(x) \geq 0\ \forall x \in K\}$ is a proper quadratic module. In fact, Q is archimedean. Given $f \in A$, let $a = \max_{x \in K} |f(x)|$ which exists because K was assumed to be compact. Choose $m \in \mathbb{N}$ with $m > a$ (which exists because $\mathbb{R}$ is archimedean), then $m \pm f \in Q$.

Proposition 38. *Let $A = \mathbb{R}[X_1, \ldots, X_n]$ and $G = \{g_1, \ldots, g_s\} \subset A$, then the property $(*)$ holds for $Q(G)$ if and only if $Q(G)$ is archimedean.*

Proof. One direction is easy. Assume $Q(G)$ is archimedian and let $f = X_1^2 + \cdots + X_n^2 \in A$ and hence $\exists m \in \mathbb{N}$ such that $m - f \in Q(G)$. Therefore, $m - f \in Q(G)$ implies that f verifies property $(*)$ for $Q(G)$.

For the other direction, assume that $Q(G)$ satisfies property $(*)$ and we need to show (EXERCISE) that $Q(G)$ is archimedean.

□

The following lemmas have analogous results when we were discussing cones. The proofs are left as exercises.

Lemma 6. *If Q is a quadratic module, then $I = Q \cap -Q$ is an ideal.*

Lemma 7. *If Q is a maximal proper quadratic module, then $Q \cup -Q = A$.*

Proof. Suppose $f \notin Q \cup -Q$. Then both $Q[f]$ and $Q[-f]$ are not proper. So $-1 \in Q + f\sum A^2, -1 \in Q - f\sum A^2$ are not proper. Write

$$-1 = q_1 + f s_1 \tag{$\dagger$}$$

and $-1 = q_2 - f s_2$ where $s_1, s_2 \in \sum A^2$ are sums of squares. Then $-s_2 - s_1 = q_1 s_2 + q_2 s_1 \in Q$ and hence $(s_1 + s_2) \in Q \cap -Q = I$. We want to see that $-s_1 \in I$, but $-s_1 = -(s_1 + s_2) + s_2 \in Q$ so $-s_1 \in I$. So $s_1 \in I \implies f s_1 \in I \implies f s_1 \in Q$. But then by the above equation $(\dagger)$ we have $-1 \in Q$ ↯.

□

Lemma 8. *Suppose $Q \subset A = \mathbb{R}[X_1, \ldots, X_n]$ is a proper maximal quadratic module which is archimedean. Then, for each f there exists a unique $a \in \mathbb{R}$ such that $f - a \in I$.*

Proof. Let $A = \{a \in \mathbb{R} |\ f - a \in Q\}$, $B = \{a \in \mathbb{R} |\ b - f \in Q\}$. The sets A, B are non-empty by the archimedean property of Q. Let $a_0 = \sup A$ and $b_0 = \inf B$, and we want to see that $a_0 \leq b_0$. In an easy first step, if $a \in A$ and $b \in B$ then $f - a, b - f \in Q$ and hence $b - a \in Q$, and if Q is proper this means that $b - a \geq 0$. We now claim that $a_0 = b_0$. If $a_0 < c < b_0$ then $f - c, c - f \notin Q$, which is a contradiction with the fact that $Q \cup -Q = A$ since Q was maximal and proper (using the previous Lemma). So, $a_0 = b_0$ and we're done if we can show $a_0 \in A$. Suppose, seeking a contradiction, that $a_0 \notin A$, so $f - a_0 \notin Q$. Then, $Q[f - a_0]$ is not proper and we can write $-1 = q + (f - a_0)s$, where $s \in \sum A^2$. Using the archimedean property of Q on $s \in A$, we have that there exists an N such that $N - S \in Q$. Based on a_0 being the supremum of A, there exists $0 < \varepsilon < \frac{1}{N}$ such that $f - (a_0 - \varepsilon) \in Q$. Now, $\varepsilon(N - s) \in Q$ and we have $-1 + \varepsilon s = q + (f - (a_0 - \varepsilon))s \in Q$ and adding this equation to the equation $\varepsilon(N - s) \in Q$ we get $\varepsilon N - 1 \in Q$, but $\varepsilon N - 1 < 0$ which contradicts the fact that Q is proper.

□

Example 22. Let $Q = \{f \in A |\ f(0) \geq 0\}$. Then $I = Q \cap -Q = \{f \in A |\ f(0) = 0\}$, and if $f \in A$ then $f - f(0) \in I$, so set $a = f(0)$.

12 February 25, Day 12

We need to add an assumption to the first problem of the second assignment. Add that $P \cap -P = \{0\}$ for the cone P in the statement, which amounts to assuming that $a \geq 0$ and $-a \geq 0$ implies $a = 0$.

We now continue with today's lecture. We begin by recalling the Lemma we had just proven.

Lemma 8. *if $Q \subset A = \mathbb{R}[X_1, \ldots, X_n]$ is a maximal, proper quadratic module which is also archimedean. Then, for every $f \in A$ there exists $a \in \mathbb{R}$ such that $f - a \in Q \cap -Q$.*

Now, consider the following sets.

$$\begin{aligned} G &= \{g_1, \ldots, g_x\} \subset \mathbb{R}[X_1, \ldots, X_k] \\ K_G &= \{x \in \mathbb{R}^n |\ g_1(x) \geq 0, \ldots, g_s(x) \geq 0\} \\ Q(G) &= \{p_0 + p_1 g_1 + \cdots + p_s g_s |\ p_i \in \sum A^2\} \qquad \text{(archimedean)} \\ \text{WTS:} \quad & f > 0 \text{ on } K_G \quad \Longrightarrow \quad f \in Q(G) \end{aligned}$$

Our goal for today is to show that $f > 0$ on K_G implies that $f \in Q(G)$. The first step towards this goal is to prove the following proposition.

Proposition 39. *There exists $p \in \sum A^2$ such that $pf \in 1 + Q(G)$.*

Proof. Consider the quadratic module $Q_1 = Q(G) - f \sum A^2$. First note that $Q_1 \supset Q(G)$, and also Q_1 is archimedean since $Q(G)$ is archimedean. We are done if we can show that $-1 \in Q_1$ since in that case $\exists p \in \sum A^2$ such that $pf = 1 + Q(G)$. We aim to show that Q_1 is not proper.

Assume, for the sake of seeking a contradiction, that Q_1 is a proper quadratic module and hence $-1 \notin Q_1$. By Zorn's lemma, we can choose a quadratic module $Q_0 \supset Q_1$ which is maximal with respect to the property of being a proper quadratic module containing $Q(G)$. Hence, Q_0 is a maximal, proper, archimedean module and by Lemma 8 we have $Q_0 \cup -Q_0 = A$. By the previous lemma for each X_i there exists a unique a_i such that $X_i - a_i \in I = Q_0 \cap -Q_0$. Let $a = (a_1, \ldots, a_k)$, then for every $f \in A$ we have $f - f(a) \in I$. We claim that $a \in K_G$, which is verified by checking that $g_i(a) \geq 0$ for all $1 \leq i \leq s$. Write

$$g_i(a) = \underbrace{-(g_i - g_i(a))}_{\in Q_0} + g_i,$$

and since $g_i \in Q(G) \subset Q_0$ we have that $g_i(a) \in Q_0$. Since Q_0 is proper, this means that $g_i(a) \geq 0$.

Now we want to get a contradiction with $f > 0$ by showing that $f(a) \leq 0$. We proceed in a similar fashion as above and write

$$-f(a) = \underbrace{(f - f(a))}_{\in Q_0} - f,$$

and $-f \in Q_1 \subset Q_0$ by definition of Q_1, and so again we have $-f(a) \in Q_0$ which was assumed to be proper, which gives $-f(a) \geq 0$ and implies $f(a) \leq 0$ which is a contradiction $\lightning$.

□

The last step in proving the Theorem 37 (Putinar Positivstellensatz) is the following proposition.

Proposition 40. *There exists $h \in Q(G)$ and $N \in \mathbb{N}$ such that $N - h \in \sum A^2$ and $hf \in 1 + Q(G)$.*

Before we prove the proposition, we use the above proposition to prove the Theorem 37.

Proof of Theorem 37. By the archimedean property of $Q(G)$, we can choose $k \in \mathbb{N}$ such that $k + f \in Q(G)$. By the Proposition 40, we have $h \in Q(G)$, $N \in \mathbb{N}$ such that $N - h \in \sum A^2$ and $hf - 1 \in Q(G)$. We we aim to show that $(k - \frac{1}{N}) + f \in Q(G)$ and then inductively we can show that $f \in Q(G)$. We have that

$$(k - \frac{1}{N}) + f = \frac{1}{N}(\underbrace{(N - h)}_{\in \sum A^2}\underbrace{(k + f)}_{\in Q(G)} + \underbrace{(hf - 1)}_{\in Q(G)} + \underbrace{kh}_{Q(G)}) \in Q(G).$$

We can repeat the same argument $k \cdot N$ times we obtain $f \in Q(G)$. In particular, if we let $k' = k - \frac{1}{N}$ then we can similarly show that $(k' - \frac{1}{N}) + f \in Q(G)$, and after kN steps we obtain $f \in Q(G)$ as desired.

□

We now prove the last component to the proof of the Putinar Positivstellensatz, the Proposition 40.

Proof of Proposition 40. Again, using the archimedean property of $Q(G)$, choose $k \in \mathbb{N}$ such that $2k - p, 2k - p^2 f - 1 \in Q(G)$. Set $h = p(2k - p)$, and see that

$$hf - 1 = p(2k - p)f - 1 = 2k(pf - 1) + \underbrace{(2k - p^2 f - 1)}_{\in Q(G)}$$

by choice of k and $pf - 1 \in Q(G)$ by the previous Proposition, and hence $hf - 1 \in Q(G)$. Set $N = k^2$ and we have that $N - h = k^2 - p(2k - p) = (k - p)^2 \in \sum A^2$. So we have found a N and h such that $N - h$ is a square and $hf = 1 + q$ for some $q \in Q(G)$.

□

We are done talking about the Positivestellensatz. We are ready to begin the next section, where we will be looking more closely at semi-algebraic sets.

12.1 Semi-algebraic sets

We have seen from the definition that the class of semi-algebraic sets $\{S |\ S \subset R^k,\ R \text{ real closed field}\}$ for a given, arbitrary real closed field is closed under finite set operations (union, intersection, complement), and by the Tarski-Siedenberg quantifier elimination theorem we also know that this class is closed under taking projections. We now examine which type of topological properties this class possess.

Definition 12.1 (Open semi-algebraic sets)**.** Say that a semi-algebraic set $S \subset R^k$ is *open* if the following formula holds (written in shorthand notation):

$$(\forall x \in S)(\exists r > 0)(\forall y)(|x - y|^2 < r \implies y \in S).$$

Similar definitions for closure, interior, boundary, etc. show that the class of semi-algebraic sets are closed under these operations. What should it mean for a semi-algebraic set to be connected?

Example 23. Consider $R = \mathbb{Q}_{alg}$. Note that $[0,1] = [0, \frac{1}{\pi}) \cup (\frac{1}{\pi}, 1]$ and that each of the sets on the right hand side are open subsets of R but that they are NOT semi-algebraic. So, we need to be careful to decide how to define the notion of *connectedness* of semi-algebraic sets.

Definition 12.2 (Connected semi-algebraic sets)**.** A non-empty semi-algebraic set $S \subset R^k$ is said to be *semi-algebraically connected* if it can not be expressed as a disjoint union of two non-empty open semi-algebraic subsets of S.

Definition 12.3 (Semi-algebraic map)**.** A map $f : S \to T$ is said to be *semi-algebraic* provided S, T are semi-algebraic sets and the graph $\gamma(f) \subset S \times T$ defined by $\gamma(f) = \{(a, f(a)|\ a \in S\}$ is a semi-algebraic subset of $S \times T$.

Definition 12.4 (Semi-algebraic path)**.** A *semi-algebraic path* is a semi-algebraic map $\gamma : [0,1] \to S$ which is continuous, where the definition of continuity is the usual one: the map $f : S \to T$ is continuous at x_0 if

$$(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x)((x - x_0)^2 < \delta \implies (f(x) - f(x_0))^2 < \varepsilon).$$

Definition 12.5 (Path-connected semi-algebraic sets)**.** A non-empty semi-algebraic set is said to be *semi-algebraically path connected* if for every $x, y \in S$ there exists a semi-algebraic path $\gamma : [0,1] \to S$ such that $\gamma(0) = x$ and $\gamma(1) = y$.

It turns out that for $R = \mathbb{R}$, the notion of being connected is the same as being semi-algebraically connected, and additionally for any real closed field R we will eventually show that the notions of connectivity and path-connectivity are equivalent, and hence for the special case $R = \mathbb{R}$ all three notions are the same.

Definition 12.6 (Germ of a semi-algebraic function)**.** Consider the germs of semi-algebraic functions on $(0, \infty)$. A *germ* is an equivalence class of functions where $f_1 \sim f_2$ if $f_1|_{(0,t_0)} = f_2|_{(0,t_0)}$ for some $t_0 > 0$.

We will show that the germs of semi-algebraic functions to the right of the origin form a real closed field, and that this field is isomorphic to the field of algebraic Puiseiux series in ε with coefficients in R, and is also isomorphic to the real closure of $R(\varepsilon)$.

13 March 2, Day 13

We need to slightly fix the last problem #5 of Assignment #2: Show that $K = \{x|\ Ax \leq b\}$ is empty if and only if $\exists u \in \mathbb{R}^m_+$ such that $u^t A = 0$ and $u^t \cdot b < 0$.

Solution: Sketch. If $x \in K$ and $Ax \leq b$, then $0 = u^t Ax \leq u^t b < 0$. □

Unfortunately, the general Positivestellensatz does not provide such a simple certificate. However, we can view the Positivstellensatz as a generalization of this type of certificate (of checking the empty-ness of a certain type of semi-algebraic set).

13.1 Semi-algebraic sets, Extension

Let $R \subset R'$ be two real closed fields. Suppose that $S \subset R^k$ is semi-algebraic and, hence, defined by some formula $\phi(X)$ where ϕ is some first order formula over R with free variables $X = (X_1, \ldots, X_k)$. Such a formula will also define a semi-algebraic set over R', since the coefficients of ϕ are in R' as well. We denote this semi-algebraic set (in the larger space) by $\mathrm{Ext}(S, R')$. It is not hard to see, using the T-S transfer principle.

Proposition 41. *The set $Ext(S, R')$ is well defined as it does not depend on the formula ϕ which defines S.*

Proof. Let ϕ' be another formula with coefficients in R such that $\mathcal{R}(\phi, R^k) = S = \mathcal{R}(\phi', R^k) := \{x \in \mathbb{R}^k | \ \phi'(x)\}$. Then consider the quantified first order formula

$$(\forall x)(\phi(x) \iff \phi'(x))$$

which is satisfied over R and hence over R' using the Tarski-Siedenberg transfer principle 18.

□

Let $f : X \to Y$ be a semi-algebraic function (the graph of f is a semi-algebraic set) where $X \subset R^m$, $Y \subset R^n$ are semi-algebraic subsets and consider the map

$$\text{Ext}(f, R') : \text{Ext}(x, R') \to \text{Ext}(y, R')$$

which is a semi algebraic map whose graph is just

$$graph(\text{Ext}(f, R')) = \text{Ext}(graph(f), R').$$

We have some elementary, useful sets to define: open and closed balls, spheres, etc.. We define the ball (resp. closed ball, sphere) centered at $x \in R^k$ with radius r to be

$$\begin{aligned} B_k(x, r) &= \{(y_1, \ldots, y_k) \in \mathbb{R}^k | \ \sum (x_i - y_i)^2 < r^2\} \\ \overline{B}_k(x, r) &= \{(y_1, \ldots, y_k) \in \mathbb{R}^k | \ \sum (x_i - y_i)^2 \leq r^2\} \\ S^{k-1}(x, r) &= \{(y_1, \ldots, y_k) \in \mathbb{R}^k | \ \sum (x_i - y_i)^2 = r^2\}. \end{aligned}$$

Example 24. Let us now consider $R\langle\varepsilon\rangle$ the real closure of $R(\varepsilon)$. Let $P \in R[X_1, \ldots, X_k]$ and let $S = \{x \in R^k | \ P(x) > 0\}$. Then, S is an open semi-algebraic set (CLAIM).

Proof. Let $x \in S$. We need to find $r > 0$ such that $B_k(x, r) \subset S$. The way we will proceed is to consider the non-archimedean extension $R' = R\langle\varepsilon\rangle$. NOTE: we use the same notation to indicate the ball $B_k \subset R^k$ as well as $B_k \subset R'^k$ (we DROP the notation $\text{Ext}(\cdot, \cdot)$ for commonly used elementary semi-algebraic sets). We claim that $B_k(x, \varepsilon) \subset \text{Ext}(S, R')$.

Let $x \in S$, then $P(x) = a > 0$ for some $a \in R$. Now if $y \in B_k(x, \varepsilon)$ then $|y_i| < |x_i| + \varepsilon$, so the coordinates of y are bounded, $y_i \in R\langle\varepsilon\rangle_b$, and we have that $P(y) - a$ is infinitesimal since $\lim_\varepsilon (P(y) - a) = P(\lim_\varepsilon y) - a = P(x) - a = 0$. So, in particular, $P(y) > 0$ in R' since $P(y) = (a - P(y)) - a > 0$ and $a - P(y)$ is infinitesimal. Now, consider the first order sentence $\exists r > 0 \ B_k(x, r) \subset S$ which is true over R' since we showed that $B_k(x, \varepsilon) \subset Ext(S, R')$, and hence by Tarski-Seidenberg this sentence is true over R.

In the above paragraph, we used the so-called *valuation map*,

$$\upsilon : R\langle\varepsilon\rangle \to \mathbb{Q}$$
$$\upsilon\left(\sum_{i \geq i_0} a_i \varepsilon^{\frac{i}{q}}\right) = \frac{i_0}{q}$$

the set of *bounded elements*

$$R\langle\varepsilon\rangle_b := \{x \in R\langle\varepsilon\rangle | \ \upsilon(x) \geq 0\},$$

and the map

$$\lim_\varepsilon R\langle\varepsilon\rangle \to R$$
$$\lim_\varepsilon \left(\sum_{i \geq i_0} a_i \varepsilon^{\frac{i}{q}}\right) = a_0.$$

Note, for example, that $\varepsilon^{-1/2} \notin R\langle\varepsilon\rangle_b$ but that $\varepsilon^{1/2} \in R\langle\varepsilon\rangle_b$. Note that $\lim_\varepsilon \varepsilon^{1/2} = 0$ and that $\varepsilon^{1/2}$ is smaller than any positive element of R. We call $x \in R\langle\varepsilon\rangle_b$ to be an *infinitesimal* if $\lim_\varepsilon x = 0$. For example, $1 + \varepsilon^{1/2} \in R\langle\varepsilon\rangle_b$ but it is not infinitesimal. If $x \in R\langle\varepsilon\rangle_b$, then $(x - \lim_\varepsilon x)$ is infinitesimal since $lim_\varepsilon(x - \lim_\varepsilon x) = \lim_\varepsilon x - \lim_\varepsilon x = 0$.

The principle we used in the above example is so crucial to understanding the methods we're going to be using again and again, that we'll state the next proposition in hopes of elucidating the principle that we're using.

Proposition 42. *Let R be real closed and $R' = R\langle\varepsilon\rangle$. Let Φ be a first order sentence with coefficients in $R[\varepsilon]$, and let $\Phi'[T]$ be the formula obtained by Φ by replacing ε by T. Then Φ is true over R' if and only if R' if and only if*

$$\exists t_0 \in R \text{ such that } \Phi'[t] \text{ is true for every } t \in (0, t_0).$$

Proof. Suppose that Φ is true over R'. Let A be the semi-algebraic subset of R defined by $A := \{t \in R |\ t > 0 and I'(t)\}$. If A contains an interval $(0, t_0)$, done. Otherwise, there exists an interval $(0, t_0)$ such that $t \notin A$ for all $t \in (0, t_0)$. But then $\mathrm{Ext}(A, R')$ does not contain the element t_0, by virtue of $\varepsilon \in \mathrm{Ext}(\{t |\ 0 < t < t_0\}, R')$, but then $\Phi = \Phi'[\varepsilon]$ is not true $\lightning$. So, A does contain an interval $(0, t_0)$.

For the converse, suppose you are given that $\Phi'[t]$ is true for all $t \in (0, t_0)$ where $t_0 > 0$ and $t_0 \in R$. We want to see that $\Phi'[\varepsilon] = \Phi$ is a true sentence in R'. Since, $\varepsilon \in \mathrm{Ext}((0, t_0), R')$ we have that $\Phi'[\varepsilon]$ is true.

□

Let $R' = R\langle\varepsilon\rangle$ as before.

Proposition 43. *If f is a semi-algebraic function $f : S \to R$ and $x \in S$, then f is semi-algebraically continuous at x if and only if for every $y \in Ext(S, R')$ such that $\lim_\varepsilon y = x$ then $\lim_\varepsilon f(y) = f(x)$.*

Proof. Suppose that f is continuous at $x \in R$. By the usual definition of continuity, the following first order formula with coefficients in R is true.

$$(\forall a > 0)(\exists b > 0)(|y - x| < b \implies |f(y) - f(x)| < a).$$

Then, let $y \in \mathrm{Ext}(S, R')$ with $y \in R\langle\varepsilon\rangle$ and suppose that $\lim_\varepsilon y = x$. Then, in particular we have the following first order formula which is satisfied by y,

$$(\forall a \in R)(a > 0 \implies |f(y) - f(x)| < a)$$

which implies that $\lim_\varepsilon |f(y) - f(x)| = 0$, and hence $\lim_\varepsilon f(y) = f(x)$.

For the converse, suppose that f is not continuous at $x \in R$. Then the negation of the above formula is true,

$$(\exists a > 0)(\forall b > 0)(\exists y \in S)(|y - x| < b \wedge |f(y) - f(x)| \geq a).$$

This is a sentence in R and hence is also a sentence in R'. Choose $b = \varepsilon$, then $\lim_\varepsilon y = x$ but $\lim_\varepsilon f(y) \neq f(x)$. This finishes the proof of the statement.

□

The next theorem which we want to prove relates the set of germs of continuous semi-algebraic functions to the right of the origin with the elements of $R\langle\varepsilon\rangle$ the real closed field of Puisseux series.

Theorem 44. *The set of germs of continuous semi-algebraic functions to the right of the origin is real closed (and isomorphic to $R\langle\varepsilon\rangle$).*

14 March 4, Day 14

The next assignment, Assignment #3, has been assigned and is DUE after spring break.

Proposition 45. *Let S be a semi-algebraic subset of R^k, and $a_0, \ldots, a_n$ be continuous semi-algebraic functions on S. Let $x \in S$ and $y \in R$ a simple root (*i.e.*, a root of multiplicity one) of the polynomial*

$$a_0(x) + a_1(x)T + \cdots + a_n(x)T^n.$$

Then, there exists an open semi-algebraic neighborhood U of x in S and a continuous semi-algebraic function $f : U \to R$ such that $f(x) = y$ and for all $u \in U$, $f(u)$ is a simple root of the polynomial

$$a_0(u) + a_1(u)T + \cdots + a_n(u)T^n.$$

Example 25. If $S = R$ and $a_0(X) = X^2$, $a_1(X) = 0$ and $a_2(X) = 1$ then the polynomial has a root when $X = 0$ but not on any open neighborhood of $X = 0$ in R.

Proof of Prop. By the mean value theorem, since the root at y is simple there exists $m > 0$ such that for all $0 < m' \leq m$ we have that $P(x, y + m')P(x, y - m') < 0$. Furthermore, we may as well assume that $\frac{\partial P}{\partial Y}(x, Y) > 0$, where $\frac{\partial P}{\partial Y}(x, Y)$ is just the formal derivative

$$\frac{\partial P}{\partial Y}(x, Y) = a_1(x) + \cdots + na_n(x)y^{n-1}.$$

Let us consider the semi-algebraic subset $V = \{(u, s) |\ \frac{\partial P}{\partial Y}(u, s) > 0\}$ which is an open subset of $S \times R$. For every m', $0 < m' \leq m$, we have that $U_{m'} = \{u |\ P(u, y+m')P(u, y-m') < 0$ and $\{u\} \times [y-m', y+m'] \subset V\}$ defines an open semi-algebraic subset of S which contains the element $x \in S$. Hence, $U_{m'}$ is an open semi-algebraic neighborhood of x for each such m'. Now, let $U = U_m$ and note that for every $u \in U$ there is a unique root in R contained in the interval $[y - m, y + m]$, and so we have a well defined function $f : U \to R$ taking u to the unique root in R of $a_0(u) + \ldots, +a_n(u)T^n$, and finally note that $f(x) = y$.

It only remains to show that $f : U \to R$ is continuous, and in particular it suffices to show continuity at x. Continuing to use the method from yesterday, let $\phi \in \mathrm{Ext}(U, R\langle\varepsilon\rangle)$ with $\lim_\varepsilon \phi = x$. We need to show that $\lim_\varepsilon \mathrm{Ext}(f, R\langle\varepsilon\rangle)(\phi) = f(x) = y$, which will prove continuity of f at x. Since ϕ is infinitely close to x, it must be contained in the extension of any open neighborhood of x. That is, for every $m' \in R$ with $0 < m' \leq m$, since $U_{m'}$ is open we must have $\phi \in \mathrm{Ext}(U_{m'}, R\langle\varepsilon\rangle)$. Hence, if we evaluate and compare $|\mathrm{Ext}(f, R\langle\varepsilon\rangle)(\phi) - y| < 2m'$, hence is smaller than every positive element of R. So $\lim_\varepsilon(\mathrm{Ext}(f, R\langle\varepsilon\rangle)(\phi)) - y = 0$ as desired.

□

Next, we formally define the notion of *germs of functions*.

Definition 14.1 (Germs of functions)**.** Let $f, g : (0, t_0) \to R$ be semi-algebraic continuous functions. Say that f is equivalent to g and write $f \sim g$ if and only if there exists t_1, $0 < t_1 \leq t_0$, such that $f|_{(0,t_1)} \equiv g|_{(0,t_1)}$. This is an equivalence relation and the set of equivalence classes of semi-algebraic functions is called the *set of germs of semi-algebraic functions to the right of the origin.* A representative of one of the equivalence classes has the form $f : (0, t_f) \to R$, with $t_f > 0$.

Observations:

1. The set F of equivalence classes is a field and in fact an ordered extension of the ordered field $R(\varepsilon)$ ordered by making $\varepsilon > 0$ an infinitesimal (smaller than any other positive element of R). Of course, $i : R(\varepsilon) \hookrightarrow F$ since elements of $R(\varepsilon)$ which agree on an open interval must be the same element of $R(\varepsilon)$. If $\phi, \psi \in F$ and $f : (0, t_f) \to R$ (resp. $g : (0, t_g) \to R$) represent ϕ (resp. ψ), then $\phi + \psi, \phi \cdot \psi$, and ϕ^{-1} is represented by $f + g, f \cdot g : (0, \min\{t_f, t_g\}) \to R$ and $f^{-1} : (0, t_1) \to R$ where $f \neq 0$ on $(0, t_1)$ (unless f is the zero function).

2. If we can show that F is real closed and an algebraic extension of $R(\varepsilon)$ then, by the first problem of the first Assignment #1, there is a unique R-isomorphism between F and $R\langle\varepsilon\rangle$.

Proposition 46. *The ordered field F satisfies the intermediate value property for polynomials.*

Proof. We need to prove the intermediate value property for arbitrary $P \in F[X]$, but it suffices to prove the property for polynomials with simple roots. If P were not separable, then write $P = Q_1Q_2$ with $Q_1 = gcd(P, P')$, and then $P(a)P(b) < 0$ means that either Q_1 or Q_2 changed signs, so we can reduce to the case that P has only simple roots. We need to prove: if $a, b \in F$ and $a < b$ such that $P \in F[X]$ has only simple roots and satisfies $P(a)P(b) < 0$, then there must exist $c \in (a, b)$ such that $P(c) = 0$. Let $P = \phi_0 + \phi_1 X + \ldots \phi_n X^n$, with $\phi_i \in F$. We might as well assume that a, b, ϕ_i are represented by functions $p, q, f_i : (0, t_0) \to R$ defined on the same interval for $0 \leq i \leq n$. By shrinking the interval $(0, t_0)$, if necessary, we have that there exists $t_1 > 0$ such that for every $t \in (0, t_1)$

$$(f_0(t) + f_1(t)p(t) + f_2(t)p^2(t) + \cdots + f_n(t)p^n(t)) \cdot (f_0(t) + f_1(t)q(t) + f_2(t)q^2(t) + \cdots + f_n(t)q^n(t)) < 0,$$

and so the polynomial $\widetilde{P}_t(X) = f_0(t) + f_1(t)X + \cdots + f_n(t)X^n$ has at least one root in the interval $(p(t), q(t))$.

By the assumption that the polynomial $P \in F[X]$ had only simple roots, the number of roots of $\widetilde{P}_t(X)$ is constant in the interval $(0, t_1)$. If we let $x_1(t), \ldots, x_r(t)$ be the r real roots of $\widetilde{P}_t(X)$ and assume that these are in ascending order, then there exists $1 \leq i_0 \leq r$ such that $p(t) < x_i(t) < q(t)$. Now, the *root functions* $x_i(t)$ can not cross in the interval $(0, t_1)$ since otherwise the number of roots would change, and hence $p(t) < x_i(t) < q(t)$ for all $t \in (0, t_1)$. The equivalence class of $x_i(t)$, which is a continuous, semi-algebraic function defined to the right of the origin, is the root of $P(T)$ that we were trying to find.

We just need to see that the extension is algebraic. Let $\phi \in F$ be represented by $f : (0, t_f) \to R$ a semi-algebraic and continuous function. What does it mean that f is a semi-algebraic function? This means that the graph of f is semi-algebraic. So we can write $graph(f) = \{(x, y) |\ \Phi(x, y)\}$ where

$$\Phi : \begin{array}{c} P_1(x,y) = 0 \wedge Q_{1,i}(x,y) > 0, \ldots \\ \vee \\ P_2(x,y) = 0 \wedge Q_{2,i}(x,y) > 0, \ldots \\ \vee \\ \vdots \\ \vee \\ P_s(x,y) = 0 \wedge Q_{s,i}(x,y) > 0, \ldots \end{array}$$

So if we define $P = P_1 \cdots P_s$, then $graph(f) \subset V(P, R^2)$. In particular, $P(t, f(t)) = 0$ on $(0, t_f)$. Now, $R(\varepsilon) \subset F$, and so $P_0(t) + P_1(t)f(t) + \cdots + P_d(t)(f(t))^d = 0$ on $(0, t_0)$, and so in F we have

$$\phi_0 + \phi_1\phi + \cdots + \phi_d\phi^d = 0,$$

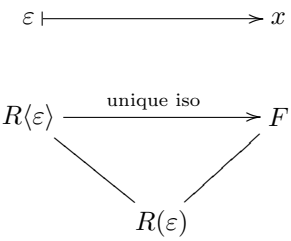
where $\phi, \phi_0, \ldots, \phi_d$ are the germs represented by polynomials $f, P_0, \ldots, P_d$. This shows that the extension is algebraic and finishes the proof.

□

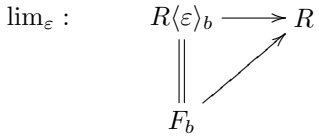
15 March 9, Day 15

From last time, R is a real closed field and F is the set of germs of continuous semi-algebraic functions to the right of the origin, $f : (0, t_0) \to R$. We had just proved the following theorem.

Theorem 47. *The set F is the real closure of the ordered field $R(\varepsilon)$ (which is ordered by making ε infinitesimal with respect to R).*



The subset $R\langle\varepsilon\rangle_b$ of bounded Puisseux series is mapped by this unique isomorphism to the set of germs of bounded semi-algebraic continuous functions $f : (0, t_0) \to R$, which we denote by F_b. The map $\lim_\varepsilon$ then can be thought of as either a map $\lim_\varepsilon : R\langle\varepsilon\rangle_b \to R$ or $\lim_\varepsilon : F_b \to R$ (after composing by the unique isomorphism).



Composition

EXERCISE 2. Suppose that $\varphi \in F$, represented by $f : (0, t_0) \to R$ and let g be a semi-algebraic function which is continuous on the image of f. Then $g \circ f : (0, t_0) \to R$ is a semi-algebraic continuous function. Show that the germs of $g \circ f$ and $g \circ \varphi$ coincide if φ is another representative of the class of f in F.

Proposition 48. *Suppose that $S \subset R^k$ is a semi-algebraic set and let $\varphi \in Ext(S, R\langle\varepsilon\rangle)$. Let φ be represented by $(f_1, \ldots, f_k)$ where each $f_i : (0, t_0) \to R$ is a semi-algebraic continuous function. Then, there exists $t_1 > 0$, $t_1 \in R$ such that $f(t) = (f_1(t), \ldots, f_k(t)) \in S$ for all $t \in (0, t_1)$.*

Proof. Let Φ be a formula with coefficients in R defining S. Let $P \in R[X_1, \ldots, X_k]$. Then $P(\varphi) > 0$ if and only if $P(f_1(t), \ldots, f_k(t)) > 0$ for all $t \in (0, t_1)$. It follows that $\exists t_1$ such that $(f_1(t), \ldots, f_k(t) \in S$ for all $t \in (0, t_1)$.

□

Theorem 49. *Let $f : (0, a) \to R$ be a continuous, bounded semi-algebraic function. Then there exists a continuous extension to a semi-algebraic function $\bar{f} : [0, a) \to R$.*

Remark 50. Note that the theorem fails for continuous functions which aren't semi-algebraic, and that there is no analogous statement for higher dimensions (bigger than one). It is an exercise to show that there is no continuous extension of the function $f(x, y) = \frac{y}{x}$ on the domain $S = \{(x, y) |\ x > y, x^2 + y^2 < 1, y > 0\}$ to the origin $(0, 0)$.

Proof of Theorem. Let $\varphi \in R\langle\varepsilon\rangle$ represent the germ of f. Since f is bounded, $\varphi \in R\langle\varepsilon\rangle_b$. Define $\bar{f}(t) = f(t)$ for $t \in (0, t_0)$ and $\bar{f}(0) = \lim_\varepsilon \varphi =: b$. We just need to check continuity at zero. For each $r > 0$, $r \in R$ the set

$$U_r = \{t \in R |\ |f(t) - b| \leq r\}$$

is a semi-algebraic subset of R, and we're done if we can show that it contains an interval. We claim that $\varepsilon \in \mathrm{Ext}(U_r, R\langle\varepsilon\rangle)$, but $\mathrm{Ext}(f, R\langle\varepsilon\rangle)(\varepsilon) = \varphi$, and hence $|\varphi - \lim_\varepsilon \varphi|$ is infinitesimal and positive, and write $0 < |\varphi - \lim_\varepsilon \varphi| << 1$ which implies $|\varphi - \lim_\varepsilon \varphi| \leq r$. From last time, since $\varepsilon \in \mathrm{Ext}(U_r, R\langle\varepsilon\rangle)$ we have $\exists \delta > 0$, $\delta \in R$ such that $(0, \delta) \subset U_r$, which implies that f is continuous at 0.

□

Notation 2 (Infinitesimal notation). To solidify the notation we just introduced, if ε is an infinitesimal, *i.e.,* it is positive and smaller than every $a \in R$, then use the notation $0 < \varepsilon << 1$. So, the notation $0 < \varepsilon << 1$ is equivalent to $(\forall a)(0 < \varepsilon < a)$ where the universal quantifier is taken over R.

Example 26. Consider $R = \mathbb{R}\langle\varepsilon\rangle$. Then $f : (0,1) \to R$ given by $f = \frac{1}{\varepsilon} - X$. Then this function f is NOT bounded *over* $\mathbb{R}$, but it is bounded over R.

Theorem 51 (Curve selection lemma)**.** *Let $S \subset R^k$ be a semi-algebraic set and $x_0 \in \overline{S}$ in its closure. Then there exists a continuous semi-algebraic path $\gamma : [0,1] \to \overline{S}$ such that $\gamma(0) = x_0$ and $\gamma((0,1]) \subset S$.*

Proof. The idea is to look at the intersection of $B_k(x_0, \varepsilon) \cap \mathrm{Ext}(S, R\langle\varepsilon\rangle) \neq \emptyset$ which is non-empty by the condition that $x_0 \in \overline{S}$. Let φ belong to this intersection, and let $f : (0, t_0) \to R$ be a representative of φ, and write $f = (f_1, \ldots, f_k)$ and recall that we've just seen that there exists $t_1 > 0$, $t_1 \in R$ such that $f(t) \in S$ for each $t \in (0, t_1)$.

We extend f to zero by setting $\bar{f}(0) = \lim_\varepsilon \varphi$, and notice that φ is bounded since $\varphi \in B(x_0, \varepsilon)$ and $x_0 \in R^k$. Similar to the previous theorem, $\lim_\varepsilon \varphi = \bar{f}(0) = x_0$ and $\bar{f}$ is a continuous extension of f. So we have a path $\bar{f} : [0, \frac{t_1}{2}] \to \overline{S}$ such that $\bar{f}(0) = 0$ and $\bar{f}(t) \in S$ for $t \in (0, \frac{t_1}{2}]$, and we obtain our final path γ by reparameterizing $\bar{f}$ to the correct interval $[0,1]$.

□

Compactness

We would like to have an appropriate notion of compactness. The usual definition, namely that every open cover has a finite subcover, will not work. In particular, there are real closed fields that, under this definition, the closed unit disk would not be compact.

Example 27. Consider $R = \mathbb{Q}_{alg}$. Then

$$[0,1] = \bigcup_{0<r<\frac{1}{e}} [0, r) \cup (r, 1]$$

has no finite subcover. If $R = \mathbb{R}\langle\varepsilon\rangle$ then

$$[0,1] = \bigcup_{\substack{\ell \text{ infinitesimal} \\ r \in \mathbb{R}}} [0, \ell) \cup (r, 1]$$

has no finite subcover.

Definition 15.1. Say that a semi-algebraic set $S \subset R^k$ is *compact* if it is closed and bounded.

The main property that we need to get out of a semi-algebraic set being compact is that a semi-algebraic function should attain its maximum and minimum on the compact set.

Theorem 52. *Let $S \subset R^k$ be a closed and bounded semi-algebraic set and $g : S \to R^\ell$ a continuous semi-algebraic map. Then $g(S)$ is closed and bounded. In particular, g attains its maximum and minimum values on S.*

Proof. Claim: $g(S)$ is closed. Let $y_0 \in \overline{g(S)}$ and let $y_1 \in B_\ell(y_0, \varepsilon) \cap \mathrm{Ext}(g(S), R\langle\varepsilon\rangle)$. Let $x_1 \in \mathrm{Ext}(S, R\langle\varepsilon\rangle)$ be such that $y_1 = \mathrm{Ext}(g, R\langle\varepsilon\rangle)(x_1)$. Let $x_0 = \lim_\varepsilon x_1$ which exists since $x_1 \in \mathrm{Ext}(S, R\langle\varepsilon\rangle)$ which is bounded since S is bounded. Check that $y_0 = g(x_0)$ and hence $y_0 \in g(S)$, which implies that $g(S)$ is closed.

Claim: $g(S)$ is bounded. Hint: First show that if S is closed and bounded and $g : S \to R$ is a continuous semi-algebraic function and $\varphi \in \mathrm{Ext}(S, R\langle\varepsilon\rangle)$, then $g \circ \varphi$ is bounded over R. Then, consider the semi-algebraic set $A = \{||g(x)|| : x \in S\} \subset R$ which is a semi-algebraic subset of R, hence a finite union of points and open intervals. Look at $\mathrm{Ext}(A, R\langle\varepsilon\rangle)$, which can not contain infinite elements, so in particular $\frac{1}{\varepsilon} \notin \mathrm{Ext}(A, R\langle\varepsilon\rangle)$. This means that A does not contain an unbounded interval, so the set A is bounded, which shows directly that $g(S)$ is bounded.

□

16 March 11, Day 16

16.1 Differential calculus with semi-algebraic functions

From what we have discussed so far, it should be clear that if R is an arbitrary real closed field and $f : U \to V$ is a semi-algebraic map between semi-algebraic subsets $U \subset R^m$ and $V \subset R^n$, then you can talk about the (possible) differentiability of the function f at a point $x_0 \in U$. Generally, you can write formulas to check differentiability of the function f, and the points which satisfy such a formula would then be, itself a semi-algebraic set. For example, the function f has a derivative at $x_0 \in U$ if the usual condition

$$\lim_{|x_0-y|\to 0} \frac{f(y)-f(x_0)}{y-x_0} = b$$

is satisfied. It is not hard to write a first order formula (using universal and existential quantifiers) which is equivalent to the above expression. In particular, we can write a formula $\Phi(x)$ which checks if $f : U \to V$ is has derivatives up to order ℓ, and set $S^\ell(U,V) = \{x|\ \Phi(x)\}$.

Theorem 53 (Inverse function theorem)**.** *Let R be real closed and suppose that U, V are open neighborhoods of 0 in $\mathbb{R}^n$ and $f \in S^\ell(U,V)$ with $f(0) = 0$ such that $df_0 = (\frac{\partial f_i}{\partial x_j})$ is non-singular. Then there exists open semi-algebraic neighborhoods $U' \subset U$, $V' \subset V$ of zero such that $f|_{U'}$ is a semi-algebraic homeomorphism onto V' and $(f|_{U'})^{-1} : V' \to U'$ has derivatives up to order ℓ, that is, $(f|_{U'})^{-1} \in S^\ell(U', V')$.*

The proof of the above theorem would be a good exercise to see if you remember advanced calculus. Just do the same thing as in $\mathbb{R}$, but you had better not use the archimedean property of $\mathbb{R}$ since we are over an arbitrary real closed fields. A similar exercise would be to prove that the Implicit Function Theorem hold over an arbitrary real closed field.

16.2 Growths of semi-algebraic functions, Lojasiewicz inequality

Our next goal is to prove the following: every open semi-algebraic set can be written as the finite union of basic open semi-algebraic sets. There are several steps towards this goal, not the least of which is to prove the Lojasiewicz inequality.

Proposition 54. *Let $f : (a, \infty) \to R$ be a semi-algebraic map (not necessarily continuous). Then, there exists $c, x_0 \in R$ and $p \in \mathbb{N}$ such that $|f(x)| \le c \cdot x^p$ for all $x \ge x_0$.*

Proof. We use the first exercise from the first assignment in which we proved the above when f is a polynomial. Since the graph of f is a semi-algebraic set, suppose it has a representation as

$$graph(f) = \left\{ (x,y) \in R^2 \;\middle|\; \begin{array}{c} (h_1(x,y) = 0 \wedge g_{1,\alpha}(x,y) > 0 \wedge \dots) \\ \vee \\ (h_2(x,y) = 0 \wedge g_{2,\alpha}(x,y) > 0 \wedge \dots) \\ \vee \\ \vdots \\ \vee \\ (h_m(x,y) = 0 \wedge g_{m,\alpha}(x,y) > 0 \wedge \dots) \end{array} \right\}$$

where h_i are not the zero polynomial and at least one such h_i exists since otherwise the graph would be an open set. Set $h = h_1 \cdots h_m$ which is a non-zero polynomial, then $graph(f) \subset \{(x,y)|\ h(x,y) = 0\}$ since $h(x, f(x)) = 0$ for all $x \in (a, \infty)$. Write

$$h = q_m(X)Y^m + \cdots + q_0(X)$$

where $q_i \in R[X]$, and suppose that $|f(x)| \geq 1$. Then,

$$q_m(x)(f(x))^m + \cdots + q_0(x) = 0$$

and

$$\begin{aligned} |q_m(x)||f(x)|^m \leq & |q_{m-1}(x)||f(x)|^{m-1} + \cdots + |q_0(x)| \\ |q_m(x)||f(x)| \leq & |q_{m-1}(x)| + \cdots + |q_0(x)| \\ |f(x)| \leq & \frac{|q_{m-1}(x)| + \cdots + |q_0(x)|}{q_m(x)}. \end{aligned}$$

The last line above holds if we assume that $x > x_0'$ the largest root of $q_m(x)$. Finally, we have

$$|f(x)| \leq 1 + \frac{|q_{m-1}(x)| + \cdots + |q_0(x)|}{q_m(x)}$$

for $x \geq 2x_0'$, so set $x_0 = 2x_0'$. Now, we can use $p = \max \deg\{q_0, \ldots, q_{m-1}\}$ and an appropriate c.

□

We remark at this point that if there exists $h(X, Y) \not\equiv 0$ and $h(x, f(x)) = 0$ for $x \geq a$, then p can be chosen to be $p = \deg h$.

Proposition 55. *Let $S \subset R^k$ a closed semi-algebraic set and $f : S \to R$ a continuous semi-algebraic function. Then, there exists $c \in R$ and $p \in \mathbb{N}$ such that*

$$|f(x)| \leq c(1 + ||x||^2)^p.$$

In particular, $|f|$ is bounded by a polynomial.

Proof. If $A \cap \{x|\ |x|^2 = t\} = \emptyset$, then set $V(t) = 0$ and if $A \cap \{x|\ |x|^2 = t\} \neq \emptyset$, then set

$$V(t) = \sup_{x \in A \cap \{x||x|^2 = t\}} |f(x)|.$$

The map $V : (0, \infty) \to R$ is a semi-algebraic function. So, by the previous proposition, there exists $t_0, c_1 \in R$ and $p \in \mathbb{N}$ such that $|V(t)| \leq c_1|t|^p$ for all $t \geq t_0$. Now set

$$c_2 = \sup_{x \in A \cap \{x|||x||^2 \leq t_0\}} |f|,$$

and set $c = \max\{c_1, c_2\}$. Then, we have that $|f| \leq c(1 + ||x||^2)^p$ for all $x \in A$, as desired.

□

Here is another intermediate result before we achieve our goal. The following proposition is (more or less) the Lojasiewicz inequality. First, we need a the definition of a locally closed semi-algebraic set.

Definition 16.1 (Locally closed)**.** A semi-algebraic subset $S \subset R^k$ is said to be *locally closed* if $S = F \cap G$ where F is a closed semi-algebraic subset of R^k and G is an open semi-algebraic subset of R^k. Equivalently, if every point of S has a neighborhood whose closure (relative closure in S) is in the set S, $\forall x \in S\ \exists V$ open neighborhood of x (in the subspace topology of S) such that $\overline{V} \subset S$ (where the overline denotes closure in S).

Example 28. Any basic semi-algebraic set is locally closed. The subset of R^2 defined by $\{(x, y)|\ (x = 0 \wedge y = 0) \vee (x \neq 0 \wedge y \neq 0)\}$, which is visualized by removing the x and y axes and then adding back the origin, is NOT locally closed.

Note that the following theorem does NOT hold in general when A is not locally closed. For example, consider the subset of the plane defined by removing the x-axis and then adding back the origin. Considering the maps $f = X^2 + Y^2$ and $g = \frac{1}{Y}$, the map $f^N g = (X^2 + Y^2)^N / Y$ can not be continuously extended to the origin for any $N \in \mathbb{N}$.

Proposition 56. *Let $A \subset R^k$ a locally closed semi-algebraic set and $f : A \to R$ a continuous semi-algebraic function. Let $U := \{x \in A |\ f(x) = 0\}$ and suppose that $g : A\text{–}U \to R$ be a semi-algebraic, continuous function. Then, there exists $N \in \mathbb{N}$ such that $f^N g$ continuously extends to a map $F : A \to R$ by setting $F(x) = 0$ for all $x \in \{x \in A |\ f(x) = 0\}$.*

Proof. (Exercise: Any locally closed semi-algebraic set $A \subset R^n$ is semi-algebraically homeomorphic to a closed semi-algebraic subset of R^{n+1}.) By the exercise, we can assume that A is closed. If we can show that $f^{N-1}g$ is bounded for some $N \in \mathbb{N}$ and that for each $x' \in A \cap \{f = 0\}$ there is a neighborhood V of x' for which $f^{N-1}(x')g(x') \leq (constant)$, then it follows that $f^N g$ is continuous on A by setting $f^N g(x') = 0$ for $x' \in A \cap \{f = 0\}$.

For each $x \in A$, $u \in R$ we define the set $A_{x,u} = \{y |\ y \in A \wedge ||y - x||^2 \leq 1 \wedge u|f(y)| = 1\}$ which is a semi-algebraic subset of A, and it is closed and bounded (just look at the formula describing it). Now, set $v(x, u) = \sup_{y \in A_{x,u}} |g(y)|$ if $A_{x,u}$ is non-empty and $v(x, u) = 0$ otherwise. Then,

$$v : A \times R \to R$$

is a semi-algebraic function. There exists a partition of $A \times R$ into semi-algebraic sets B_i and for each i there are semi-algebraic maps $h_i(X, U, V) \not\equiv 0$ such that $h_i(x, u, v(x, u)) = 0$ for all $(x, u) \in B_i$. Let $x' \in A$, and let $h_{x'}$ be the product of all the h_i's such that $x' \in \pi(B_i) = B_i \cap \{x'\} \times R$. Then $h_{x'}(x', u, v(x', u)) = 0$, but $h_{x'}(X, U, V) \not\equiv 0$.

Wanting to use the previous proposition, choose $p \in \mathbb{N}$ to be the sum of the degrees of these finite number of chosen h_i's (and note that p is independent of x'), that is, we're thinking of $h_i(x', U, V)$ to be a polynomial in U, V. Then, by the previous proposition, there exists $c_{x'}, r_{x'}$ such that $|v(x', u)| \leq c_{x'}|u|^p$ for all $u > r_{x'}$.

Now, the next step is to see that $|u| = \frac{1}{f}$ and to unravel the definition of v, and doing so allows one to see that the above inequality implies that $|f(y)|^p \cdot |g(y)| \leq c_{x'}$ whenever (the analogous condition for $u > r_{x'}$ holds) we have $|f(y)| < \frac{1}{r_{x'}}$, which is exactly what we wanted to show.

We have proved that for any $x' \in A$, for all values where $|f(y)|$ is sufficiently small, then $|f(y)|^p |g(y)|$ is bounded by a constant. Choosing $N = p + 1$, we have that $f^N g$ is continuous at x' for all $x' \in A$ by setting $f^N(x')g(x') = 0$ whenever $f(x') = 0$.

□

We remark that the assumption that f be continuous is necessary. Indeed, if $f(0) = 0$ and $f(x) = 1$ for $x \neq 0$, then set $g \equiv 1$ and there is no way to extend $f^N g$ to the point $x = 0$ continuously. Additionally, the condition that the set A be locally closed is also necessary. Indeed, if $A = \{y > 0\} \cup \{(0, 0)\}$, $f = x^2 + y^2$ and $g = \frac{1}{y}$, then there is no way to extend $(x^2 + y^2)^N \frac{1}{y}$ to the origin.

We just remark that we never used the archimedean property of R, indeed R may not be archimedean for arbitrary real closed R. So the above theorems hold when R is, say for example, $R = \mathbb{R}\langle\varepsilon\rangle$ the real closed field of Puisseux series over R.

17 March 23, Day 17

We started the day by reviewing the proof of the Proposition from last time. We will now prove the following Theorem, which is due to Lojasiewicz. Afterwards, in the last part of the day we state and prove the Lojasiewicz inequality.

Theorem 57 (Lojasiewicz)**.** *Let A be a locally closed semi-algebraic set and let $f, g : A \to R$ a continuous semi-algebraic functions such that $f^{-1}(0) \subset g^{-1}(0)$. Then, there exists $N \in \mathbb{N}$ and a continuous semi-algebraic function $h : A \to R$ such that $g^N = hf$.*

Proof. Since $f^{-1}(0) \subset g^{-1}(0)$, we may look at the function $h = \frac{1}{f}$ which is defined in the set $\{g \neq 0\}$, that is, in the complement A–$\{g = 0\}$. But now, we can, by the previous proposition, there exists N such that $g^N\widetilde{h}$ extends to A as $h := g^N\widetilde{h} = 0$ if $g = 0$ and $h = g^N\frac{1}{f}$ if $g \neq 0$. Then, $g^N = hf$, as desired.

□

Aside. For a locally closed semi algebraic set A, the ring $S^0(A)$ of continuous semi-algebraic functions on A is NOT an integral domain. If we let $f \in S^0(A)$ and set $U = A$–$\{f = 0\}$, then there is a restriction map $\rho : S^0(A) \to S^0(U)$ which is NOT necessarily surjective (another map g might be continuous on U but not extend to A; it might "blow up"). However, if we *localize* $S^0(A)_f$ at f first, then the associated restriction map

$$\rho : S^0(A)_f \to S^0(U)$$

is surjective since for any $g \in S^0(U)$ there exists N, $\widetilde{g} = f^N g \in S^0(A)$ and $\frac{\widetilde{g}}{f^N} \in S^0(A)_f$ satisfies $\rho(\frac{\widetilde{g}}{f^N}) = g$.

In fact, this surjective map ρ is also injective. If $h \in S^0(A)$ restricts to zero, $\rho(h) \equiv 0$ on U, or alternatively $\rho(h) = 0$ in $S^0(U)$. Then $hf = 0$ in $S^0(A)$, which implies that $h = 0$ in $S^0(A)_f$.

Theorem 58 (Lojasiewicz inequality)**.** *Suppose A is a closed and bounded semi-algebraic set and $f, g : A \to R$ continuous semi-algebraic functions such that $f^{-1}(0) \subset g^{-1}(0)$. Then, there exists $c > 0$ and $N \in \mathbb{N}$ such that $|g(x)|^N < c|f(x)|$ for all $x \in A$.*

Proof. Immediate by taking $c = 1 + \sup_A |h|$ the supremum of h with h from the previous theorem, which exists since A is closed and bounded and h is continuous.

□

The following theorem is a useful consequence of the Lojasiewicz inequality. Recall, a basic open semi-algebraic set is a semi-algebraic set defined by a conjunction of inequalities.

Theorem 59. *Let $S \subset R^k$ be an open, semi-algebraic set. Then S has a representation as a finite union of basic open semi-algebraic sets.*

Proof. Every semi-algebraic set S is a finite union of basic semi-algebraic sets, that is, sets B which are defined by a conjunction of equalities and inequalities, say $B = \{f_1 = \cdots = f_\ell = 0 \wedge g_1 > 0 \wedge \ldots \wedge g_m > 0\}$. However, such sets B are only basic open if there are no equalities, that is, if $\ell = 0$.

Let $f = f_1^2 + \cdots + f_\ell^2$ and set $g = \prod_{i=1}^m (|g_i| + g_i)$. If S is open, then $A = R^k$–S is closed. If $x \in A$ and $f(x) = 0$ then $g(x) = 0$ by the construction of g and the fact that some condition of some B needs to fail. By Lojasiewicz Theorem, there exists $N \in \mathbb{N}$ such that $g^N = hf$ for some continuous semi-algebraic function $j : A \to R$. Furthermore, there exist $c > 0$, $p \in \mathbb{N}$ such that $|h| \leq c(1 + ||x||^2)^p$ on A. The basic open semi-algebraic set B' defined by

$$B' := \{f \cdot c(1 + ||x||^2)^p < (2^m \prod_{i=1}^m g_i)^N, g_1 > 0 \wedge \ldots \wedge g_m > 0\}$$

satisfies $B \subset B' \subset S$. Showing this finishes the proof since we can now replace all B with B' which are basic open.

□

18 March 25, Day 18

Hint for Problem 1 on Assignment #3. Want to show that for $G = \{g_1, \ldots, g_s\} \subset A = \mathbb{R}[X_1, \ldots, X_k]$, if there exists a $u \in Q(G)$ such that $\{x \in \mathbb{R}^k |\ u(x) \geq 0\}$ is compact, then $Q(G)$ is archimedean, that is, for every $a \in A$ there exists a $N \geq 1$ such that $N \pm a \in Q(G)$. Using the notation as before, we have $K_G = \{x \in \mathbb{R}^k |\ g_i(x) \geq 0, i = 1, \ldots, s\}$, and given u as in the statement, write $u = P_0 + P_1 g_1 + \cdots + P_s g_s$, with $P_i \in \sum A^2$. Note that $K_G \subset K_u$, and hence K_u compact implies K_G compact.

Aside: Ideally, we would like a statement like K_G is compact if and only if $Q(G)$ is archimedean. However, already this is false if $s > 1$ or $k > 2$. But counterexamples are sort of hard. What is true, however, is that K_G is compact if and only if $P(G)$, the cone generated by G is archimedean.

Based on the fact that K_G is compact if and only if $P(G)$ is archimedean, we have that K_u is compact implies $P(\{u\})$ is archimedean, and $P(\{u\}) \subset Q(\{u\}) \subset Q(G)$. This can be used to prove that $Q(G)$ is archimedean.

We still need some hints to prove $(**)$: K_G is compact if and only if $P(G)$ is archimedean. To that end, here are some additional exercises aimed toward proving this result.

EXERCISE 3 (1). Let $Q \subset A$ be a quadratic module and let $H_Q = \{a \in A |\ \exists N \text{ s.t. } N \pm a \in Q\}$. Show that

1. H_Q is a ring.
2. $Q \cap H_Q$ is an archimedean quadratic module.
3. Q is archimedean implies $H_Q = A$.
4. $\sum a_i^2 \in H_Q$ implies $a_i \in H_Q$.

EXERCISE 4 (2). Deduce from the above exercise that Q is archimedean if and only if $\exists N \geq 1$ such that $N - (X_1^2 + \cdots + X_k^2) \in Q$.

Theorem 60. *K_G is compact if and only if $P(G)$ is archimedean.*

EXERCISE 5 (3). The forward direction is the difficult direction of the above theorem. If K_G is compact then there exists an $N \geq 1$ such that $N - x_1^2 - \cdots - x_k^2 > 0$ for $x \in K_G$. Use Positivstellensatz to deduce that there exists some $p, q \in P(G)$ such that $p \cdot (N - X_1^2 - \cdots - X_k^2) = 1 + q$ (*i.e.*, check that this is the conclusion of the Positivstellensatz, Cor. **??**). Now, define $P' = P(G) + (N - X_1^2 - \cdots - X_k^2)P(G)$, which is a quadratic module which contains $N - X_1^2 - \cdots - X_k^2$ and hence is archimedean from the previous result (Exercise (2)). Using the previous properties of archimedean quadratic modules, there exists N' such that $N' - X_1^2 - \cdots - X_k^2 \in P(G)$ implies that $P(G)$ is archimedean.

We're now ready to continue with the scheduled lecture for today. The main theorem which we have been desiring to prove for some time seems like a natural result that we would like to have. It says that the term *basic semi-algebraic set* is a natural definition. We have proven:

Theorem 61. *If $S \subset R^k$ is an open (resp. closed) semi-algebraic set then S is a finite union of basic open (resp. closed) semi-algebraic set.*

Theorem 62. *Let $F, G \subset R^k$ be two closed, non-empty and disjoint semi-algebraic sets. Then, there exists a continuous, semi-algebraic function $f = \sum_i P_i \sqrt{1 + \sum_j Q_i j^2}$ such that $f > 0$ on F and $f < 0$ on G.*

Sketch. Assume that G is defined by a formula

$$\bigvee_{\lambda=1}^{m} \bigwedge_{\mu=1}^{q_\lambda} (g_{\lambda\mu} \geq 0).$$

We define a continuous semi-algebraic function, $h_\lambda = \sum_{\mu=1}^{q_\lambda} (|g_{\lambda\mu}| - g_{\lambda\mu})$ and let $h = \prod_{\lambda=1}^{m} h_\lambda$. Then $h = 0$ on G and $h > 0$ on F. So $\frac{1}{h}$ is continuous on F and $\frac{1}{h} < c(1 + ||x||^2)^r$ for some $c > 0$, $r \in \mathbb{N}$ by Prop. 55.

Now, define $\varepsilon(x) = \frac{1}{c(1+||x||^2)^r}$, and $\delta : R^k \to (0,1)$ to be described later. Consider

$$f_1 = \prod_{\lambda=1}^{m}(\sum_{\mu=1}^{q_\lambda}\sqrt{g_{\lambda\mu}^2 + \delta^2} - g_{\lambda\mu}).$$

Note that $f_1(x) > h(x) > \varepsilon(x)$ on F, and the last thing to check is that you can chose δ such that $f_1(x) < \frac{\varepsilon}{2}$ over G. Indeed, set $\delta = \frac{1}{d(1+||x||^2)^s}$ for chosen $d > 0$, $s \in \mathbb{N}$. Finally, set $f = \frac{1}{\varepsilon}f_1 - 1$, but this isn't in the format that we were requiring. So, instead, set $f = (1 + ||x||^2)^*(\frac{1}{\varepsilon}f_1 - 1)$ for some sufficiently high power $(*)$, to get f in the required form

□

We remark that the above holds over arbitrary real closed fields, even non-archimedean fields.

18.1 Real algebraic varieties

A semi-algebraic set is defined using inequalities and equalities of polynomials. We will now focus more on algebraic varieties, that is, sets defined by polynomial *equalities*. In particular, we will focus on varieties of the form $V_{\mathbb{F}}(F) = \{x|\ F(x) = 0\}$ where $\mathbb{F}$ is *any* field (maybe real, ordered or not, algebraically closed or not).

Definition 18.1 (Real algebraic set)**.** A *real algebraic set* $V \subset R^k$ is defined by a *single* polynomial equality $P = 0$, $P \in A = R[X_1, \ldots, X_k]$ whenever R is a real field, since $-1 \notin \sum A^2$ is equivalent to R being real.

Definition 18.2 (Regular functions on varieties)**.** Given a real algebraic set, we can define $I(V) = \{f \in R[X_1, \ldots, X_k]|f(x) = 0,\ \forall x \in V\}$. We define the *ring of regular functions* on V to be $A = R[X_1, \ldots, X_k]/I(V)$. We can define a topology on V, the Zariski topology on V, where the closed sets are algebraic subsets of V. Given an open subset of $U \subset V$ in this topology, define $\mathcal{R}_U = \{\frac{f}{g}|\ f, g \in A,\ \{g = 0\} \cap U = \emptyset\}$. The pair $(U, \mathcal{R}_U)$ is a *sheaf* on V.

Definition 18.3 (Real affine algebraic variety)**.** A *real affine algebraic variety* is a topological space X which is equipped with a sheaf $\mathcal{R}$ and is isomorphic (as a ringed topological space) to some real algebraic set.

Definition 18.4 (Real algebraic variety)**.** A *real algebraic variety* is a topological space which is equipped with a sheaf $\mathcal{R}$ such that there exists a finite open cover $\{U_i\}_{i\in I}$ such that $(U_i, \mathcal{R}|_{U_i})$ is a real affine algebraic variety.

Example 29. The so-called projective space $\mathbb{P}_R^n = \{L|\ L \text{ is a subspace of } R^{n+1} \text{ of } \dim L = 1\}$, is an algebraic variety. We need to give the structure sheaf and the finite covering.

Example 30. The grassmanian $\mathbb{G}r_R(n,k) = \{L|\ L \text{ is a subspace of } R^{n+1} \text{ of } \dim L = k\}$, is the first example of a non-affine algebraic variety (in the case $R = \mathbb{C}$ only!), but in our case when R is real closed this is an affine real algebraic variety.

19 Day 19, March 30

19.1 Some background on Sheaf Theory

Say you want to define (something like) a smooth manifold, but so that it does not depend on the embedding in the ambient space. In the following discussion, we speak roughly about the background of sheaf theory, but some (important) details will be left out in order to preserve readability. A C^∞ smooth manifold, roughly, is X a topological space which locally looks like $\mathbb{R}^n$. There needs to be an open covering, $\{U_\alpha\}_{\alpha\in I}$ and homeomorphisms $\varphi_\alpha : U_\alpha \to \mathbb{R}^n$, called the *charts* or *local coordinates*. Now, there needs to be some

relationships on the charts φ_α. In particular, the intersection $U_\alpha \cap U_\beta$ and the charts $\varphi_\alpha, \varphi_\beta$ need to behave in a "nice" way. Specifically, there needs to be transition maps $\varphi_{\alpha,\beta} : \varphi(U_\alpha \cap U_\beta) \to \varphi_\beta(U_\alpha \cap U_\beta)$ which allow you to compare the charts (local coordinates) for points in the intersection of two sets of the open covering. When the transition maps are, themselves, C^∞ maps (from $\mathbb{R}^n$ to $\mathbb{R}^n$), then what we have defined is (up to some technical details) a "n-dimensional C^∞ manifold". To continue in this thread, we would next wish to define maps between these objects.

Another way to define a smooth manifold is to define its *structure sheaf*. We first should just define, abstractly, a sheaf. To that end, we first define a presheaf.

Definition 19.1 (Presheaf)**.** A *presheaf* $\mathcal{F}$ of functions is a topological space of functions given by the following data. For every open $U \subset X$, $\mathcal{F}(U)$ is a ring of $\mathbb{R}$-valued functions on U. If $U \subset V$ are two open subsets of X, then there is a restriction homomorphism $r_{V,U} : \mathcal{F}(V) \to \mathcal{F}(U)$ which may not be surjective, but satisfies

1. $r_{U,U} = Id$.
2. $U \subset V \subset W$ implies $r_{W,U} = r_{V,U} \circ r_{W,V}$.

Definition 19.2 (Sheaf)**.** A *sheaf* is a presheaf which additionally satisfies

3. For $s, t \in \mathcal{F}(U)$, if $r_{V,U}(s) = r_{V,U}(t)$ for all $U \subset V$ open, then $s = t$.
4. If $\{U_\alpha\}$ is an open cover of U, and $s_\alpha \in \mathcal{F}(U_\alpha)$ with $r_{U_\alpha, U_\alpha \cap U_\beta}(s_\alpha) = r_{U_\beta, U_\alpha \cap U_\beta}(s_\beta)$, then $\exists s \in F(U)$ such that $r_{U,U_\alpha}(s) = s_\alpha$.

If X is a C^∞ manifold, we write $\mathcal{O}_x$ for the structure sheaf on X, which is given by $\mathcal{O}_x(U)$ =ring of C^∞ functions $U \to \mathbb{R}$. This is the second method for describing a smooth manifold. The first way was to make-up a manifold by glue-ing together simple pieces (subsets of $\mathbb{R}^n$) using transition maps that belong to some class (of functions, say C^∞ maps).

19.2 Algebraic geometry

For this subsection, unless otherwise stated, R is a real closed field.

Definition 19.3 (Real algebraic set)**.** Let $V \subset R^k$ such that $V = \{P = 0 |\ P \in R[X]\}$, where $X = (X_1, \ldots, X_k)$. Then, V is called a *real algebraic set*.

We make a real algebraic set, V, into a topological space by defining the Zariski topology on V. A closed set in the Zariski topology of V is $K = \{x \in V |\ f(x) = 0 \text{ for some } f \in \mathcal{R}[V]\}$, where $\mathcal{R}[V] = \{\frac{p}{q} |\ p, q \in R[X], q(x) \neq 0 \text{ for all } x \in V\}$ is the set of regular functions on V. Let $\mathcal{O}_V$ be the structure sheaf on V (based on the previous discussion). If $U \subset V$ is a Zariski open set, then $\mathcal{O}_V(U) = \mathcal{R}_U$.

Definition 19.4 (Real affine algebraic variety)**.** A *real affine algebraic variety* $(X, \mathcal{O}_X)$ is a ringed topological space (defined to be a topological space equipped with a structure sheaf of functions) that is isomorphic (as ringed topological spaces) to $(V, \mathcal{O}_V)$ where $V \subset R^k$ is a real algebraic set.

Definition 19.5 (Real algebraic variety)**.** A *real algebraic variety* $(X, \mathcal{O}_X)$ is a ringed topological space such that there is a finite open covering $\{U_\alpha\}$ such that each $(U_\alpha, \mathcal{O}_X|_{U_\alpha})$ is a real affine algebraic variety.

In the above definition, the notation $\mathcal{O}_X|_{U_\alpha}$ means the sheaf which is the restriction of $\mathcal{O}_X$ which takes only subsets of U_α as inputs, *i.e.*, its basically the same as $\mathcal{O}_X$ but only write $\mathcal{O}_X(U)$ for $U \subset U_\alpha$.

Example 1 (Projective space as a real algebraic variety). Let $\mathbb{P}^n_R$ denote the set

$$\mathbb{P}^n_R = \{L |\ L \subset R^{n+1} \text{ linear subspace of dimension } 1\}.$$

Before we even define a topology on $\mathbb{P}^n_R$, let's introduce homogeneous coordinates so that we can discuss the points of $\mathbb{P}^n_R$. The point $\{(tx_0, \ldots, tx_n) |\ t \in R\} \in \mathbb{P}^n_R$ is described by homogeneous coordinates $(x_0 : x_1 : \cdots : x_n) = (\lambda x_0 : \lambda x_1 : \cdots : \lambda x_n)$ for $\lambda \neq 0$ non-zero scalar.

For $i = 0, \ldots, n$ we define $U_i = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n_R |\ x_i \neq 0\} \subset \mathbb{P}^n_R$, which will eventually be (after we have a topology) our open covering. Clearly, $\mathbb{P}^n_R = \cup_{i=0}^n U_i$. The charts will be $\varphi_i : U_i \to R^n$ defined by

$$\varphi(x_0 : \cdots : x_n) = (\tfrac{x_0}{x_i}, \ldots, \tfrac{x_{i-1}}{x_i}, \tfrac{x_{i+1}}{x_i}, \ldots, \tfrac{x_n}{x_i})$$

which is a bijective map.

We next define the Zariski topology on $\mathbb{P}^n_R$, which is given by $U \subset \mathbb{P}^n_R$ is open if and only if $\varphi_i(U_i \cap U)$ is open in R^n for each $i = 0, \ldots, n$. That is, we use the real affine variety R^n (and the bijective maps φ_i) to construct the topology on $\mathbb{P}^n_R$.

Consider the following isomorphism (chart).

$$\varphi_i(U_i \cap U_j) \to \varphi_j(U_i \cap U_j)$$
$$(\tfrac{x_0}{x_i}, \ldots, \tfrac{x_{i-1}}{x_i}, \hat{1}, \tfrac{x_{i+1}}{x_i}, \ldots, \tfrac{x_n}{x_i}) \overset{\cdot \frac{x_i}{x_j}}{\mapsto} (\tfrac{x_0}{x_j}, \ldots, \tfrac{x_{j-1}}{x_j}, \hat{1}, \tfrac{x_{j+1}}{x_j}, \ldots, \tfrac{x_n}{x_j})$$

Which is a bi-regular isomorphism with the obvious inverse map.

For any open $U \subset \mathbb{P}^n_R$, set $\mathcal{R}(U) = \cap_{i=0}^n \mathcal{R}(U \cap U_i)$ where $\mathcal{R}(U \cap U_i)$ is the set of regular functions on the subset of U_i (which is defined using the previous charts, transition map defined above).

It will turn out that $\mathbb{P}^n_R$ is a real *affine* variety, but this will take some work. This is NOT true when you replace R with $\mathbb{C}$. In particular, $\mathbb{P}^n_{\mathbb{C}}$ is NOT a complex affine variety, and the set of regular functions $\mathcal{R}(\mathbb{P}^n_{\mathbb{C}})$ is the constants, and for R a real closed field there are LOTS of non-constant regular functions in $\mathcal{R}(\mathbb{P}^n_R)$. This marks (another) significant difference between real algebraic geometry and (complex) algebraic geometry.

Example 2. We will show that $\mathbb{G}r_R(n,k) = \{L \subset R^n |\ L \text{ is } k\text{-dimensional subspace of } R^n\}$. In one particular case, $\mathbb{G}r_R(n+1,1) = \mathbb{P}^n_R$. Furthermore, we will show that $\mathbb{G}r_R(n,k)$ has a natural structure of a real algebraic variety, and that $\mathbb{G}r_R(n,k)$ is in fact a real affine variety.

In general, over any field of characteristic zero, if $L \subset V$ is a linear subspace and $\{v_1, \ldots, v_k\}$ is a basis of L, then $v_1 \wedge v_2 \wedge \ldots \wedge v_k \in \bigwedge^k V$ is an element in the exterior product of V. The Plücker embedding,

$$L \mapsto \overline{v_1 \wedge v_2 \wedge \ldots \wedge v_k} \in \mathbb{P}(\bigwedge^k V)$$

gives a map $\varphi_{n,k} : \mathbb{G}r(n,k) \to \mathbb{P}(\bigwedge^k V)$.

20 Day 20, April 1

We continue our discussion on the real Grassmanian. As a set, the real Grassmanian $\mathbb{G}r(n,k) = \{V \subset R^n |\ V \text{ a subspace of dimension } k\}$. Our first task is to impose the structure of a real algebraic variety on the set $\mathbb{G}r(n,k)$. The procedure will follow closely what we did (last time) for real projective space. We will cover $\mathbb{G}r(n,k)$ by certain sets U_i which map to affine spaces, and then glue together the pre-images to give $\mathbb{G}r(n,k)$ the structure of a real algebraic variety.

Let $e_1, \ldots, e_n$ be the canonical basis vectors of R^n. We denote $[n] = \{1, \ldots, n\}$. For each $\sigma \in [n]$, if $\#|\sigma| = k$, we let $V_\sigma = span(e_i)_{i \in \sigma}$, $W_\sigma = span(e_i)_{i \notin \sigma}$ and $U_\sigma = \{V \in \mathbb{G}r_R(n,k) |\ V \cap W_\sigma = \{0\}\}$. For example, in the case $k = 1$, it is a good (easy) exercise to check that these definitions coincide to the previous case of real projective space.

As a set, the real Grassmanian is covered by these sets,

$$\mathbb{G}r_R(n,k) = \bigcup_{\substack{\sigma \subset [n] \\ \#|\sigma| = k}} U_\sigma.$$

Consider the projections, for $V \in U_\sigma$, which are $P_{V_\sigma}, P_{W_\sigma}$ isomorphisms of V when $V \in U_\sigma$, hence $P_V = P_{W_\sigma} \circ P_{V_\sigma}^{-1} : V_\sigma \to W_\sigma$ is a homomorphism. In particular, if $v = v_\sigma + w_\sigma$, then $v = v_\sigma + P_V(v_\sigma)$, and hence for $V \in U_\sigma$ there is a homomorphism which describes V as $V = \{v_\sigma + P_V(v_\sigma) |\ v_\sigma \in V_\sigma\}$, and hence there is a one-to-one correspondence between $V \in U_\sigma$ and homomorphisms $P_V : V_\sigma \to W_\sigma$.

Let us examine this homomorphism P_V more closely. Considering the matrix which represents this linear map in the standard basis of R^n, let $A_V = (a_{ij})_{\substack{i \notin \sigma \\ j \in \sigma}}$ be this matrix representing P_V. Now, consider the charts

$$\begin{aligned} \varphi_\sigma : U_\sigma &\to R^{(n-k)\times k} \\ V &\mapsto A_V \end{aligned}$$

and we need to find the appropriate transition maps, which need to be regular maps (in this case, given by a quotient of polynomials in which the denominator does not vanish on the domain).

We need to show that $\varphi_\sigma(U_\sigma \cap U_\tau), \varphi_\tau(U_\sigma \cap U_\tau)$ are Zariski open sets in $R^{(n-k)\times k}$, and that the map defined by

$$\begin{aligned} \theta_{\sigma\cdot\tau} : \varphi_\sigma(U_\sigma \cap U_\tau) &\to \varphi_\tau(U_\sigma \cap U_\tau) \\ A &\mapsto \varphi_\tau \circ \varphi_\sigma^{-1}(A) \end{aligned}$$

is regular. Of course, the difficulty is not in defining the map $\theta_{\sigma\cdot\tau}$ but in showing that this map is given by polynomials.

First, we show that $\varphi_\sigma(U_\sigma \cap U_\tau)$ is Zariski open, and by symmetry then $\varphi_\tau(U_\sigma \cap U_\tau)$ is also Zariski open. Let $\tau \subset [n]$ with $|\tau| = k$, and let $V \in U_\sigma$. Then, A_V is the matrix of $P_V : V_\sigma \to W_\sigma$. Let A'_V be the matrix $(a_{ij})_{\substack{i \in [n] \\ j \in \sigma}}$ obtained by augmenting the matrix A_V by Id_{R^σ} (put a 1 in a_{ii} when $i \in \sigma$ and a zero when $i \neq j$, $i, j \in \sigma$). Consider

$$\begin{aligned} P'_V : V_\sigma &\to R^n \\ v_\sigma &\mapsto v_\sigma + P_V(v_\sigma) \end{aligned}$$

and notice that $P'_V(V) = V$, and $P'_V = Id_{V_\sigma} + P_V$. Let B be the $\tau \times \sigma$ matrix extracted from A'_V. Then, $V \in U_\tau$ if and only if B is invertible, which is from the following diagram. This verifies that $\{A_V \in R^{(n-k)\times k} |\ B \text{ is not invertible}\}$ is a Zariski open subset (since when we augmented A_V to A'_V and then looked at the determinant we ended up with checking if a polynomial is zero). This shows that $\varphi_\sigma(V_\sigma \cap V_\tau)$ is Zariski open.

Last, we need to show that the transition map $\theta_{\sigma\cdot\tau}$ is regular. We let C be the matrix $C = A'_V B^{-1}$ and note that C is the matrix for a linear map $C : V_\tau \to R^n$ which takes a vector $v_\tau \mapsto v_\tau + w_\tau$ where $w_\tau \in W_\tau$. In particular, the image of the map C on V_τ is just V. Lets write $C = (c_{ij})_{\substack{i \in [n] \\ j \in \tau}}$. Extracting $C' = (c_{ij})_{\substack{i \notin \tau \\ j \in \tau}}$ from C, we obtain $C'_V = \varphi_\tau(V)$. The process of extracting, augmenting, or taking inverses are regular maps (on matrices?). So, we end up with a regular map $A_V \mapsto C'_V$, as desired.

We next aim at showing that the real Grassmanian is in fact a real projective variety. Consider the map

$$\begin{aligned} \varphi_{n,k} : \mathbb{G}r_R(n,k) &\to \mathbb{P}(\bigwedge^k R^n) \\ span(v_1, \ldots, v_k) &\mapsto \overline{v_1 \wedge \ldots \wedge v_k} \end{aligned}$$

We will actually prove that the real Grassmanian is a real affine variety. For each $V \in \mathbb{G}r_R(n,k)$ there is a one-to-one correspondence (via a set map Ψ) to the $n \times n$ matrix of the orthogonal projection onto V with respect to the canonical basis. What types of matrices in $R^{n\times n}$ can be in this image? We would need to have $A^2 = A$, so the eigenvalues are $0, 1$, and A needs to be symmetric and $tr(A) = k$. The real algebraic set $H_{n,k} = \{A \in R^{n\times n} |\ A \text{ symmetric},\ A^2 = A,\ tr(A) = k\}$ in $R^{n\times n}$ is the image of the map Ψ, and we still need to show that this map (which right now is just a map of sets), actually preserves the structure of the real algebraic variety.

For each U_σ in $\mathbb{G}r_R(n,k) = \bigcup_{\substack{\sigma\subset[n]\\ \#|\sigma|=k}} U_\sigma$, we have

$$U_\sigma \qquad\qquad \Psi(U_\sigma) \subset H_{n,k}$$

$$R^{(n-k)\times k}$$

The set $\Psi(U_\sigma)$ is Zariski open in $H_{n,k}$, and $\Psi\circ\varphi_\sigma^{-1}$ gives a biregular isomorphism between $R^{(n-k)\times k} \to \Psi(U_\sigma)$.

21 Day 21, April 6

NO CLASS NEXT TUESDAY. The goal for the remainder of the semester is to discuss the following topics.

1. Quantitative aspects of real algebraic geometry.
2. Algorithmic aspects of real algebraic geometry. It is recommended to register to A. Gabrielov's course next semester entitled *Using algebraic geometry.*

Today, however, we discuss a little bit of dimension theory of real algebraic varieties. The reason for this is to go over some pitfalls which one must avoid.

Normally from the point of view of commutative algebra, ring theory: given a commutative ring A (say a polynomial ring), the dimension (or *krull dimension*) of A is normally defined to be the length of the longest chain of prime ideals in A.

$$\dim A = n \qquad iff \qquad P_0 \subset P_1 \subset \cdots \subset P_n = A,$$

where each P_i is a prime ideal of A, and there is no longer such chain. Given an ideal $I \subset A$. The dimension of I is the dimension of the quotient ring $\frac{A}{I}$. This is the usual definition, which leads to the following.

Definition 21.1. If $V \subset R^n$ is an irreducible real algebraic set then $\dim V$ is defined to be the dimension of $R[X_1,\ldots,X_n]/\mathcal{I}(V)$ where $\mathcal{I}(V)$ is the ideal of polynomials which vanish on V.

In the above, an *irreducible real algebraic set* is one which can not be written as a union of two non-empty real algebraic sets. Notice that in the above definition, since V is irreducible, then $\mathcal{I}(V)$ is a prime ideal (EXERCISE).

Theorem 63. *Jacobian criterion Let $P \subset R[X_1,\ldots,X_n]$ be a prime ideal and suppose that $P = (F_1,\ldots,F_s)$ and let $\dim P = d$. Then $\mathcal{J}(P) = [\frac{\partial F_i}{\partial X_j}]_{\substack{1\le i\le s\\ 1\le j\le n}}$ has rank $n-d$ over the field of fractions of $R[X_1,\ldots,X_n]/P$. In particular, this rank does not depend on the set of generators $F_1,\ldots,F_s$.*

Example 31. Consider $P = (X, Y, X-Y) \subset R[X,Y]$. Then $\dim P = \dim \frac{R[X,Y]}{(X,Y,X-Y)} = 0$. And, the rank of

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \end{bmatrix}^T$$

is clearly 2.

Definition 21.2. Let $V \subset R^n$ be an irreducible (real algebraic) set and suppose $\mathcal{I}(V) = (F_1,\ldots,F_s)$ and let $x \in V$. The tangent space (or *Zariski* tangent space) $T_{x,V} \subset R^n$ is the linear subspace of R^n defined by the following equations using the entries of the Jacobian.

$$\sum_{j=1}^{n} \frac{\partial F_i}{\partial x_j}(x) X_j = 0, \quad i = 1,\ldots,s$$

By the previous Theorem, the dimension $\dim T_{x,V} \geq \dim V$ whenever V is an irreducible real algebraic set.

Example 32. For instance, consider V defined by $Y^2 = X^3 + X^2$. Then, $\dim T_{x,V} = 1$, for $x \neq 0$. It is clear that the Jacobian matrix $\mathcal{J}(Y^2 - X^3 - X^2)$ is the zero matrix when $x = 0$, and hence $\dim T_{x,V} = 2$ when $x = 0$.

Definition 21.3. We say that $x \in V$ is a *non-singular point* of an irreducible algebraic set V if $\dim T_{x,V} = \dim V$. Otherwise, the point x is said to be a *singular point*.

These criterion for a point to be singular require the GLOBAL DATA which, in this case, are the generators of the ideal $\mathcal{I}V$. We give equivalent LOCAL definitions of tangent space, singular points. To this end, after some change of coordinates, we may as well assume that the point x we are inspecting is the origin $x = 0$.

Let $m_0 = \{f \in R[X_1, \ldots, X_n] |\ f(0) = 0\}$. We have a natural isomorphism $\varphi : \frac{m_0}{m_0^2} \xrightarrow{\sim} (R^n)^\wedge$ to the dual $(R^n)^\wedge$ of R^n. In particular, the subspace $T_{0,V} \subset R^n$ is translated (in the dual) to a quotient of $(R^n)^\wedge = \frac{m_0}{m_0^2}$.

EXERCISE 6. Check that $(T_{0,V})^\wedge \cong \frac{m_0}{(m_0^2 + \mathcal{I}(V))}$. In fact, it is not hard to show that $\frac{m_0}{(m_0^2+\mathcal{I}(V))} \cong \frac{m_{0,V}}{m_{0,V}^2}$ where $m_{0,V}$ is the ideal of $\mathcal{R}_V$ (the regular functions on V) which vanish at 0.

Example 33. Going back to our previous example, let V be defined by the equation $Y^2 = X^3 + X^2$. Then $A = \frac{R[X,Y]}{(Y^2 - X^3 - X^2)}$, then $m_{0,V} = (\bar{X}, \bar{Y})$ and $m_{0,V}^2 = (\bar{X}^2, \bar{Y}^2, \bar{X}\bar{Y}) = (\bar{X}^2, \bar{X}^3, \bar{X}\bar{Y})$. Then, $\dim \frac{m_{0,V}}{m_{0,V}^2} = 2$.

This ends the definition of the local definition of the (Zariski) tangent space: use $(T_{x,V})^\wedge \cong \frac{m_{x,V}}{m_{x,V}^2}$. For the local criterion for non-singularity, we define $\mathcal{R}_{V,0}$ to be the ring of germs of regular functions at 0. That is, $\mathcal{R}_{V,0} = \{f \in R_{U,0} |\ U \text{ is a Zariski open nbh of 0 in } V\}$, where $f, g \in \mathcal{R}_{V,0}$ are equal in the ring whenever they agree on some neighborhood U of 0 in V. This ring, $\mathcal{R}_{V,0}$ is a local ring which means that it has a unique maximal ideal, which we denote $m_{V,0} \subset R_{V,0}$ (we will see how this ideal relates with previously defined $m_{0,V}$ in a moment, but briefly one is "contained" in the other). In general, $\dim R_{V,0} \leq \dim \frac{m_{V,0}}{m_{V,0}^2}$. The point 0 is non singular if $\dim R_{V,0} = \dim \frac{m_{V,0}}{m_{V,0}^2}$. This criterion is important in ring theory, and warrants its own terminology.

Definition 21.4. A local ring (A, m) is called *regular* if the above property on dimension is satisfied. That is, if $\dim A = \dim_{A/m} \frac{m}{m^2}$.

Example 34. The Grassmanian $\mathbb{G}r_R(n,k)$ is a real algebraic variety and is covered by the real affine algebraic varieties U_σ, $\mathbb{G}r_R(n,k) = \cup_{\substack{\sigma \subset [n] \\ |\sigma| = k}} U_\sigma$, and each $U_\sigma \cong R^{(n-k)\times k}$. In particular, since there are no singular points in $R^{(n-k)\times k}$, this shows that the Grassmanian is a non-singular variety (it does not contain any singular points).

Now, let's leave talking about just real algebraic sets, but let's discuss real affine varieties and real algebraic varieties.

Definition 21.5. Let X be a real algebraic variety and $x \in X$. We say that x is a non-singular point of dimension d in X if $\dim R_{x,X} = \dim \frac{m_{x,X}}{m_{x,X}^2} = d$. Say that X is non-singular of dimension d if every point $x \in X$ is a non-singular point of dimension d.

In particular, based on the previous example, the Grassmanian $\mathbb{G}r_R(n,k)$ is a non-singular real algebraic variety of dimension $(n-k)k$.

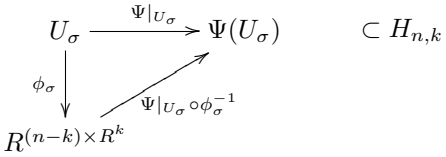
Next, let's look at points which may belong to more than one irreducible component of a non-irreducible algebraic set. Consider the real algebraic set V defined by $XY = 0$. The origin belongs to both irreducible components of V, and hence it can not be non-singular (this takes a little work to show, but the implication is that if $x \in V$ is non-singular then it belongs to exactly one irreducible component of V).

Example 35. Consider the algebraic set V defined by $X(Y^2 + X^2 - X^3)$ which consists of the Y-axis and a (an elliptic) curve with an isolated point at the origin. The origin is a singular point.

Example 36. Consider the algebraic set V defined by $Y^3+2X^2Y-X^4=0$, which gives an irreducible algebraic set V. After completing the square we obtain $Y^2(1+Y)=(X^2-Y)^2$, hence $X^2=Y(1+Y\sqrt{1+Y})$. There is only a doubt that the origin is singular or not. It appears (geometrically, looking at the picture) that there is nothing "special" happening at the origin, all the derivatives exist in a nbh of the origin. However, using the Jacobian criterion, it is shown that the origin is actually a singular point.

22 Day 22, April 8

Some comments on the most recent assignment, Assignment #4. Problems (3)-(4) are really the same problem, so there are only 8 problems. In this problem (3)-(4), we have $H_{n,k}=\{A\in R^{n\times n}|A=A^T,\ A=A^2,\ trA=k\}$ is a real affine algebraic variety. We have been given the map Ψ in the problem. We need to see that the following diagram commutes, and that the maps in it are regular.



We now begin a new topic: the notion of effective algorithms.

22.1 Effectivity: Tarski-Seidenberg

Recall that the Tarski-Seidenberg quantifier elimination theorem stated that each quantified first order formula in the language of the reals is equivalent to a quantifier free first order formula. We make this statement precise in the following paragraph.

T-S Quantifier Elimination Theorem

Let $\Phi:=(Q_1Y^1)(Q_2Y^2)\dots(Q_\omega Y^\omega)\varphi(X,Y^1,Y^2,\dots,Y^\omega)$ be a quantified first order formula in the language of the reals where Y^i is a block of k_i variables, $Q_i\in\{\exists,\forall\}$, and $Q_i\neq Q_{i+1}$. So, the quantifiers are alternating. Furthermore, X, the free variables of the quantified formula, is a block of k variables, and φ is a quantifier free $\mathcal{P}$-formula, where $\mathcal{P}\subset D[X,Y^1,\dots,Y^\omega]$. Recall, that a $\mathcal{P}$-formula is a formula where all the atoms involve only polynomials from the family $\mathcal{P}$ (so $\mathcal{P}$ can assumed to be finite, for example). Suppose that $|\mathcal{P}|\leq s$ and for all $P\in\mathcal{P}$ we have $\deg P\leq d$. Then, there exists a quantifier free formula

$$\Psi(X):=\bigvee_{i=1}^{N}\bigwedge_{j=1}^{N_i}(P_{ij}\varepsilon_{ij}0)$$

where $\varepsilon_{ij}\in\{>,<,=\}$ and $\Psi(X)\iff\Phi(X)$, and with $P_{ij}\in D[X]$.

Questions:

1. How efficiently can you compute Ψ given Φ? That is, if Φ is very "complex" then how many arithmetic operations are required to compute the polynomials P_{ij} in terms of the complexity of Φ?

2. Can we obtain tight bounds on $N, N_i, \deg P_{ij}$ in terms of $k, k_1,\dots,k_\omega, s, d$?

These questions are kind of natural to ask. But, initially, the bounds we might come up with are very bad. In one case, the bounds to the answer of the (1rst/2nd?) question results in a bound consisting of a

tower of exponents, the length of which depends on the number of variables. There is an example that shows that the bounds must depend at least doubly exponentially on the number of quantifier eliminations ω. It will be a goal to prove the following theorem.

Theorem 64. *The quantities N, N_i and the polynomials $\deg P_{ij}$ can be computed using at most*

$$(sd)^{(k+1)\prod_{i=1}^{\omega} O(k_i+1)}$$

algebraic operations. In the above notation, $O(k_i+1)$ means big-oh notation and in this case means something like $k_i + 1 + C$ where C is a constant which does not depend on N, N_i or $\deg P_{ij}$.

In the special case where $k = 0, \omega = 1$, and $Q_1 = \exists$, we have to eliminate the quantifier from the quantified first order formula $\exists Y^1 \phi(Y^1)$. This problem is called the *Existential theory of the reals* and involves deciding whether or not a certain set is empty. The number of algebraic operations required to answer the question is then bounded by $(sd)^{O(k_1)}$, based on effective quantifier elimination.

A different question one might ask is to decide if a given semi-algebraic set is connected or not. Or, more generally, to decide the number of connected components of a given semi-algebraic set.

22.2 Quantitative Questions

Given a $\mathcal{P}$-semi-algebraic set $S \subset R^k$ with $|\mathcal{P}| \leq s$, $\deg P \leq d$ for $P \in \mathcal{P}$, can we obtain an upper bound on $b_0(S)$ the number of connected components of S? More generally, can we obtain an upper bound on $b_i(S)$ for all $i \geq 0$, where $b_i(S)$ is the i-th betti number of S. We aim to show that $b_0(S) \leq (sd)^{O(k)}$.

We next discuss, on the side, the notion of sign conditions on $\mathcal{P}$ and the number of realizable sign conditions. For a family of s polynomials $\mathcal{P} = \{P_1, \ldots, P_s\} \subset R[X_1, \ldots, X_k]$ in k variables, the number of possible *sign conditions* $\sigma \in \{-1, 1, 0\}^{\mathcal{P}}$ is less than or equal to 3^s. However, we say that a sign condition σ is *realizable* if the set $\{x \in R^k | \ sign(P_i(x)) = \sigma(P_i), i = 1, \ldots, s\}$ is non-empty. It turns out that the number of realizable sign conditions is bounded by $(sd)^{O(k)}$ as above. Showing these facts will be our goals for the remainder of the semester.

22.3 Triangulation Theorem for Semi-algebraic Sets

A useful tool in examining semi-algebraic sets is the so-called semi-algebraic triangulation theorem. This theorem allows you to view a semi-algebraic set as a simplicial complex, whose structure is particularly simple.

Definition 22.1 (Simplicial complex)**.** An abstract (finite) simplicial complex is a subset of $K \subset 2^{[n]}$ which is closed under taking subsets.

Example 37. The sets $2^{[n]}, \emptyset, \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}\}$ are examples of abstract simplicial complexes.

To each abstract simplicial complex K, we have an associated geometric object $|K|$ which is a polyhedron defined by

$$|K| = \bigcup_{\sigma \in K} |\sigma|$$

where $|\sigma| = \{\sum_{i \in \sigma} x_i e_i | \ x_i > 0, \sum_i x_i = 1\}$ and $e_0, \ldots, e_n$ are the standard basis vectors in R^{n+1}.

Example 38. For $\sigma = [n]$, we have that $|[n]|$ is the standard open n-simplex in R^{n+1}. For $K = 2^{[n]}$ we have that $|K|$ is the standard closed n-simplex in R^{n+1}. For a non-standard example, the simplicial complex $K = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}\}$ has realization $|K|$ in R^3 as the union of two closed line segments.

Definition 22.2. Let $S \subset R^k$ be a closed and bounded semi-algebraic subset of R^k. Then a semi-algebraic triangulation of S is a semi-algebraic homeomorphism $h : |K| \to S$ where K is a finite simplicial complex.

The following theorem, which is our goal to prove, says that closed and bounded semi-algebraic sets can always be triangulated.

Theorem 65. *Every closed and bounded semi-algebraic set admits a semi-algebraic triangulation.*

23 Day 23, April 15

Last time: we discussed triangulations of closed and bounded semi-algebraic sets. Specifically, given R a real closed field and $S \subset R^k$ a closed and bounded semi-algebraic set, the triangulation theorem (Thm. 65) asserts the existence of a finite simplicial complex K and a semi-algebraic homeomorphism $h : |K| \to S$ which is called the triangulation of S. Moreover, if S is defined by a $\mathcal{P}$-formula, where $\mathcal{P} \subset R[X_1, \ldots, X_k]$ with $|\mathcal{P}| = s$ and $\max_{p \in \mathcal{P}} \deg P = d$, then the number of vertices $|K_0|$ is bounded by some function $F(s, d, k)$.

Note that this means that the number of homeomorphism types of semi-algebraic sets defined by s polynomials of degree at most d in k variables is not only finite but bounded uniformly by a function $F(s, d, k)$.

For the sake of time, we defer the proof of the triangulation theorem and instead study topological aspects of simplicial complexes.

23.1 Topology of simplicial complexes, simplicial cohomology groups

What are some invariants of homeomorphism types? That is, let us describe some object $C(X)$ for which $C(X) = C(Y)$ whenever the sets $X \approx Y$ are homeomorphic.

Let K_p denote the set of p-simplices of K. So, for example, K_0 is the set of *vertices* of the simplicial complex K. That is, $K_p = \{\sigma \in K || \sigma \text{ is a } p\text{-simpliex}, card(\sigma) = p + 1\}$. Then $K = \cup_{p \geq 0} K_p$. We denote by $C^p(K)$ the $\mathbb{Z}/2\mathbb{Z}$-vector space of $\mathbb{Z}/2\mathbb{Z}$-valued functions defined on the p-simplices of K. That is, $C^p(K) = \{\varphi : K_p \to \mathbb{Z}/2\mathbb{Z}\}$ is the $\mathbb{Z}/2\mathbb{Z}$-vector space with basis $\{e_\sigma\}_{\sigma \in K_p}$ where $e_\sigma(\sigma) = 1$ and $e_\sigma(\sigma') = 0$ if $\sigma' \in K_p - \{\sigma\}$. We sometimes say that $C^p(K)$ is the vector space of *p-cochains* of K.

We next define the *coboundary* maps. Let δ_p be the map $C^p(K) \overset{\delta_p}{C}{}^{p+1}(K)$ defined by the following rule. For $\varphi \in C^p(K)$ we have $\delta^p(\varphi)([i_0, \cdots, i_{p+1}]) = \sum_{j=0}^{p+1} \varphi([i_0, \ldots, \widehat{i_j}, \ldots, i_{p+1}])$. It is an exercise to check that δ_p so defined is a homomorphism of $\mathbb{Z}/2\mathbb{Z}$-vector spaces. We have the following sequence

$$C^0(K) \overset{\delta^0}{\to} C^1(K) \overset{\delta^0}{\to} C^2(K) \to \cdots$$

which is a *complex* of vector spaces.

Definition 23.1. Simple complex of vector spaces A *simple complex* $C^\bullet$ is a sequence $\{C_i\}_{i \in \mathbb{Z}}$ of vector spaces along with homomorphisms $C^i \overset{\delta^i}{C}{}^{i+1}$ along with the additional criterion that $\delta^{i+1} \circ \delta^i = 0$.

It remains to show that the coboundary maps δ^p defined above satisfy $\delta^{p+1} \circ \delta^p = 0$. This is just a calculation, which we do below. We need to check that the following composition of maps is the zero map.

$$C^p(K) \overset{\delta^p}{\to} C^{p+1}(K) \overset{\delta^{p+1}}{\to} C^{p+2}(K)$$

Given a $p+2$-simplex $\sigma \in K_{p+2}$, we need to see what $\delta^{p+1} \circ \delta^p(\varphi)$ does to σ for an arbitrary $\varphi \in C^p(K)$. We have

$$\begin{aligned}
\delta^{p+1} \circ \delta^p(\varphi)([i_0, \ldots, i_{p+2}]) &= \sum_{j=0}^{p+2} (\delta^p \varphi)([i_0, \ldots, \widehat{i_j}, \ldots, i_{p+2}]) \\
&= \sum_{j=0}^{p+2} \sum_{\substack{0 \leq \ell \leq p+2 \\ \ell \neq j}} \varphi([i_0, \ldots, \widehat{i_\ell}, \ldots, \widehat{i_j}, \ldots, i_{p+2}]) = 0
\end{aligned}$$

The last calculation is verified by seeing that each term in the last line appears exactly twice (and noting that we choose coefficients in $\mathbb{Z}/2\mathbb{Z}$).

We let $C^\bullet(K)$ denote the cochain complex of K, and by definition we set $C^{-i}(K) = 0$ when $i > 0$. Since the compositions of two successive coboundary maps are zero $\delta^{p+1} \circ \delta^p = 0$, this means that $im(\delta^p) \subset ker(\delta^{p+1})$. Conventionally, we name the subspace $ker(\delta^{p+1})$ to be the cocycles, and the subspace $im(\delta^p)$ the coboundaries. Since both these subspaces are contained in the vector space of cochains $C^{p+1}(K)$, their quotient is a vector space and is denoted $H^{p+1}(C^\bullet(K))$ and is called the $p+1$-st cohomology group of $C^\bullet(K)$ (or just of K).

Definition 23.2. The simplicial cohomology groups $H^*(K)$ are the groups $H^i(K) = H^i(C^\bullet(K))$. The i-th $\mathbb{Z}/2\mathbb{Z}$-Betti number of K is defined to be the dimension of the i-th cohomology group and write $b_i(K) = \dim_{\mathbb{Z}/2\mathbb{Z}} H^i(K)$.

Example 39. Let $K_0 = \{[0],[1],[2],[3]\}$, $K_1 = \{[0,1],[0,2],[1,2],[1,3],[2,3]\}$, $K_2 = \{[0,1,2]\}$. The "picture" of K is a filled in triangle and a non-filled triangle which share a common edge. To compute $H^0(K)$, we need to compute $H^0(C^\bullet(K)) = ker\delta^0/im\delta^{-1} \simeq \ker \delta^0$. Let $\varphi \in C^0(K)$ and suppose that $\varphi \in \ker \delta^0$. Then φ must be constant on all the vertices of K since in our example all the vertices K_0 belong to a single connected component of K. Thus, $\dim ker\delta^0 = 1$, and in general $\dim kder\delta^0$ is the number of connected components of K and has basis consisting of φ_i which takes the value 1 on the i-th connected component of K and takes the value 0 elsewhere.

Definition 23.3. Let $S \subset R^k$ be a closed and bounded semi-algebraic set. Then we define $H^i(S) = H^i(K)$ where K is some simplicial complex coming from a triangulation of S. The next theorem says that since (the isomorphism type of) homology groups are invariant under homomorphism types this definition is well defined.

Theorem 66. *The isomorphism classes of the groups $H^i(S)$ do not depend on the particular semi-algebraic triangulation $h : |K| \to S$.*

Consider two finite simplicial complexes K, K' and compare $|K|, |K'|$ the polyhedrons in some real space. If $|K|, |K'|$ are homeomorphic then $H^*(K) \simeq H^*(K')$, but this is tricky to prove.

24 Day 24, April 20

Last time: we've defined, for a closed and bounded semi-algebraic set S, the homology groups $H^i(S, \mathbb{Z}/2\mathbb{Z})$ with coefficients in $\mathbb{Z}/2\mathbb{Z}$, which are by definition vector spaces over $\mathbb{Z}/2\mathbb{Z}$. The i-th (*mod* 2) betti number $b_i(S; \mathbb{Z}/2\mathbb{Z}) = \dim_{\mathbb{Z}/2\mathbb{Z}} H^i(S, \mathbb{Z}/2\mathbb{Z})$ which is the dimension of this vector space. Geometrically, these betti numbers give you the "number of i-dimensional holes" in S, and in particular the value of $b_0(S, \mathbb{Z}/2\mathbb{Z})$ is the number of semi-algebraic connected components of S.

We needed to triangulate S in order to talk about the homology group. We had explicit maps on simplices, namely the boundary map, for which we needed to assume that S was triangulable (for which we invoked a theorem). Recall that for a triangulation $h : |K| \to S$ we had $H^i(S, \mathbb{Z}/2\mathbb{Z}) \simeq H^i(K, \mathbb{Z}/2\mathbb{Z})$ which is a quotient of a subspace of $C^i(K)$. In particular, $\dim C^i(K)$ is the number of i-simplices in K, which implies that $b_i(S) \leq \#\{i - \text{simplices in a triangulation of } S\}$.

Example 40. We compute the betti numbers of the sphere.

For $S^{n-1} = \{(x_1, \ldots, x_n) |\ x_1^2 + \ldots x_n^2 = 1\}$, we have

$$H^i(S^{n-1}) \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{for } i = 0, n-1$$
$$H^i(S^{n-1}) \simeq 0 \qquad\qquad \text{otherwise .}$$

Example 41. For the n-fold product of the circle, $\underbrace{S^1 \times S^1 \times \cdots \times S^1}_{n\text{-times}}$ the n-dim torus, we have

$$b_i(S^1 \times S^1 \times \cdots \times S^1) = \binom{n}{i}.$$

Example 42. For the ball $B^n = \{(x_1, \ldots, x_n) |\ x_1^2 + \cdots + x_n^2 \leq 1\}$ we have $H^0(B^n) = \mathbb{Z}/2\mathbb{Z}$ and $H^i(B^n) = 0$ for $i \neq 0$.

For the above examples, if you don't already know these results from topology then you should compute them using a triangulation of the space in question and the definitions.

Theorem 67. *The simplicial co-homology groups of closed and bounded semi-algebraic sets are invariant under semi-algebraic homotopy equivalence.*

In the above, a semi-algebraic homotopy H between semi-algebraic maps $f, g : X \to Y$ is a semi-algebraic and continuous map $H : X \times [0,1] \to Y$ such that $H(\cdot, 0) = f$ and $H(\cdot, 1) = g$. We write $f \underset{s.a.}{\sim} g$ and say that f is homotopic to g. Say that two spaces X, Y are semi-algebraically homotopy equivalent if there are maps $X \xrightarrow{f} Y$, $Y \xrightarrow{g} X$ such that $g \circ f \underset{s.a.}{\sim} Id_X$ and $f \circ g \underset{s.a.}{\sim} Id_Y$.

24.1 The Mayer-Vietoris sequence

The Mayer-Vietoris sequence is an algebraic *code-ification* of the information about $X_1 \cup X_2$ based on $X_1, X_2, X_1 \cap X_2$. For example, two spaces X_1, X_2 which are themselves homotopy equivalent to a point may have a complicated union, but somehow this information can be encoded based on X_1, X_2 and $X_1 \cap X_2$.

Definition 24.1. An exact sequence of vector spaces is a complex of vector spaces

$$\cdots \to V_i \xrightarrow{\varphi_i} V_{i+1} \xrightarrow{\varphi_{i+1}} V_{i+2} \to \cdots$$

such that $ker\varphi_{i+1} = Im\varphi_i$ for each i. Note that in homology this definition is equivalent to $H^i = 0$ for all i.

Proposition 68. *For an exact sequence of vector spaces*

$$\cdots \to V_i \xrightarrow{\varphi_i} V_{i+1} \xrightarrow{\varphi_{i+1}} V_{i+2} \to \cdots$$

we have $\dim V_{i+1} \leq \dim V_i + \dim V_{i+2}$.

Proof. We have

$$\begin{aligned} \dim V_{i+2} \geq \dim \varphi(V_{i+1}) &= \dim(V_{i+1}) - \dim \ker \varphi_{i+1} \\ &= \dim V_{i+1} - \dim Im\varphi_i \\ &\geq \dim V_{i+1} - \dim V_i, \end{aligned}$$

from which the result follows.

□

Proposition 69. *For an exact sequence of vector spaces which is bounded on both sides (by zeros), and such that each of the dimensions* $\dim V_i < \infty$*, then we have* $\sum_i \dim(V_i) = 0$.

It is not hard to see the following equivalences based on the definition of exactness:

$$\begin{aligned} 0 \to V_1 \xrightarrow{\varphi} V_2 \text{ is exact } &\iff \varphi \text{ is an injection} \\ V_1 \xrightarrow{\varphi} V_2 \to 0 \text{ is exact } &\iff \varphi \text{ is a surjection} \end{aligned}$$

We also need to discuss the notion of homomorphisms of vector space complexes. For two complexes $C^\bullet, D^\bullet$ with boundary maps δ, δ',

$$\begin{array}{ccccc} C^i & \xrightarrow{\delta} & C^{i+1} & \xrightarrow{\delta} & C^{i+2} \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ D^i & \xrightarrow{\delta'} & D^{i+1} & \xrightarrow{\delta'} & D^{i+2} \end{array}$$

we say that $\phi : C^\bullet \to D^\bullet$ is a morphism of complexes if $\phi_i : C^i \to D^i$ is a vector space homomorphism such that every square above commutes.

Theorem 70 (Snake Lemma)**.** *A short exact sequence of complexes*

$$0 \to C^\bullet \xrightarrow{\phi} D^\bullet \xrightarrow{\psi} E^\bullet \to 0$$

gives rise to a long exact sequence of cohomology groups, namely

$$H^i(C^\bullet) \xrightarrow{\phi_*} H^i(D^\bullet) \xrightarrow{\psi_*} H^i(E^\bullet) \xrightarrow{d} H^{i+1}(C^\bullet) \to H^{i+1}(D^\bullet) \to \cdots .$$

This version of the snake lemma is based on another version which is probably more used in commutative algebra.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & ker(p) & \longrightarrow & ker(q) & \longrightarrow & ker(r) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle r} & & \\ 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & coker(p) & \longrightarrow & coker(q) & \longrightarrow & coker(r) & \longrightarrow & 0 \end{array}$$

The conclusion of the snake lemma is the existence of $\delta : \ker r \to coker(p)$ a connecting map (map not shown above).

Let K be a simplicial complex and suppose that $K = K_1 \cup K_2$. Let $C^\bullet(K)$, $C^\bullet(K_1)$, $C^\bullet(K_2)$, $C^\bullet(K_1 \cap K_2)$ denote the respective complexes of cochain groups. We have restriction maps

$$C^\bullet(K) \xrightarrow{r_1} C^\bullet(K_1) \xrightarrow{s_1} C^\bullet(K_1 \cap K_2)$$

and

$$C^\bullet(K) \xrightarrow{r_2} C^\bullet(K_2) \xrightarrow{s_2} C^\bullet(K_1 \cap K_2).$$

It turns out that this gives rise to the short exact sequence

$$0 \longrightarrow C^\bullet(K) \xrightarrow{r_1 \oplus r_2} C^\bullet(K_1) \oplus C^\bullet(K_2) \xrightarrow{s_1 + s_2} C^\bullet(K_1 \cap K_2) \longrightarrow 0.$$

Thus, the Mayer-Vietoris long exact sequence is given (using the snake lemma).

$$\begin{aligned} \cdots \to H^{i-1}(X_1 \cap X_2) \to H^i(X) \to H^i(X_1) \oplus H^i(X_2) \to H^i(X_1 \cap X_2) \\ \to H^{i+1}(X) \to H^{i+1}(X_1) \oplus H^{i+1}(X_2) \to \cdots \end{aligned}$$

We have the following immediate inequality.

$$b_i(X) \leq b_i(X_1) + b_i(X_2) + b_{i-1}(X_1 \cap X_2)$$

What happens when there is more than one set in the union? Suppose $X = X_1 \cup \cdots \cup X_s$. In fact, we would require *spectral sequences* to analyze this example satisfactorily. But, the inequality in the general case is given below, while the justification is not given here.

$$b_i(X) \leq \sum_{j_1} b_i(X_{j_1}) + \sum_{j_1<j_2} b_{i-1}(X_{j_1} \cap X_{j_2}) + \sum_{j_1<j_2<j_3} b_{i-2}(X_{j_1} \cap X_{j_2} \cap X_{j_3}) + \dots$$

25 Day 25, April 22

We need to cover a little more material before we can achieve our goal: to give effective bounds on topological properties of semi-algebraic sets. The first thing we will cover is the Hardt triviality theorem.

25.1 Hardt triviality

The following theorem is very important in practice. The theorem says that semi-algebraic maps can be "trivialized" in some sense.

Definition 25.1. Let $f : X \to Y$ be a semi-algebraic map. Say that f is trivial over a semi-algebraic subset $Y_i \subset Y$ if there exists

$$F_i : f^{-1}(y_i) \times Y_i \overset{s.a.\ homeo}{\to} f^{-1}(Y_i)$$

satisfying $f \circ F_i(\cdot, y) = y$ for all $y \in Y_i$ (which says that F_i is *fiber preserving*)

Theorem 71 (Hardt triviality)**.** *Suppose $f : X \to Y$ is a semi-algebraic map. Then, there exists a finite, semi-algebraic partition of Y into semi-algebraic sets $Y = \cup_{i\in I} Y_i$ such that f is trivial over each Y_i. Furthermore, the sets Y_i can be chosen to be locally closed.*

This is an extremely important theorem. The proof is by induction on the dimension of the semi-algebraic set, but we omit the proof here and refer the reader to **??**, for example. This theorem has an important immediate corollary, namely the finiteness of topological types of fibers $f^{-1}(y), y \in Y$.

Corollary 72 (Finiteness of homeomorphism types)**.** *The number of semi-algebraic homeomorphism types amongst the fibers $f^{-1}(y), y \in Y$ is finite (and less than or equal to the cardinality $|I|$ in the theorem).*

Some other very important consequences of Hardt triviality are the so-called conical structure at a point and conic structure at infinity of semi-algebraic sets.

Corollary 73 (Conic structure at a point)**.** *Let S be a semi-algebraic set and $p \in S$. For all $r > 0$ small enough, the intersection of the closed ball $\overline{B_k(p,r)} \cap S \underset{s.a.}{\cong} cone(S^{k-1}(p,r) \cap S)$ is isomorphic to the cone with base $S^{k-1}(p,r) \cap S$.*

Proof. Suppose $S \subset R^k$ and suppose $p = 0$. Let $T \subset R^k \times R$ be defined by $T = \{(x, ||x||) |\ x \in S\}$. Let $f : T \to R_{\geq 0}$ be defined by $f(x, ||x||) = ||x||$. By Hardt triviality, f can be trivialized. In particular, there exists r_0 such that the map f is trivial over $(0, r_0) \subset R_{\geq 0}$. By taking r_0 slightly smaller, there exists a map $F : S \cap \overline{S^{k-1}(0,r_0)} \times (0, r_0] \to S \cap \overline{B_k(0,r_0)}$–$\{0\}$. By the fiber preserving property of F, this map can be extended to include the origin:

$$F : S \cap S^{k-1}(0, r_0) \times [0, r_0] \to S \cap \overline{B_k(0,r_0)}\text{–}\{0\}.$$

□

Corollary 74 (Conic structure at infinity)**.** *Let S be semi-algebraic. Then, there exists $r_0 > 0$ and a fiber preserving semi-algebraic homeomorphism $S \cap \{x|\ ||x|| > r_0\} \to S \cap S^{k-1}(0, r_0) \times (r_0, infty)$.*

What follows is another consequence of Hardt triviality.

Corollary 75. *Let $P \in R[X_1, \ldots, X_k]$ such that $Z(P, R^k)$ is closed and bounded. Let $V \subset R\langle\varepsilon\rangle^k$ be the basic semi-algebraic set defined by $V := \{x|\ P^2(x) \leq \varepsilon\}$. Then, $Z(P, R\langle\varepsilon\rangle^k)$ is semi-algebraically homotopy equivalent to V.*

The above corollary allows one to replace a singular real algebraic set with a non-singular real algebraic set by adding an infinitesimal. The benefit of this is examined in the next section.

25.2 Morse theory for non-singular hyper-surfaces

Unless otherwise stated, for this section we let V denote $V \subset R^k$ a closed, bounded non-singular real algebraic hyper-surface. Also, $f : V \to R$ is a map which has non-degenerate critical points. For an example, the non-degenerate critical point of $g : R \to R$ are the x-values for which $g'(x) = 0$ and $g''(x) \neq 0$. In a more general context, if we have a map $g : M^m \to N^n$ between m and n-dimensional manifolds, then the derivative of g can be visualized as the closest approximation to g by a linear map. We have, associated to M and N respectively, the tangent spaces $T_pM, T_{f(p)}N$ at p and $f(p)$ respectively, and the point p is critical if the derivative $df_p : T_pM \to T_{f(p)}N$ (which is a linear map of f.d. vector spaces) does not have the maximal rank. In our context, $f : V \to R$ has derivative $df_p : T_pV \to R$ which does not have full rank if and only if it is the zero map (in this context this means that $df_p(T) = \{f(p)\}$). A critical point is said to be non-degenerate if the second derivative has full rank, and is said to be degenerate otherwise. In the context we are considering (when the map f is a projection onto a coordinate), the second derivative can be associated to the Hessian matrix. We summarize the above in the following:

$$\begin{aligned} p \text{ is not a critical point:} &\quad \left[\frac{\partial f}{\partial x_i}\right]_{1\leq i\leq n} \neq \vec{0} \\ p \text{ is a non-degenerate crit point:} &\quad \left[\frac{\partial^2 f}{\partial x_j \partial x_i}\right]_{1\leq i,j\leq n} \text{ is non-singular} \end{aligned}$$

Denote by $V_{\leq a}$ the set $V_{\leq a} = V \cap \{f \leq a\}$, and denote by $V_a = V \cap \{f = a\}$.

Lemma 9 (Morse Lemma A)**.** *Let $a_1 < a_2 < \cdots < a_N$ be the critical values of f and $a_i \leq c < a_{i+1}$. Then, $V_{\leq c}$ is semi-algebraically homotopy equivalent to $V_{\leq a_i}$.*

The first Morse Lemma above says that nothing *important* happens between critical values of f.

26 Day 26, April 27

We are discussing the Morse Lemma. Let $crit f|_M = \{x \in M|\ df_x = 0\}$ be the set of critical points of f, and suppose that the critical values are $v_1 < v_2 < \cdots < v_N$. Then, the following holds.

Lemma 10 (Morse Lemma A)**.** *For $c \in [v_i, v_{i+1})$ we have $M_{\leq c}$ is semi-algebraically homotopy equivalent to $M_{\leq v_i}$, where $M \leq x = M \cap f^{-1}((-\infty, x])$.*

The above can be thought of as follows. If you are discovering a surface by "scanning" it using a wall (or plane), then the above says that nothing "interesting" happens between critical levels. Let us examine a critical point at the origin. Then the graph of $y = \varphi(x_1, \ldots, x_k)$ is locally the surface, and the point 0 is a critical point provided $\frac{\partial \varphi}{\partial x_1}(0) = \cdots = \frac{\partial \varphi}{\partial x_k}(0) = 0$. Furthermore, the point is non-degenerate if the hessian matrix $Hess(\varphi)(0) = [\frac{\partial^2 \varphi}{\partial x_i \partial x_j}(0)]_{1\leq i,j\leq k}$ is invertible. Let $index(Hess(\varphi)(0)) = \ell$ be the number of negative eigenvalues of this matrix. We have the following result from calculus.

Theorem 76. *There exists a smooth change of coordinates $y_1(x_1, \ldots, x_k), \ldots, y_k(x_1, \ldots, x_k)$ such that $\varphi(y_1, \ldots, y_k) = y_1^2 + \cdots + y_{k-\ell}^2 - (y_{k-\ell+1}^2 + \cdots + y_k^2)$.*

Proof. For the invertible and real-symmetric matrix $Hess(\varphi)(0)$, we have a linear change of coordinates (P, Q for which P makes $Hess(\varphi;0)$ into a diagonal matrix and Q scales the diagonal entries to be ± 1) such that after the linear change of coordinates the $Hess(\varphi)(0)$ is diagonal and of the following form having only ± 1 as diagonal entries, with positive entries in the upper entries and negative entries in the lower entries.

In the neighborhood U, we have

$$\varphi(x_1,\dots,x_k) = \sum_{i=1}^{k} x_i \int_0^1 \frac{\partial \varphi}{\partial x_i}(tx_1,\dots,t_xk)\ dt \quad = \sum_{i,j=1}^{k} \int_0^1 \int_0^1 \frac{\partial^2 \varphi}{\partial x_i \partial x_j}(stx_1,\dots,stx_k)\ ds\ dt$$

Define

$$M(x_1,\dots,x_k) = \left[\int_0^1 \int_0^1 \frac{\partial^2 \varphi}{\partial x_i \partial x_j}(stx_1,\dots,stx_k)\ ds\ dt\right]_{1\le i,j\le k}$$

Note that $M(0) = Hess(\varphi)(0)$. In a small enough neighborhood U of 0, there is an orthogonal matrix $N(X)$ such that $N(X)^T M(X) N(X) = Hess(\varphi)(0)$, now set $Y = N(X)^{-1}X$. Now, we have that $\varphi(X) = X^T MX = (NY)^T MNY = Y^T N^T MNY = Y^T Hess(\varphi)(0)Y$, as desired.

□

Now, suppose a surface M is given by the equation $\varphi(Y) = y_1^2 + \cdots + y_{k-\ell}^2 - (y_{k-ell+1}^2 + \cdots + y_k^2)$. Then $M \le 0$ is homotopy equivalent to $M_{\le -\varepsilon} \cup_{S^{\ell-1}(\varepsilon)} \overline{B}_\ell(\varepsilon)$.

Lemma 11 (Morse Lemma B)**.** *The homotopy type of $M_{\le v_i}$ is $M_{\le v_i - \varepsilon} \cup_{S^{\ell-1}(\varepsilon)} \overline{B}_\ell(\varepsilon)$ for small $\varepsilon > 0$ and ℓ the index of the critical point v_i.*

By Mayer-Vietoris, (remember in cohomology the union goes to the sum goes to the intersection)

$$\cdots H^{i-1}S^{\ell-1} \to H^i(M \le 0) \to H^i(M_{\le -\varepsilon}) \oplus H^i(\overline{B}_\ell) \to H^i(S^{\ell-1}) \to \cdots$$

We then have the following based on the above exact sequence and the group $H^i(B_j), H^i(S^j)$ for chosen i, j. For $i \ge \ell + 1$, $H^i(M_{\le 0}) \cong H^i(M_{\le -\varepsilon})$. For $0 < i < \ell - 1$, $H^i(M_{\le 0}) \cong H^i(M_{\le -\varepsilon})$. Analyzing the cases $i = 0, i = \ell, i = \ell - 1$ we obtain the following result: either $b_\ell(M_{\le 0}) = b_\ell(M_{\le -\varepsilon}) + 1$ and the other betti numbers stay the same, OR $b_{\ell-1}(M_{\le 0}) = b_{\ell-1}(M_{\le -\varepsilon}) - 1$ and the other betti numbers stay the same. This tells you a lot about the topology of the surface. For example, if M is a compact hypersurface then the sum of the betti numbers is at most the number of critical points:

$$\sum_i b_i(M) \le \#\text{ of critical points of a morse function on } M.$$

Theorem 77. *Let R be a real closed field and $P \in R[X_1,\dots,X_k]$, with $\deg P \le d$ and $Z(P, R^k)$ a non-singular, bounded hypersurface. Then, $\sum_i (Z(P, R^k)) \le d(d-1)^{k-1}$.*

Proof. First, assume that $R = \mathbb{R}$. Choose coordinates such that the projection onto the X_1-coordinate is a morse function (a perhaps unremarkable result which we state here but do not prove, see BCR for proof **??**). The critical points of the projection on the X_1-coordinate restricted to $Z(P, R^k)$ are points in R^k which satisfy $P = \frac{\partial \varphi}{\partial x_2} = \cdots = \frac{\partial \varphi}{\partial x_k} = 0$.

Lemma 12 (Bezout's Theorem)**.** *If $P_1,\dots,P_k \in \mathbb{C}[X_1,\dots,X_k]$ of degrees $d_1,\dots,d_k$, then the number of isolated complex, common zeros is at most $d_1 \cdot d_2 \cdots d_k$.*

In this case, it turns out, that the number of real solutions is bounded by the number of complex solutions, which in turn is bounded by Bezout's Theorem. Hence, the number of real solutions is at most $d(d-1)^{k-1}$ as desired.

Finally, by the Tarski-Siedenberg transfer principle (and very careful construction of a first order sentence!) we get the analogous result over arbitrary real closed fields R.

□

The statement of Bezout's Theorem is false when you replace $\mathbb{C}$ with $\mathbb{R}$ as a following example will show. Basically, the fallacy is that an isolated real solution need not come from an isolated complex solution. For example, consider $P_1 = ((x-1)(x-2)(x-3))^2 + ((y-1)(y-2)(y-3))^2$ and $P_2 = z$ and $P_3 = z$. There are 9 isolated zeros to $P_1 = P_2 = P_3 = 0$, and the product of the degrees is 6.

The last lecture will be dedicated to removing the assumption that the semi-algebraic set in the previous theorem was non-singular and bounded.

Theorem 78. *If $P_1, \ldots, P_\ell \in R[X_1, \ldots, X_k]$ are polynomials of degree at most $\deg P_i \leq d$ then $\sum_i b_i(Z(\{P_1, \ldots, P_\ell\}, R^k)) \leq d(2d-1)^{k-1}$.*

27 Day 27 (Last Day), April 29

Theorem 77. *Let $Q \in R[X_1, \ldots, X_k]$ and suppose $\deg Q = d$. Suppose further that $Z(Q, R^k)$ is bounded and non-singular, then $\sum_i b_i(Z(Q, R^k)) \leq d(d-1)^{k-1}$.*

We now try to remove the requirement that $Z(Q, R^k)$ is bounded and non-singular. That is, our last goal is to prove the following.

Theorem 78. *Let $\mathcal{P} = \{P_1, \ldots, P_s\} \subset R[X_1, \ldots, X_k]$, $\deg P_i \leq d$. Then $\sum_i b_i(Z(\mathcal{P}, R^k)) \leq d(2d-1)^{k-1}$.*

Proof. Let $Q = P_1^2 + \cdots + P_s^2$, so that $\deg Q \leq 2d$. Note that $Z(\mathcal{P}, R^k) = Z(Q, R^k)$. We need to reduce to the case that $Z(Q, R^k)$ is non-singular. To that end, as in previous arguments, we introduce infinitesimals. Let $0 < \varepsilon << \frac{1}{\Omega} << 1$, and consider the extension $R\langle \frac{1}{\Omega}, \varepsilon \rangle$. Consider the polynomial $Q_1 = Q + \varepsilon(|x|^2 - \Omega)$ and the semi-algebraic set $W \subset R\langle \frac{1}{\Omega}, \varepsilon \rangle^k$ defined by $Q_1 \leq 0$. Notice that outside the ball of radius Ω the inequality $Q_1 \leq 0$ can not be satisfied. After examining Q_1 where ε is though of as being very small, we see that W is infinitesimally close to the intersection of $\{Q = 0\}$ with the ball of radius Ω. It then follows from Hardt triviality theorem (and its corollaries) that $\lim_\varepsilon W$ is semi-algebraically homotopy equivalent to $Z(Q, R\langle \frac{1}{\Omega} \rangle^k) \cap \overline{B_k(0, \Omega)}$, which (by the conical structure at infinity theorem) is homeomorphic to $Z(Q, R\langle \frac{1}{\Omega} \rangle^k)$ itself. Finally, using the transfer principle, the betti numbers of the extension $Z(Q, R\langle \frac{1}{\Omega} \rangle^k)$ are equal to those of $Z(Q, R^k)$ itself. Therefore, it suffices to bound $\sum_i b_i(W)$ the sum of the betti numbers of W.

We have that W is bounded by $Z(Q_1, R\langle \frac{1}{\Omega}, \varepsilon \rangle^k)$ and that $Z(Q_1, R\langle \frac{1}{\Omega}, \varepsilon \rangle^k)$ is non-singular. We can then apply the previous theorem to $Z(Q_1, R\langle \frac{1}{\Omega}, \varepsilon \rangle^k)$, but we still need to relate this to W. By Alexander duality (ref?), can bound the sum of betti numbers of W by $\sum b_i(W) \leq \frac{1}{2} \sum b_i(\partial W)$, and hence by $\sum b_i(W) \leq \frac{1}{2} \cdot 2d(2d-1)^{k-1} = d(2d-1)^{k-1}$, as desired.

□

One might ask how good these bounds are. Are there really semi-algebraic sets that have betti numbers this high? The answer is: sort of, yes. For example, consider $Q = \sum_{i=1}^k [(x_i - 1) \cdots (x_i - d)]^2$ which has $b_0(Z(Q, R^k)) = d^k$, and $\deg Q = 2d$. The bound from above would yield a bound of $2d(2d-1)^{k-1}$, which is off by a factor of around 4^k. But, at least this gives an example of an exponentially growing b_0 first betti number. As another example, we could look at $Q_1 = Q - \varepsilon$ and then we have $b_0 = d^k$ and $b_{k-1} = d^k$, and hence $\sum b_i \leq 2d^k$, which is a little closer to the upper bound (??).

We could ask the following question.

PROBLEM: Let $\mathcal{P} = \{P_1, \ldots, P_s\} \subset R[X_1, \ldots, X_k]$, with $\deg P_i \leq d$. Each sign condition $\sigma \in \mathcal{P}^{\{-1,0,1\}}$ gives a semi-algebraic subset of R^k, and R^k is partitioned by the non-empty realizations of these sign conditions. Let $F(s, k, d)$ be the maximum number of connected components of realizations of realizable sign conditions on collections of $\mathcal{P} \subset R[X_1, \ldots, X_k]$ with $|\mathcal{P}| = s$ and $\deg P \leq d$ for all $P \in calP$. What is an upper bound on $F(s, k, d)$? Let us first consider $F(s, k, 1)$, which is asking how many connected regions can you have in R^k if you have s hyperplanes. Even easier, when $k = 1$ we have $F(s, ki, 1) = s + 1$. If

$k = 2$, then $F(s, 2, 1) = F(s-1, 2, 1) + F(s-1, 1, 1)$ which is interpreted as when I add a s-th line to $s-1$ lines in general position (in R^k), then you add s more regions, and $s = F(s-1, 1, 1)$. In general, $F(s, k, 1) = F(s-1, k, 1) + F(s-1, k-1, 1)$. This looks like the recurrence for binomial coefficients, but we need to be careful and consider the initial conditions. We have $F(s, 1, 1) = s + 1$ and $F(1, k, 1) = 2$, and so the solution for the recurrence is $F(s, k, 1) = \sum_{i=0}^{k} \binom{s}{i}$.

Lets try to find a lower bound on $F(s, d, k)$. For each polynomial $P_i \in \mathcal{P}$, we can replace $P_i = L_{i,1} \dots L_{i,d}$ with the product of linear polynomials (hyperplanes) to reduce to the previous case. Then $\sum_{i=0}^{d} \binom{sd}{i} \leq F(s, k, d)$. For very large s, Stirling approximation of factorial gives an approximation of the sum as $(\frac{esd}{k})^k$. It turns out that you can define the betti numbers for any semi-algebraic set and that for our case we have $b_0(R^k - \cup_{P \in \mathcal{P}} Z(P, R^k))$ is related, by Alexander duality, to

$$b_0(R^k - \cup_{P \in \mathcal{P}} Z(P, R^k)) = b_{k-1}(\cup_{P \in \mathcal{P}} Z(P, R^k)).$$

From Mayer-Vietoris,

$$b_{k-1}(\cup_{P \in \mathcal{P}} Z(P, R^k)) \leq 1 + \sum_{1 \leq i \leq s} b_{k-1}(Z(P, R^k)) + \sum_{1 \leq i < j \leq s} b_{k-2} Z(\{P_i, P_j\}, R^k) + \cdots + \sum_{1 \leq i_1 < \cdots < i_k \leq s} b_0(Z(\{P_1, \dots, P_{i_k}\}, R^k)).$$

Using the bounds from before, we have

$$b_{k-1}(\cup_{P \in \mathcal{P}} Z(P, R^k)) \leq 1 + (\binom{s}{1} + \binom{s}{2} + \cdots + \binom{s}{k}) d(2d-1)^{k-1},$$

which can be approximated (and makes the bound looser) by

$$\sum_{i=0}^{k} \binom{s}{i} d(2d-1)^{k-1}.$$

To conclude, we have shown upper and lower bounds on $F(s, d, k)$ to be

$$\sum_{i=0}^{k} \binom{sd}{i} \leq F(s, k, d) \leq \sum_{i=0}^{k} \binom{s}{i} d(2d-1)^{k-1}.$$

It is not known which of these (if either) is tight. It would be a nice question to solve, to decide (for example) if the construction using products of hyperplanes is the worst possible. (???)

A lot of the questions that arise can be answered using "cylindrical algebraic decomposition". A cylindrical decomposition of R^k adapted to a particular semi-algebraic subset $S \subset R^k$ is a decomposition of R^k into graphs and bands of semi-algebraic, continuous functions defined over "cells" (of a decomposition of R^{k-1}) such that the graphs and bands are "adapted" to the semi-algebraic set S; that is, each graph and band is either contained or disjoint from S.

This is very important, and the importance arises from the fact that this can be done *effectively*. You can actually obtain descriptions of the cells of the decomposition. The number of cells in a decomposition is of the order $(sd)^{2^k}$, which is double exponential. It turns out that this is actually an upper bound on the sum of the betti numbers of the semi-algebraic set S, however notice that this double exponential bound is much worse than the previous bound (*i.e.*, Morse theory is better).

The other use of cylindrical decomposition is to answer questions about eliminating quantifiers. The cylindrical structure of the cylindrical decomposition allows one to decompose, say, the X-axis into cells over which the number of different signs that the polynomial can attain stays fixed. This allows one to answer questions in existential theory (with one block of quantifiers), and even allows one to (effectively) eliminate *blocks* of quantifiers.

It turns out that quantifier elimination is *inherently* doubly exponential, so there is not any way to get a cylindrical decomposition which has a much better bound. There are other types of decompositions that are not cylindrical, however, which have better bounds. In modern approaches, however, the "critical point method" used in the Morse theory section is generally used due to the benefits of the single exponential bound.

Index

References

[1] Saugata Basu, Richard Pollack, and Marie-François Roy. *Real Algebraic Geometry.* Springer, 2006. 1

[2] Jacek Bochnak, Michel Coste, and Marie-François Roy. *Real Algebraic Geometry.* Springer, 1998. 1

[3] Murray Marshall. *Positive Polynomials and Sums of Squares.* American Mathematical Society, 2008. 1