Summary of Formalization

Eric Paul

Introduction

There are three main theorems formalized. They are the following:

Theorem 1 (Lindenbaum)**.** *If X and Y are linear orders such that X embeds in an initial segment of Y and Y embeds in a final segment of X, then $X \cong Y$.*

Theorem 2 (Sum Refinement)**.** *Let X, Y, A, and B be linear orders such that $X + Y \cong A + B$. Then there exists a linear E such that at least one of the following holds:*

- *$A + E \cong X$ and $E + Y \cong B$ or*
- *$X + E \cong A$ and $E + B \cong Y$*

Theorem 3 (Finite Left Cancellation)**.** *If X and Y are linear orders, $0 \neq n \in \mathbb{N}$, and $nX \cong nY$, then $X \cong Y$.*

We shall explain how they are formalized at a high level that parallels the structure of the code.

Lindenbaum

This proof follows the proof of CSB in the Mathematics in Lean book.

Let α and β be linear orders. Let $f\colon \alpha \to \beta$ such that $f[\alpha]$ is an initial segment of β. Let $g\colon \beta \to \alpha$ such that $g[\beta]$ is a final segment of α. We now want to show that $\alpha \cong \beta$.

First, we check if β is empty. If β is empty, then since we have a map $f\colon \alpha \to \beta$, we must also have that α is empty. Therefore, we trivially have that $\alpha \cong \beta$.

Otherwise, β is nonempty. Our goal is now to define a function $h\colon \alpha \to \beta$ that will be an isomorphism.

We begin by defining a function $\mathrm{sbAux}\colon \mathbb{N} \to \mathcal{P}(\alpha)$

$$\mathrm{sbAux}(n) = \begin{cases} \alpha \setminus g[\beta] & \text{if } n = 0 \\ (g \circ f)[\mathrm{sbAux}(n-1)] \cup \mathrm{sbAux}(n-1) & \text{otherwise} \end{cases}$$

We now define $\mathrm{sbSet} = \bigcup_{n \in \mathbb{N}} \mathrm{sbAux}(n)$.

We now can define $h\colon \alpha \to \beta$.

$$h(x) = \begin{cases} f(x) & \text{if } x \in \text{sbSet} \\ g^{-1}(x) & \text{otherwise} \end{cases}$$

(Note that this is where we use the assumption that β is nonempty as the precise formulation of g^{-1} here requires it.)

We must now show that h is an isomorphism. The explanation for why h is a bijection is the same as for CSB. We now just need to show that h is order preserving.

We begin by showing that sbSet is an initial segment. To this end, we shall first show that each sbAux(n) is an initial segment.

Notice that since $g[\beta]$ is a final segment of α, $\alpha \setminus g[\beta]$ is an initial segment of α. Thus, sbAux(0) is an initial segment of α.

Assume that for n we have that sbAux(n) is an initial segment of α. Then sbAux$(n+1) = (g \circ f)[\text{sbAux}(n)] \cup \text{sbAux}(n)$. Now let $y \in \alpha$ such that $y < x$ for some $x \in \text{sbAux}(n+1)$. Our goal is to show that $y \in \text{sbAux}(n+1)$. Since $x \in \text{sbAux}(n+1)$ we have two cases.

The first is that $x \in \text{sbAux}(n)$. Then since sbAux(n) is an initial segment, we have that y must be in sbAux(n) and so $y \in \text{sbAux}(n+1)$ and we are done.

Otherwise, we have that $x \in (g \circ f)[\text{sbAux}(n)]$. We now split into two cases. The first case is that $y \in g[\beta]$. Then since $f[\alpha]$ is an initial segment of β, $f[\text{sbAux}(n)]$ is an initial segment of β. Therefore, $(g \circ f)[\text{sbAux}(n)]$ is an initial segment of $g[\beta]$. So since $(g \circ f)[\text{sbAux}(n)]$ is an initial segment of $g[\beta]$ and $y \in g[\beta]$, we have that $y \in (g \circ f)[\text{sbAux}(n)]$ and so we are done. Otherwise, we have that $y \notin g[\beta]$. Thus, we have that $y \in \text{sbAux}(0)$. Since $\text{sbAux}(0) \subseteq \text{sbAux}(n+1)$, $y \in \text{sbAux}(n+1)$ and so we are done.

So we have shown that sbAux(n) is an initial segment for all n. Now since the union of initial segments is an initial segment, we have that sbSet is an initial segment of α.

To check that h is order preserving the only interesting case is when we have $x \in \text{sbSet}$ and $y \notin \text{sbSet}$. Since sbSet is an initial segment, we have that $x < y$. And so our goal is to show that $h(x) < h(y)$. We have that sbSet is an initial segment and by the definition of h, $h[\text{sbSet}]$ is an initial segment. Therefore, since h is a bijection, $h(y)$ must be greater than every element of $h[\text{sbSet}]$. Thus, $h(x) < h(y)$.

And so we have shown that h is an isomorphism and have that $\alpha \cong \beta$.

Sum Refinement

Let α, β, γ, and δ be linear orders. Let $f\colon \alpha + \beta \to \gamma + \delta$ be an isomorphism.

We begin by comparing $f[\alpha]$ to γ. Both of them are initial segment of $\gamma + \delta$. Therefore, either γ is an initial segment of $f[\alpha]$ or $f[\alpha]$ is an initial segment of γ.

We look first at the case where γ is an initial segment of $f[\alpha]$. We let $e = f[\alpha] \setminus \gamma$.

Our first goal is to show that $\gamma + e \cong \alpha$. We will use the following lemma (which hides much of the work): if a is a linear order and b is an initial segment of a, then $b + (a \setminus b) \cong a$. This lemma gives us that $\gamma + (f[\alpha] \setminus \gamma) \cong f[\alpha]$. Since $f[\alpha] \setminus \gamma = e$ and $f[\alpha] \cong \alpha$, we have that $\gamma + e \cong \alpha$.

Now our goal is to show that $e + \beta \cong \delta$. We will again use a lemma to do the heavy lifting: if a is an initial segment of a linear order and $b \subseteq a$, then $(a \setminus b) + a^c \cong b^c$. This lemma gives us that $(f[\alpha] \setminus \gamma) + f[\alpha]^c \cong \gamma^c$. Notice that $\gamma^c = \delta$ and $f[\alpha] \setminus \gamma = e$. Furthermore, since f is an isomorphism, $f[\alpha]^c \cong \alpha^c \cong \beta$. Thus, we have that $e + \beta \cong \delta$ and so we are done.

The other case is that $f[\alpha]$ is an initial segment of γ. Here we let $e = \gamma \setminus f[\alpha]$.

Our first goal is to show that $\alpha + e \cong \gamma$. By the lemma used in the first goal of the previous case, we have that $f[\alpha] + (\gamma \setminus f[\alpha]) \cong \gamma$. Since $f[\alpha] \cong \alpha$ and $e = \gamma \setminus f[\alpha]$, we have that $\alpha + e \cong \gamma$.

Our next goal is to show that $e + \delta \cong \beta$. By the lemma used in the second goal of the previous case, we have that $(\gamma \setminus f[\alpha]) + \gamma^c \cong f[\alpha]^c$. We have that $e = \gamma \setminus f[\alpha]$, $\gamma^c = \delta$, and since f is an isomorphism, $f[\alpha]^c = \beta$. So we have that $e + \delta \cong \beta$ and so we are done.

Finite Left Cancellation

This proof follows the proof Tarski has in the book Ordinal Algebras.

Let α and β be linear orders and let $n \in \mathbb{N}$. Our goal is to show that $n\alpha \cong n\beta$ implies that $\alpha \cong \beta$. We do this by first showing if $n\alpha$ is initial in $n\beta$ then α is initial in β and dually that if $n\alpha$ is final in $n\beta$ then α is final in β. If we assume we have shown these two facts, then we complete the proof as follows. Since $n\alpha \cong n\beta$, we have that $n\alpha$ is initial in $n\beta$ and so α is initial in β. Also, since $n\alpha \cong n\beta$, we have that $n\beta$ is final in $n\alpha$ and so β is final in α. Since α is initial in β and β is final in α, we have by Lindenbaum that $\alpha \cong \beta$.

So it just remains for us to show those facts. Our goal is to show that if $n\alpha$ is initial in $n\beta$, then α is initial in β. We prove this by induction.

Our base case is that $n = 1$. Since $1\alpha \cong \alpha$ and $1\beta \cong \beta$, we are done.

Assume we have shown that for $n \in \mathbb{N}$ and for all linear orders α and β, if $n\alpha$ is initial in $n\beta$ then α is initial in β. We now want to show that if $(n+1)\alpha$ is initial in $(n+1)\beta$, then α is initial in β. Since multiplication on the right distributes, we have that $n\alpha + \alpha$ is initial in $n\beta + \beta$. Furthermore, since $n\alpha + \alpha$ is initial in $n\beta + \beta$, there exists a linear order e such that $(n\alpha + \alpha) + e \cong n\beta + \beta$. By associativity, we have that $n\alpha + (\alpha + e) \cong n\beta + \beta$.

By Sum Refinement, there exists a linear order e' such that we are in one of the following cases.

The first case is that $n\alpha + e' \cong n\beta$ and $e' + b \cong (\alpha + e)$. Since $n\alpha + e' \cong n\beta$, we have that $n\alpha$ is initial in $n\beta$. Then by our induction hypothesis, we have that α is initial in β and we are done.

The second case is that $n\beta+e' \cong n\alpha$ and $e'+(\alpha+e) \cong \beta$. Since $n\beta+e' \cong n\alpha$, we have that $n\beta$ is initial in $n\alpha$. Then by our induction hypothesis, we have that β is initial in α. Therefore, β is initial in $\alpha+e$. We also have that $e'+(\alpha+e) \cong \beta$ and so $(\alpha + e)$ is final in β. Since β is initial in $\alpha + e$ and $\alpha + e$ is final in β, we have by Lindenbaum that $\beta \cong \alpha + e$. Therefore, α is initial in β and we are done.

The proof that if $n\beta$ is final in $n\alpha$ then β is final in α is dual to the proof we just gave. So, as explained at the beginning, these two proofs imply that we have shown that if $n\alpha \cong n\beta$, then $\alpha \cong \beta$.