Spaces of orderings of semigroups

Jennifer Chubb

George Washington University

Logic/Topology Seminar
March 21, 2006

Outline

1. **Introduction**
   - Ordering semigroups
   - The topological space $\mathtt{LO}(G)$
2. **Topology**
   - Cantor space
   - Gröbner bases
3. **Computability**
   - Definitions and terminology
   - Results

Outline

Basic Definitions

Let G be a semigroup (a set with associative operation).

Definition

A linear ordering, $<$, on the elements of G is a *left ordering of G* if it is preserved under left multiplication. That is, for $a, b, c \in G$ we have

$$a < b \Rightarrow ca < cb.$$

Right-orderings are defined similarly.

Definition

An ordering is a *bi-ordering of G* if it is both a left and right ordering of G.

Easy Observations

Definition

A semigroup is called *left-orderable (bi-orderable)* if it admits a left ordering (a bi-ordering).
Let $\mathtt{LO}(G)$ be the set of all left orders of the semigroup G.

- Left-orderable abelian semigroups are bi-orderable.
- If G is a left-orderable semigroup, then G is not finite.
- Every left-orderable group is right-orderable.

The subbasis topology, τ.

- For $a, b \in G$ we define $U_{a,b} = \{<\in \mathrm{LO}(G) | a < b\}$.
- Let τ be the smallest topology on $\mathrm{LO}(G)$ containing $\{U_{a,b}\}_{a,b\in G}$.

Observation

This collection is a subbasis, so every open set is a *union of sets* of the form

$$U_{a_1,b_1} \cap U_{a_2,b_2} \cap \ldots \cap U_{a_n,b_n}.$$

The metric topology, τ'.

Alternatively, we can define a topology using a metric.

1. Let $\emptyset = G_0 \subset G_1 \subset G_2 \ldots$ be a filtration of G by finite subsets with $\bigcup_i G_i = G$.
2. For $<_1$ and $<_2$ in $\mathtt{LO}(G)$, we define

$$d(<_1, <_2) = \frac{1}{2^r}, \text{ where } r = \max\{i \mid <_1 \ \& \ <_2 \text{ agree on } G_i\},$$

   and set $d(<_1, <_2) = 0$ if $r = \infty$ (that is if $<_1$ and $<_2$ agree on all G_i).
3. Let τ' be the corresponding metric topology.

(It is easy to check that d really is a metric.)

Proposition

These topologies are identical, that is, $\tau = \tau'$.

Proof.

1. For set $V = U_{a_1,b_1} \cap \ldots \cap U_{a_n,b_n}$ and any $< \in V$, there is r so that $B(<, 1/2^r)$ is contained in V.
   - Choose i so that all of $\{a_j, b_j\}_{j=1..n}$ are in G_i.
     Let r be this i.
2. For each $B = B(<, 1/2^r)$ and any $<_1 \in B$ there is an element of τ containing $<_1$ that is a subset of B.
   - $<$ and $<_1$ must agree on G_{r+1}, so in fact we have

$$B = \bigcap_{a,b \in G_{r+1}} U_{a,b}.$$

So, the topology is independent of the choice of filtration!

Properties of the space

Theorem

$\mathrm{LO}(G)$ *is compact and totally disconnected.*

Proof.

- Totally disconnected:
  – If $<_1 \neq <_2$, then there are $a, b \in G$ so that $<_1 \in U_{a,b}$ and $<_2 \in U_{b,a}$.
- Compact:
  – Let $\{<_1, <_2, \dots\}$ be a sequence in $\mathrm{LO}(G)$. We show it has a convergent subsequence.

Properties of the space

Proof. cont.

Let $\mathcal{S}_0 =_{def} \{<_1^0, <_2^0, \dots\}$ be a subsequence of orders that agree on G_0. G_0 is finite!

Recursively, let $\mathcal{S}_{i+1} =_{def} \{<_1^{i+1}, <_2^{i+1}, \dots\}$ be a subsequence of orders from $\mathcal{S}_i$ that agree on G_{i+1}.

Let $\mathcal{S} =_{def} \{<^i\}_{n\in\omega}$, where $<^i$ is the ith term in S_i.

Claim. $\mathcal{S}$ converges to an order, $<^\infty$, given by

$$a <^\infty b \Leftrightarrow \text{For a.e. } n, a <^n b.$$

Proof of Claim. $d(<^n, <^\infty) \leq \frac{1}{2^n}$. □

Outline

Reminders and observations

- Recall that Cantor space can be thought of as 2^ω with the usual topology derived from the tree $2^{<\omega}$.
- A topological space is homeomorphic to the Cantor space exactly when it is totally disconnected, compact, metrizable, and perfect (ie. every point is a limit point).
- $\mathtt{LO}(G)$ is totally disconnected, compact, and metrizable.
- When is it perfect?

When is $\mathtt{LO}(G)$ perfect?

- $\mathtt{LO}(\mathbb{Z}^n)$ is for $n \geq 2$.
- $\mathtt{LO}(\mathbb{Z}^\infty)$ is. ???
- It is unknown whether the free group with $n > 1$ generators, F_n, has $\mathtt{LO}(F_n)$ perfect.
- For *groups* satisfying certain additional criteria, a subcollection of their bi-orders is homeomorphic to the Cantor space.

$\mathrm{LO}(\mathbb{Z}^2)$

- $\mathrm{LO}(\mathbb{Z}^n)$ is homeomorphic to the Cantor space for all $n \geq 2$. We'll see the idea for the proof for $n = 2$.
- Observe that $\mathrm{LO}(G)$ is perfect if and only if all sets of the form

$$U_{a_1,b_1} \cap \ldots \cap U_{a_n,b_n}$$

are always either empty or infinite.
- We'll assume that $\mathrm{LO}(\mathbb{Z}^2)$ is not perfect and obtain a contradiction.

$\mathtt{LO}(\mathbb{Z}^2)$

Theorem

$\mathtt{LO}(\mathbb{Z}^2)$ is homeomorphic to the Cantor space.

Proof idea.

Assume there is $U_{a_1,b_1} \cap \ldots \cap U_{a_n,b_n}$ containing exactly one element, $<$.
Each ordering of $\mathbb{Z}^2$ divides the plane into a positive half and negative half, and so corresponds to a unique ordering on $\mathbb{Z}^2$. ("Positive" here means "$>(0,0)$" in $\mathbb{Z}^2$.) The boundary is a line through the origin.
There are either infinitely many different lines or no lines determining an order for which $a_1 < b_1$, $a_2 < b_2$, and so forth. This contradicts our hypothesis.

□

An application: Gröbner bases

First, a little background...

- Let $K[x_1, \ldots, x_n]$ be a polynomial ring over a field.
- The subcollection of monomials form a monoid (a semigroup also equipped with a unique identity – in this case $x_1^0 x_2^0 \ldots x_n^0 = 1$).
- This monoid of monomials is isomorphic to $\mathbb{Z}^n_{\geq 0}$ via

$$x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \mapsto (i_1, i_2, \ldots, i_n)$$

and we identify them.

Well-orderings of the monoid

Definition

A linear ordering, $<$, of G is a *well-ordering* if and only if each subset of G has an $<$-smallest element. We denote the collection of left well-orderings of G by $\mathrm{LWO}(G)$.

Fact

For $\mathbb{Z}^n_{\geq 0}$, an ordering is a well-ordering if and only if 0 is the least element of $\mathbb{Z}^n_{\geq 0}$ with respect to that order. In other words,

$$\mathrm{LWO}(\mathbb{Z}^n_{\geq 0}) = \mathrm{LO}(\mathbb{Z}^n_{\geq 0}) \setminus \bigcup_{a \neq 0} U_{a,0}.$$

We call $\mathrm{LWO}(\mathbb{Z}^n_{\geq 0})$ the space of *monomial orderings* for the polynomial ring $K[x_1, \ldots, x_n]$.

Properties of the space $\mathtt{LWO}(\mathbb{Z}^n_{\geq 0})$

- $\mathtt{LWO}(\mathbb{Z}^n_{\geq 0})$ is totally disconnected and metrizable.
  - These properties are inherited from $\mathtt{LO}(\mathbb{Z}^n_{\geq 0})$.
- The space is compact.
  - It is a closed subset of a compact space – by the Fact.
- This space is perfect for $n > 1$.
  - We can adapt the reasoning in the proof for all of $\mathbb{Z}^n$.

Okay, great. What does this have to do with Gröbner bases?

What are Gröbner bases?

The basics

- Choose an ordering of monomials from the polynomial ring, $\prec$.
- A polynomial f can be expressed as a linear combination of monomials. Denote by $\mathtt{LM}(f)$ the $\prec$-largest monomial appearing in f, and call this the *leading monomial of* f.
- Let $I \lhd K[x_1, \ldots, x_n]$ be a non-zero ideal in the polynomial ring, and let $\mathtt{LM}(I)$ be the ideal in $K[x_1, \ldots, x_n]$ generated by the leading monomials of elements of I.

Definition

A set of polynomials $\{f_1, \ldots, f_d\} \subset I$ is a *Gröbner basis* of I if their leading monomials generate $\mathtt{LM}(I)$.

The application

Proposition

For any ideal $I \lhd K[x_1, \ldots, x_n]$ and any set of polynomials $f_1, \ldots, f_d \in I$, the set of monomial orderings on $K[x_1, \ldots, x_n]$ for which $\{f_1, \ldots, f_d\}$ is a Gröbner basis is *open*.

The proof of this fact uses some divisibility properties of Gröbner bases.

This, along with compactness of the space of orderings on the monomials, allows us to quickly prove the existence of universal Gröbner bases.

Theorem (Existence of universal Gröbner bases)

For any ideal $I \lhd K[x_1, \ldots, x_n]$ there is a finite set of polynomials $\{f_1, \ldots, f_s\} \in I$ that is a Gröbner basis for I with respect to any monomial ordering.

Proof.

- For $f_1, \ldots, f_s \in I$ let $V_{f_1,\ldots,f_s}$ be the set of orderings for which this collection of polynomials is a Gröbner basis for I.
- By the Proposition, each of these sets is open. They also happen to cover the space of monomial orderings.
- We observed earlier that this space is compact, so there must be a finite subcover, $V_{f_1,\ldots,f_s}, \ldots, V_{g_1,\ldots,g_t}$.
- This collection, $\{f_1, \ldots, f_s\} \cup \ldots \cup \{g_1, \ldots, g_t\}$ is the basis we seek.

□

Outline

The basics

First, everything happens in $\mathbb{N}$, which we call ω.

Definition

A set, function, or relation is called *computable* if there is a computer program that will compute membership, output, and truth values, respectively, for any input.

- We sometimes talk about things like subsets of $\mathbb{Z}$ or a relation on the rationals and say that they are computable. This just means that there is a suitable way to code (maybe using prime numbers or the fundamental theorem of arithmetic) whatever we're talking about so that the information is represented as a subset of ω.

The basics

Definition

A set (or function or relation) A is *Turing reducible to* or *computable in* B, and we write $A \leq_T B$, if when we are given information about B for free, A becomes computable.

Definition

We write $A \equiv_T B$ when $A \leq_T B$ and $B \leq_T A$.
Note that $\equiv_T$ is an equivalence relation on 2^ω. We call the equivalence classes *Turing degrees* and write $\mathtt{deg}(A)$ for $[A]_{\equiv_T}$.

Definition

A group is computable if its universe is computable and the group operation is a computable function.

On the computable strength of orderings of some nice groups

Theorem

A computable torsion free abelian group of rank 1 (think $\mathbb{Z}$) has exactly two orders, both of which are computable.

Theorem

A computable torsion free abelian group of (finite) rank strictly greater than 1 has orders of every Turing degree.

Proof idea.

WLOG, we can assume G is divisible, and for simplicity, assume it has rank 2. Let $\{a, b\}$ be a basis for G and fix a set A of arbitrary Turing degree.

Think of the charactaristic function of A as a binary string representing a real number r. (A non-computable set will necessarily correspond to an irrational number.)

Use the map $f : p_1 a + p_2 b \mapsto p_1 + p_2 r$ to define an order $<_r$ on G,

$$g <_r h \Leftrightarrow f(g) <_{\mathbb{R}} f(h).$$

It can then be shown that the Turing degree of the ordering is the same as that of A.

For details, ask Sarah. □

A little more computability...

We can use algorithms to describe functions that are not necessarily *total*. These functions are called *partial computable functions.*

Facts about $0'$

$0'$, called the halting set, is a non-computable set of natural numbers that codes information about computable functions. In particular, it can answer the question

Is this partial computable function defined at this input?

Theorem

A computable torsion free abelian group of infinite rank has orders of every Turing degree above the halting set.

Note that this suggests that there are computable torsion free abelian groups of infinite rank that do not admit a computable order.

It turns out however, that every such group is isomorphic to a computable group that *does* admit a computable order.

Trees and orderings

These observations lead to a *negative* result that is of interest since the positive version holds for computable fields.

Theorem

There is a computable binary tree, T, so that for any computable torsion free abelian group G we have

$$\{\mathrm{deg}(f) | f \text{ is an infinite path on } T\} \neq$$

$$\{\mathrm{deg}(<) | < \text{ is a left order on } G\}.$$

References

- Sikora, Adam S., *Topology on the spaces of orderings of groups,* Preprint, 2003.
- Solomon, Reed, Π^0_1 *classes and orderable groups,* Preprint, 2003.