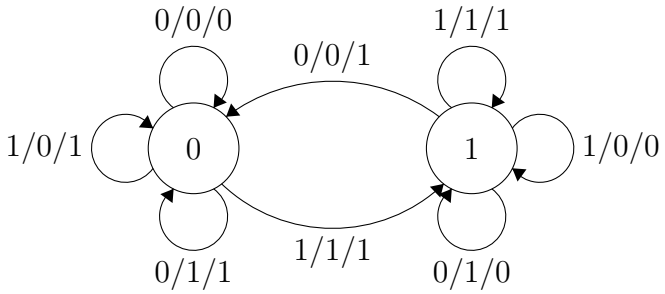
1 Intro

This entire project came about from trying to generalize the standard algorithm for addition in $\mathbb{Z}$. We work one column at a time, and addition in one column takes place in a finite group ($\mathbb{Z}/10$). However, we occasionaly have to "carry" the output from one column's computation into the next column, so addition in previous columns can impact the addition of future columns.

The *automatic* interpretation is that addition in $\mathbb{Z}$ can be computed using a **Finite State Automaton** (shown below). This is a fairly powerful requirement, as it says that addition in $\mathbb{Z}$ is essentially as easy as addition in $\mathbb{Z}/10$. We only have to remember one piece of information at a time (namely what we are carrying).



Here an edge from p to q labelled $a/b/c$ to mean that, given inputs a and b, while in state p, we should output c and transition to q. Intuitively, the states correspond to what we are currently carrying. It is clear that this machine does actually compute the basic addition algorithm in base 2, provided one starts in state 0. While an analogous machine exists for the computation in base 10, it is somewhat more cumbersome to draw.

The *cohomological* interpretation is that addition in $\mathbb{Z}$ can be approximated by addition in $\mathbb{Z}/10^n$, provided we are adding integers of length at most $n-1$. When adding integers of length n, $\mathbb{Z}/10^n$ does not (in general) correctly compute the sum in $\mathbb{Z}$, since the sum of two n digit numbers may result in a sum of length $n+1$, which $\mathbb{Z}/10^n$ cannot represent. This "error" is captured by a function $\rho_n : \mathbb{Z}/10^n \times \mathbb{Z}/10^n \to \mathbb{Z}/10$, which returns the overflow digit. These ρ_n satisfy the *Cocycle Condition*, and witness $\mathbb{Z}/10^{n+1}$ as a $\mathbb{Z}/10$-by-$\mathbb{Z}/10^{n+1}$ group extension.

This says that every element of $\mathbb{Z}/10^{n+1}$ can be written as (d, ds) where $d \in \mathbb{Z}/10$ and $ds \in \mathbb{Z}/10^n$. Then we can compute the $\mathbb{Z}/10^{n+1}$ addition

$(x, xs) + (y, ys)$ by inductively computing $xs + ys \in \mathbb{Z}/10^n$ and then computing $x + y + \rho_n(xs, ys) \in \mathbb{Z}/10$.

This perspective then lets us write addition in $\mathbb{Z}$ as the limit of addition in each of these approximations. Formally $\mathbb{Z}$ is the "finite-support subgroup" in the projective limit $\varprojlim \mathbb{Z}/10^n$.

With this perspective in mind, it is natural to ask if we can draw this parallel in other settings. That is, for some finite abelian group G equipped with a cocycle $\rho : G \times G \to G$ (denoting a generalized "carry" function), can we construct a new group by iteratively adding and carrying "one column at a time" analogous to realizing $\mathbb{Z}$ (actually the 10-adics...) as a projective limit of fixed-length approximations? If so, one would expect this limit group to admit an automatic structure which computes its addition in a finitary way, analogous to the standard addition algorithm for $\mathbb{Z}$.

We give positive answers to both of these questions, and constructive proofs of the relevant automata.

2 Cohomology

Let G be a finite abelian group, and $\rho : G \times G \to G$ a 2-cocycle satisfying a coherence condition $(\star)$, which we define below. We will inductively define G_n by iterating group extensions, where each $\rho_n : G_n \times G_n \to G$ is "essentially the same" as the provided ρ. The structure of these group extensions will provide the data required for a projective limit, which will end up being an automatic structure.

Somewhat surprisingly, we can *also* find cocycles $\rho'_n : G \times G \to G_n$, which are also "essentially the same" as the provided ρ. However, these induce the data of a direct limit, which is infinite torsion, but still automatic (indeed the same automaton will compute addition in the direct and proejctive limits). This is analogous to using essentially the same addition algorithm to compute in $\varinjlim \mathbb{Z}/10^n$, the subgroup of S^1 given by rationals with denominator a power of 10.

Perhaps *even more* surprisingly, proving the projective limit case directly seems to be extremely difficult, and so we pass through the injective construction as part of the proof. Some intuition for why this is the case will be provided before the proof of the existence of the projective limit, though we will start with the injective case as it is simpler.

2.1 Injective Limit

Let G be an abelian group, and $\rho : G \times G \to G$ a 2-cocycle. We demand ρ additionally satisfy the coherence condition below:

$$\forall a, b, c \in G. \rho\left(\rho(a, b), \rho(a + b, c)\right) = \rho\left(\rho(b, c), \rho(a, b + c)\right) \qquad (\star)$$

Note: All of our group extensions will come with trivial action. For a group extension $K \hookrightarrow G \twoheadrightarrow Q$ with cocycle $\rho : Q \times Q \to K$, we identify G with $Q \times K$ and addition $(q_1, k_1) + (q_2, k_2) = (q_1 + q_2, k_1 + k_2 + \rho(q_1, q_2))$.

Theorem 1. *We can inductively define group extensions $G_n \hookrightarrow G_{n+1} \twoheadrightarrow G$ with cocycles $\rho'_n : G \times G \to G_n$ "essentially the same" as ρ.*

Proof. Inductively assume we have defined G_n satisfying $G_{n-1} \hookrightarrow G_n \twoheadrightarrow G$.

Define $\rho'_n : G \times G \to G_n$ by $(g_1, g_2) \mapsto (\rho(g_1, g_2), 0^{n-1})$.

To show ρ'_n is a cocycle, we need to check $\rho'_n(a, b) + \rho'_n(a+b, c) = \rho'_n(b, c) + \rho'_n(a + b, c)$:

$$\begin{aligned}
&\rho'_n(a, b) + \rho'_n(a + b, c) = \\
&\rho'_n(b, c) + \rho'_n(a, b + c) \\
&\qquad\qquad \Longleftrightarrow \\
&(\rho(a, b), 0^{n-1}) + (\rho(a + b, c), 0^{n-1}) = \\
&(\rho(b, c), 0^{n-1}) + (\rho(a, b + c), 0^{n-1}) \\
&\qquad\qquad \Longleftrightarrow \\
&\Big(\rho(a, b) + \rho(a + b, c),\ \rho'_{n-1}(\rho(a, b), \rho(a + b, c))\Big) = \\
&\Big(\rho(b, c) + \rho(a, b + c),\ \rho'_{n-1}(\rho(b, c), \rho(a, b + c))\Big) \\
&\qquad\qquad \Longleftrightarrow \\
&\Big(\rho(a, b) + \rho(a + b, c), \Big(\rho(\rho(a, b), \rho(a + b, c)), 0^{n-2}\Big)\Big) = \\
&\Big(\rho(b, c) + \rho(a, b + c), \Big(\rho(\rho(b, c), \rho(a, b + c)), 0^{n-2}\Big)\Big)
\end{aligned}$$

The first equality is definitional. The second follows from addition in G_n, and the third from the (inductive) definition of ρ'_{n-1}.

Finally, at the end of it all, the two terms are indeed equal. Equality in the first component is the cocycle condition for ρ, and equality in the second component is exactly $(\star)$. $\square$

So now we see each $G_n \hookrightarrow G_{n+1}$. Then we have a diagram:

$$G_1 \hookrightarrow G_2 \hookrightarrow G_3 \hookrightarrow G_4 \hookrightarrow G_5 \hookrightarrow \cdots$$

which admits a direct limit $\overrightarrow{G}$.

Note: While we (for the purposes of this informal discussion) leave "essentially the same" undefined, it should be clear what is meant: Each $\rho'_n : G \times G \to G_n$ is just $s_n \circ \rho$, where s_n is the canonical (set theoretic) section $G \to G_n$ since G_n is also an extension of G.

2.2 Projective Limit

Now, to define a projective limit, we want a family of extensions $G \hookrightarrow G_{n+1} \twoheadrightarrow G_n$, but this requires a family of cocylces $\rho_n : G_n \times G_n \to G$, which represent the "overflow" of doing addition with elements with n-many digits. Of course, without knowledge of the limit (which we have in $\mathbb{Z}$), it is unclear how to properly define $\rho_n \ldots$ Intuition and formal manipulations suggest

$$\rho_{n+1}((x,a),(y,b)) = \rho(a,b) + \rho(a+b, \rho_n(x,y)) \tag{1}$$

is the right definition (Here $x, y \in G_n$ and $a, b \in G$).

Somewhat unfortunately, a direct proof that these ρ_n are all cocycles seems difficult. Thankfully, intuition *also* suggests that the G_n should be the same as in the injective case, and it is only the limiting behavior that differs. We will prove this intuition correct, and then use it to cheat and indirectly prove the ρ_n are cocylces.

Theorem 2. *If $G_n \hookrightarrow G_{n+1} \twoheadrightarrow G$ is a group extension as in the previous section, then $G \hookrightarrow G_{n+1} \twoheadrightarrow G_n$ is* also *a group extension.*

Proof. Say $G_n \hookrightarrow G_{n+1} \twoheadrightarrow G$ is an extension as above, and inductively assume we can write G_n as an extension $G \hookrightarrow G_n \twoheadrightarrow G_{n-1}$.

Consider $\varphi : G_{n+1} \twoheadrightarrow G_n$ by $(g_1, g_2, \ldots, g_n, g_{n+1}) \mapsto (g_1, g_2, \ldots, g_n)$.

It is shockingly non-routine to verify φ is indeed a group hom, so a proof is included here:

Say $\alpha, a, \beta, b \in G$ and $x, y \in G_{n-1}$:

$$\begin{aligned}
\varphi((\alpha, xa) + (\beta, yb)) &= \varphi((\alpha + \beta, xa + yb + \rho'_n(\alpha, \beta))) && \text{addition in } G_{n+1} \\
&= \varphi((\alpha + \beta, (x + y + \rho(\alpha, \beta)0^{n-1}, a + b + \text{stuff}))) && \text{inductive addition in } G_n \\
&= (\alpha + \beta, x + y + \rho(\alpha, \beta)0^{n-1}) && \text{defn } \varphi \\
&= (\alpha, x) + (\beta, y) && \text{addition in } G_n \\
&= \varphi((\alpha, xa)) + \varphi((\beta, xb))
\end{aligned}$$

Importantly, the addition on lines 2 and 4 both take place in G_n, though we are switching our representation. On line 2, we consider G_n inductively as $G \hookrightarrow G_n \twoheadrightarrow G_{n-1}$, while in line 4 we consider G_n as in the previous section, $G_{n-1} \hookrightarrow G_n \twoheadrightarrow G$. Also, importantly, the "stuff" in line 2 comes from whatever magic $\rho_{n-1} : G_{n-1} \times G_{n-1} \to G$ happens to do. While we do *technically* give a constructive definition of the ρ_n, actually figuring out what they do is a real pain. Thankfully, φ immediately kills whatever stuff we happen to collect!

Back to the proof at hand, it is clear that the kernel of φ is $\{0^n g \mid g \in G\}$, which is clearly isomorphic to G as a group. Thus $G \hookrightarrow G_{n+1} \twoheadrightarrow G_n$ is an extension! □

Dual to before, these group extensions give rise to a diagram:

$$\cdots \twoheadrightarrow G_5 \twoheadrightarrow G_4 \twoheadrightarrow G_3 \twoheadrightarrow G_2 \twoheadrightarrow G_1$$

which admits a projective limit $\overleftarrow{G}$, as desired.

3 Automata

Finite State Automata give us a way of computing addition in a group using only finite information. Formally, an automaton $\mathcal{A}$ is a tuple

$$(\Gamma, \gamma_0 \in \Gamma, \tau_\gamma : \Gamma \times \Gamma \to \Gamma, \mu_\gamma : \Gamma \times \Gamma \to \Gamma)$$

Γ is the **State Set** of the machine, γ_0 is the **Initial State**, τ_γ is a family of **Transition Functions**, and μ_γ is a family of **Multiplication Functions**.

There are two natural ways to compute with $\mathcal{A}$, giving rise to two functions (both written $\mathcal{A}(x, y)$). We start by defining counterparts, indexed by the current state. Here, as usual, ϵ and $\frown$ are the unit and multiplication in the free monoid Γ^*:

Inductively, define functions on finite strings $x, y \in \Gamma^*$ by

- $\mathcal{A}_\gamma(\varepsilon, \varepsilon) = \varepsilon$
- $\mathcal{A}_\gamma(a \frown x, b \frown y) = \mu_\gamma(a, b) \frown \mathcal{A}_{\tau_\gamma(a,b)}(x, y)$

Put $\mathcal{A}(x, y) = \mathcal{A}_{\gamma_0}(x, y)$.

Computation in this machine proceeds by looking at one letter of our input string at a time. If our machine is in state γ while looking at letters a and b, then we output $\mu_\gamma(a, b)$. Then we transition to a new state $\tau_\gamma(a, b)$ to recursively compute the rest of the multiplication. Of course, we need somewhere to start, and we start at γ_0, the aptly named initial state.

We could also coinductively define functions on infinite strings $x, y \in \Gamma^\omega$ by simply ignoring the base case in the above construction.

Note: this is *note* the most general notion of automata considered in the literature. Our set of states Γ is the same as our set of letters, but this needs not be the case! Additionally, it is extremely unclear which automata compute a function obeying the group laws. It seems characterizing the machines giving rise to groups is too difficult a problem to tackle in the time we have.

Now, let's show that $\overleftarrow{G}$ and $\overrightarrow{G}$ are both automatic. Fix a finite abelian group G and a cocycle $\rho : G \times G \to G$. Define $\mathcal{A} = (G, 0, \tau_g, \mu_g)$, where

- $\tau_g(a, b) = \rho(a, b) + \rho(a + b, g)$
- $\mu_g(a, b) = a + b + g$

Notice μ_g "carries a g" while adding its inputs, and the intuition is that we find ourselves in state g exactly when we should be carrying a g. Of course, what *should* we carry when we add a and b (with a carry of g)? The answer to this question will tell us what state to transition to. Recalling our carry operation is based on ρ, we ask what ρ thinks about the computation $a + b + g$.

It is quick to verify that (in G_2)

$$(a,0)+(b,0)+(g,0)=(a+b+g,\rho(a,b)+\rho(a+b,g))$$

and this is where our transition function (representing what we should carry) comes from.

Honestly, the rest is (co-)induction. I will include the proofs for posterity, but nothing of note happens. We simply verify that this machine does what I assert it does.

Theorem 3. *$\mathcal{A}$ correctly computes multiplication in $\overrightarrow{G}$ when it computes with Γ^*.*

Proof. We want to show that $\mathcal{A}(x,y)=z \iff x+y=z$. Here $+$ is taking place in $\overrightarrow{G}$, and we are identifying strings of G with the iterated tuples showing up in iterated extensions G_n in the natural way.

We induct on the length of our strings, with a stronger inductive hypothesis: We will show $\mathcal{A}_g(x,y)=z \iff x+y+(g,0^{n-1})=z$

$\mathcal{A}_g(a,b)=c \iff a+b+g=c$ by definition.

$$\begin{aligned}
\mathcal{A}_g(ax,by)=cz &\iff (a+b+g=c)\wedge\mathcal{A}_{\tau_g(a,b)}(x,y)=z && \text{defn}\\
&\iff (a+b+g=c)\wedge x+y+(\tau_g(a,b),0^{n-2})=z && \text{IH}\\
&\iff ax+by+(g,0^{n-1})=cz && \text{see below}
\end{aligned}$$

For the last implication, notice:

$$\begin{aligned}
(a,x)+(b,y)+(g,0^{n-1}) &= (a+b,x+y+(\rho(a,b),0^{n-2}))+(g,0^{n-1})\\
&= (a+b+g,x+y+(\rho(a,b),0^{n-2})+0^{n-1}+(\rho(a+b,g),0^{n-2}))\\
&= (a+b+g,x+y+(\tau_g(a,b),0^{n-2}))
\end{aligned}$$

So $(a,x)+(b,y)+(g,0^{n-1})=(c,z)$ if and only if $a+b+g=c$ and $x+y+(\tau_g(a,b),0^{n-2})=z$, as desired.

NOTE: I found this glitch while texing this – The above only goes through if $\rho(\rho(a,b) + \rho(a+b,g)) = 0$. That is, if we never have a carry that directly impacts the immediate next column. As an example, if we were in $\mathbb{Z}$ and carrying 9 times what we typically would, then $9 + 9 = 98$, and $99 + 99 = 1878$ (since we carry the 9, and now 9+9+9 = 187). There is an "obvious" fix to this problem: we might sometimes have to remember a carry from more than one digit ago... I'm not sure how to formalize this, though. A variant on this proof will go through if we know that for each G, ρ there's some bound $n_{G,\rho}$ where we never need to remember what happened more than $n_{G,\rho}$ many digits ago. For $\mathbb{Z}/10$ and 9 times the standard carry, $n = 2$ works, as the sum $9999 + 9999$ shows. □

Theorem 4. *Similarly, $\mathcal{A}$ correctly computes multiplication in $\overleftarrow{G}$ when it computes with Γ^ω.*

Proof. The proof is analogous to the above, occasionally saying "coinduction" instead of "induction".

Unfortunately, the same glitch regarding carrying across more than one digit is inherited by this proof... □

4 Future Questions

1. Can we fix the glitch (yes, but I need to actually do it)
2. Does every cocycle satisfy $\star$? (probably not)
3. Does every $\mathcal{A}$ which computes a group compute one of these? (probably, but I need to prove it)
4. What about nonabelian groups? (should be easy or brutal, either way we'll know quickly)
5. Does being automatic give any nice cohomological properties? (beats me)