An Example of a Cofinitary Group in Isabelle/HOL

Bart Kastermans

October 11, 2017

Abstract

We formalize the usual proof that the group generated by the function $k \mapsto k + 1$ on the integers gives rise to a cofinitary group.

Contents

theory *CofGroups*
imports *Main HOL−Library.Nat-Bijection*
begin

1 Introduction

Cofinitary groups have received a lot of attention in Set Theory. I will start by giving some references, that together give a nice view of the area. See also Kastermans [7] for my view of where the study of these groups (other

than formalization) is headed. Starting work was done by Adeleke [1], Truss [12] and [13], and Koppelberg [10]. Cameron [3] is a very nice survey. There is also work on cardinal invariants related to these groups and other almost disjoint families, see e.g. Brendle, Spinas, and Zhang [2], Hrušák, Steprans, and Zhang [5], and Kastermans and Zhang [9]. Then there is also work on constructions and descriptive complexity of these groups, see e.g. Zhang [14], Gao and Zhang [4], and Kastermans [6] and [8].

In this note we work through formalizing a basic example of a cofinitary group. We want to achieve two things by working through this example. First how to formalize some proofs from basic set-theoretic algebra, and secondly, to do some first steps in the study of formalization of this area of set theory. This is related to the work of Paulson andGrąbczewski [11] on formalizing set theory, our preference however is towards using Isar resulting in a development more readable for "normal" mathematicians.

A *cofinitary group* is a subgroup G of the symmetric group on $\mathbb{N}$ (in Isabelle *nat*) such that all non-identity elements $g \in G$ have finitely many fixed points. A simple example of a cofinitary group is obtained by considering the group G' a subgroup of the symmetric group on $\mathbb{Z}$ (in Isabelle *int* generated by the function $upOne : \mathbb{Z} \to \mathbb{Z}$ defined by $k \mapsto k + 1$. No element in this group other than the identity has a fixed point. Conjugating this group by any bijection $\mathbb{Z} \to \mathbb{N}$ gives a cofinitary group.

We will develop a workable definition of a cofinitary group (Section 2) and show that the group as described in the previous paragraph is indeed cofinitary (this takes the whole paper, but is all pulled together in Section 9). Note: formalizing the previous paragraph is all that is completed in this note.

Since this note is also written to be read by the proverbial "normal" mathematician we will sometimes remark on notations as used in Isabelle as they related to common notation. We do expect this proverbial mathematician to be somewhat flexible though. He or she will need to be flexible in reading, this is just like reading any other article; part of reading is reconstructing.

We end this introduction with a quick overview of the paper. In Section 2 we define the notion of cofinitary group. In Section 3 we define the function *upOne* and give some of its basic properties. In Section 4 we define the set *Ex1* which is the underlying set of the group generated by *upOne*, there we also derive a normal form theorem for the elements of this set. In Section 5 we show all elements in *Ex1* are cofinitary bijections (cofinitary here is used in the general meaning of having finitely many fixed points). In Section 6 we show this set is closed under composition and inverse, in effect showing that it is a "cofinitary group" (cofinitary group here is in quotes, since we only define it for sets of permutations on the natural numbers). In Section 7 we show the general theorem that conjugating a permutation by a bijection

does the expected thing to the set of fixed points. In Section 8 we define the function *CONJ* that is conjugation by *ni-bij* (a bijection from *nat* to *int*), show that is acts well with respect to the group operations, use it to define *Ex2* which is the underlying set of the cofinitary group we are construction, and show the basic properties of *Ex2*. Finally in Section 9 we quickly show that all the work in the section before it combines to show that *Ex2* is a cofinitary group.

2 The Main Notions

First we define the two main notions.

We write *S-inf* for the symmetric group on the natural numbers (we do not define this as a group, only as the set of bijections).

definition $S\text{-}inf :: (nat \Rightarrow nat)\ set$
where
$S\text{-}inf = \{f::(nat \Rightarrow nat).\ bij\ f\}$

Note here that *bij f* is the predicate that f is a bijection. This is common notation in Isabelle, a predicate applied to an object. Related to this *inj f* means f is injective, and *surj f* means f is surjective.

The same notation is used for functionn application. Next we define a function *Fix*, applying it to an object is also written by juxtaposition.

Given any function f we define *Fix f* to be the set of fixed points for this function.

definition $Fix :: ('a \Rightarrow 'a) \Rightarrow ('a\ set)$
where
$Fix\ f = \{\ n\ .\ f(n) = n\ \}$

We then define a locale *CofinitaryGroup* that represents the notion of a cofinitary group. An interpretation is given by giving a set of functions $nat \to nat$ and showing that it satisfies the identities the locale assumes. A locale is a way to collect together some information that can then later be used in a flexible way (we will not make a lot of use of that here).

locale *CofinitaryGroup* =
  fixes
    $dom :: (nat \Rightarrow nat)\ set$
  assumes
    $type\text{-}dom : dom \subseteq S\text{-}inf$ **and**
    $id\text{-}com : id \in dom$ **and**
    $mult\text{-}closed : f \in dom \wedge g \in dom \Longrightarrow f \circ g \in dom$ **and**
    $inv\text{-}closed : f \in dom \Longrightarrow inv\ f \in dom$ **and**
    $cofinitary : f \in dom \wedge f \neq id \Longrightarrow finite\ (Fix\ f)$

3 The Function *upOne*

Here we define the function, *upOne*, translation up by 1 and proof some of its basic properties.

definition *upOne* :: *int* ⇒ *int*
where
upOne n = *n* + *1*

declare *upOne-def* [*simp*] — automated tools can use the definition

First we show that this function is a bijection. This is done in the usual two parts; we show it is injective by showing from the assumption that outputs on two numbers are equal that these two numbers are equal. Then we show it is surjective by finding the number that maps to a given number.

lemma *inj-upOne*: *inj upOne*
⟨*proof*⟩

lemma *surj-upOne*: *surj upOne*
⟨*proof*⟩

theorem *bij-upOne*: *bij upOne*
⟨*proof*⟩

Now we show that the set of fixed points of *upOne* is empty. We show this in two steps, first we show that no number is a fixed point, and then derive from this that the set of fixed points is empty.

lemma *no-fix-upOne*: *upOne n* ≠ *n*
⟨*proof*⟩

theorem *Fix upOne* = {}
⟨*proof*⟩

Finally we derive the equation for the inverse of *upOne*. The rule we use references *Hilbert-Choice* since the *inv* operator, the operator that gives an inverse of a function, is defined using Hilbert's choice operator.

lemma *inv-upOne-eq*: (*inv upOne*) (*n*::*int*) = *n* − *1*
⟨*proof*⟩

We can also show this quickly using Hilbert_Choice.inv_f_eq properly instantiated : *upOne* (*n* − *1*) = *n* ⟹ *inv upOne n* = *n* − *1*.

lemma (*inv upOne*) *n* = *n* − *1*
⟨*proof*⟩

4 The Set of Functions and Normal Forms

We define the set *Ex1* of all powers of *upOne* and study some of its properties, note that this is the group generated by *upOne* (in Section 6 we prove

it closed under composition and inverse). In Section 5 we show that all its elements are cofinitary and bijections (bijections with finitely many fixed points). Note that this is not a cofinitary group, since our definition requires the group to be a subset of *S-inf*

inductive-set *Ex1* :: (*int* ⇒ *int*) *set* **where**
base-func: *upOne* ∈ *Ex1* |
comp-func: $f \in Ex1 \Longrightarrow (upOne \circ f) \in Ex1$ |
comp-inv : $f \in Ex1 \Longrightarrow ((inv\ upOne) \circ f) \in Ex1$

We start by showing a *normal form* for elements in this set.

lemma *Ex1-Normal-form-part1*: $f \in Ex1 \Longrightarrow \exists k.\ \forall\ n.\ f(n) = n + k$
⟨*proof*⟩

Now we'll show the other direction. Then we apply rule *int-induct* which allows us to do the induction by first showing it true for $k = 1$, then showing that if true for $k = i$ it is also true for $k = i + 1$ and finally showing that if true for $k = i$ then it is also true for $k = i - 1$.

All proofs are fairly straightforward and use extensionality for functions. In the base case we are just dealing with *upOne*. In the other cases we define the function *?h* which satisfies the induction hypothesis. Then f is obtained from this by adding or subtracting one pointwise.

In this proof we use some pattern matching to save on writing. In the statement of the theorem, we match the theorem against *?P k* thereby defining the predicate *?P*.

lemma *Ex1-Normal-form-part2*:
$(\forall f.\ ((\forall n.\ f\ n = n + k) \longrightarrow f \in Ex1))$ (**is** *?P k*)
⟨*proof*⟩

Combining the two directions we get the normal form theorem.

theorem *Ex1-Normal-form*: $(f \in Ex1) = (\exists k.\ \forall n.\ f(n) = n + k)$
⟨*proof*⟩

5 All Elements Cofinitary Bijections.

We now show all elements in *CofGroups.Ex1* are bijections, Theorem *all-bij*, and have no fixed points, Theorem *no-fixed-pt*.

theorem *all-bij*: $f \in Ex1 \Longrightarrow bij\ f$
⟨*proof*⟩

theorem *no-fixed-pt*:
assumes *f-Ex1*: $f \in Ex1$
and *f-not-id*: $f \neq id$
shows $Fix\ f = \{\}$
⟨*proof*⟩

6 Closed under Composition and Inverse

We start by showing that this set is closed under composition. These facts can later be conjugated to easily obtain the corresponding results for the group on the natural numbers.

theorem *closed-comp*: $f \in Ex1 \wedge g \in Ex1 \Longrightarrow f \circ g \in Ex1$
⟨*proof*⟩

Now we show the set is closed under inverses. This is done by an induction on the definition of *CofGroups.Ex1* only using the normal form theorem and rewriting of expressions.

theorem *closed-inv*: $f \in Ex1 \Longrightarrow inv\ f \in Ex1$
⟨*proof*⟩

7 Conjugation with a Bijection

An abbreviation of the bijection from the natural numbers to the integers defined in the library. This will be used to coerce the functions above to be on the natural numbers.

abbreviation *ni-bij* == *int-decode*

lemma *bij-f-o-inf-f*: $bij\ f \Longrightarrow f \circ inv\ f = id$
⟨*proof*⟩

The following theorem is a key theorem in showing that the group we are interested in is cofinitary. It states that when you conjugate a function with a bijection the fixed points get mapped over.

theorem *conj-fix-pt*: $\bigwedge f{::}('a \Rightarrow 'b).\ \bigwedge g{::}('b \Rightarrow 'b).\ (bij\ f)$
$\Longrightarrow ((inv\ f)\text{`}(Fix\ g)) = Fix\ ((inv\ f) \circ g \circ f)$
⟨*proof*⟩

8 Bijections on $\mathbb{N}$

In this section we define the subset *Ex2* of *S-inf* that is the conjugate of *CofGroups.Ex1* bij *ni-bij*, and show its basic properties.

CONJ is the function that will conjugate *CofGroups.Ex1* to *Ex2*.

definition $CONJ :: (int \Rightarrow int) \Rightarrow (nat \Rightarrow nat)$
where
$CONJ\ f = (inv\ ni\text{-}bij) \circ f \circ ni\text{-}bij$

declare *CONJ-def* [*simp*] — automated tools can use the definition

We quickly check that this function is of the right type, and then show three of its properties that are very useful in showing *Ex2* is a group.

lemma *type-CONJ*: $f \in Ex1 \Longrightarrow (inv\ ni\text{-}bij) \circ f \circ ni\text{-}bij \in S\text{-}inf$
⟨*proof*⟩

lemma *inv-CONJ*:
assumes *bij-f*: *bij f*
shows $inv\ (CONJ\ f) = CONJ\ (inv\ f)$ (**is** *?left* = *?right*)
⟨*proof*⟩

lemma *comp-CONJ*:
$CONJ\ (f \circ g) = (CONJ\ f) \circ (CONJ\ g)$ (**is** *?left* = *?right*)
⟨*proof*⟩

lemma *id-CONJ*: $CONJ\ id = id$
⟨*proof*⟩

We now define the group we are interested in, and show the basic facts that together will show this is a cofinitary group.

definition *Ex2* :: $(nat \Rightarrow nat)\ set$
where
Ex2 = *CONJ*‘*Ex1*

theorem *mem-Ex2-rule*: $f \in Ex2 = (\exists\, g.\ (g \in Ex1 \wedge f = CONJ\ g))$
⟨*proof*⟩

theorem *Ex2-cofinitary*:
assumes *f-Ex2*: $f \in Ex2$
and *f-nid*: $f \neq id$
shows $Fix\ f = \{\}$
⟨*proof*⟩

lemma *id-Ex2*: $id \in Ex2$
⟨*proof*⟩

lemma *inv-Ex2*: $f \in Ex2 \Longrightarrow (inv\ f) \in Ex2$
⟨*proof*⟩

lemma *comp-Ex2*:
assumes *f-Ex2*: $f \in Ex2$ **and**
g-Ex2: $g \in Ex2$
shows $f \circ g \in Ex2$
⟨*proof*⟩

9 The Conclusion

With all that we have shown we have already clearly shown *Ex2* to be a cofinitary group. The formalization also shows this, we just have to refer to the correct theorems proved above.

interpretation *CofinitaryGroup Ex2*
⟨*proof*⟩

end

References

[1] S. A. Adeleke. Embeddings of infinite permutation groups in sharp, highly transitive, and homogeneous groups. *Proc. Edinburgh Math. Soc. (2)*, 31(2):169–178, 1988.

[2] J. Brendle, O. Spinas, and Y. Zhang. Uniformity of the meager ideal and maximal cofinitary groups. *J. Algebra*, 232(1):209–225, 2000.

[3] P. J. Cameron. Cofinitary permutation groups. *Bull. London Math. Soc.*, 28(2):113–140, 1996.

[4] S. Gao and Y. Zhang. Definable sets of generators in maximal cofinitary groups. *Adv. Math.*, 217(2):814–832, 2008.

[5] M. Hrušák, J. Steprans, and Y. Zhang. Cofinitary groups, almost disjoint and dominating families. *J. Symbolic Logic*, 66(3):1259–1276, 2001.

[6] B. Kastermans. Isomorphism types of maximal cofinitary groups. to appear in the Bulletin of Symbolic Logic.

[7] B. Kastermans. Questions on cofinitary groups. in preparation.

[8] B. Kastermans. The complexity of maximal cofinitary groups. *Proceeding American Mathematical Society*, 137(1):307–316, 2009.

[9] B. Kastermans and Y. Zhang. Cardinal invariants related to permutation groups. *Ann. Pure Appl. Logic*, 143:139–146i, 2006.

[10] S. Koppelberg. Groups of permutations with few fixed points. *Algebra Universalis*, 17(1):50–64, 1983.

[11] L. C. Paulson and K. Grąbczewski. Mechanizing set theory. Cardinal arithmetic and the axiom of choice. *J. Automat. Reason.*, 17(3):291–323, 1996.

[12] J. K. Truss. Embeddings of infinite permutation groups. In *Proceedings of groups—St. Andrews 1985*, volume 121 of *London Math. Soc. Lecture Note Ser.*, pages 335–351, Cambridge, 1986. Cambridge Univ. Press.

[13] J. K. Truss. Joint embeddings of infinite permutation groups. In *Advances in algebra and model theory (Essen, 1994; Dresden, 1995)*, volume 9 of *Algebra Logic Appl.*, pages 121–134. Gordon and Breach, Amsterdam, 1997.

[14] Y. Zhang. Constructing a maximal cofinitary group. *Lobachevskii J. Math.*, 12:73–81 (electronic), 2003.