Computing with Compact Sets: the Gray Code Case [1]

(j.w.w. Ulrich Berger)

Dieter Spreen

University of Siegen

Computability, Constructivity, Complexity: From Logic to Algorithms
Online-only workshop, Birmingham, 20-24 September 2021

[1] This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 731143.

1. Admissible representations for real numbers

There is a plentitude of admissible and hence computationally equivalent representations for real numbers $x \in \mathbb{I} = [-1, 1]$. Here, we will consider two of them:

- *Signed digit representation*: $x \in \mathbb{I}$ is represented by any stream $d_0 : d_1 : d_2 : \ldots$ of signed digits $d_i \in \mathrm{SD} = \{-1, 0, 1\}$ such that
  - $x \in [d_0/2 - 1, d_0/2 + 1]$ and
  - $d_1 : d_2 : \ldots$ is a signed digit representation of $2x - d_0$.

  The signed digit representation is highly redundant: every non-dyadic real has continuum many signed-digit representations.

- Tsuiki's *infinite Gray code*: x is encoded by the stream $a_0 : a_1 : a_2 : \ldots$ where $a_0 \in \{0, 1, \bot(\text{“undefined”})\}$ depending on whether $x < 0$, $x > 0$, or $x = 0$, and $a_1 : a_2 : \ldots$ encodes $t(x)$ where $t\colon \mathbb{I} \to \mathbb{I}$ is the *tent* function

$$t(x) = 1 - 2|x|.$$

  - Infinite Gray is non-redundant: every $x \in \mathbb{I}$ has exactly one Gray code.

2. Formalisation in IFP (Berger/Tsuiki)

IFP is many-sorted intuitionistic first-order logic with inductive and coinductive definitions.

Aim:

1. Define predicates **S** and **G** with
   - **S**(x) meaning "x is a signed-digit real" and
   - **G**(x) meaning "x is a Gray code real"

   so that

   $$p\,\mathbf{r}\,\mathbf{S}(x) \text{ iff } p \text{ is a stream of signed digits representing } x$$

   and similarly in the other case.
2. Derive $\mathbf{S} = \mathbf{G}$ in IFP and from the proof extract an algorithm translating signed digit into Gray code and vice versa.

Let

$$\mathbf{SD}(x) \stackrel{\mathrm{Def}}{=} (x = -1 \vee x = 1) \vee x = 0,$$
$$\mathbf{II}(d, x) \stackrel{\mathrm{Def}}{=} |2x - d| \leq 1,$$

and define $\mathbf{S}(x)$ coinductively as the largest fixed point of the operator

$$\Phi(X, x) \stackrel{\mathrm{Def}}{=} (\exists d)\, \mathbf{SD}(d) \wedge \mathbf{II}(d, x) \wedge X(2x - d).$$

Moreover, let

$$\mathbf{D}(x) \stackrel{\mathrm{Def}}{=} x \neq 0 \to (x \leq 0 \vee x \geq 0)$$

and define $\mathbf{G}(x)$ coinductively as the largest fixed point of the operator

$$\Psi(X, x) \stackrel{\mathrm{Def}}{=} (-1 \leq x \leq 1) \wedge \mathbf{D}(x) \wedge \mathbf{G}(\mathbf{t}(x)).$$

Theorem (Berger/Tsuiki)

$\mathbf{S} \subseteq \mathbf{G}$ *is derivable in IFP.*

For the other direction it is known from Tsuiki's investigations that a translation from Gray code into signed digit must include concurrent computations. Algorithms extracted from intuitionistic proofs, however, are known to operate sequentially.

Berger and Tsuiki therefore extended IFP to *Concurrent Fixed Point Logic (CFP)* by adding a new connective *restriction* $\|$ and a *concurrency modality* $\downdownarrows$, together with new proof rules.

The idea behind the new connective and/or modality is best understood by considering how they are realised:

$$a\,\mathbf{r}\,(A \parallel B) \stackrel{\mathrm{Def}}{=} (\,\mathbf{r}\,B \to a \neq \bot) \wedge (a \neq \bot \to a\,\mathbf{r}\,A)$$

A closed program M denotes a value different from $\bot$ iff M reduces to whnf. Thus, the definition says

- If B is realisable, then M reduces to whnf.
- If M reduces to whnf, then M realises A (even if B is not realisable).

In this sense, one has partial correctness of M with respect to the specification A.

Rules:

$$\frac{B \to A_0 \vee A_1 \quad \neg B \to A_0 \wedge A_1}{(A_0 \vee A_1) \parallel B} \ \parallel\text{-intro, } (A_0,\ A_1,\ B \text{ Harrop})$$

$$\frac{A \parallel B \quad B' \to B}{A \parallel B'} \ (\parallel\text{-antimon})$$

$$\frac{A \parallel B \quad A \to A'}{A' \parallel B} \ (\parallel\text{-mon})$$

$+$ several other rules, all realisable.

$$c\,\mathbf{r}\,{\downdownarrows}(A) \stackrel{\mathrm{Def}}{=} c = \mathbf{Amb}(a,b) \land (a \neq \bot \lor b \neq \bot) \land \\ (a \neq \bot \to a\,\mathbf{r}\,A) \land (b \neq \bot \to b\,\mathbf{r}\,A)$$

$\mathbf{Amb}(a,b)$ is *McCarthy's amb operator*: execute the two programs a and b in parallel and take the one which becomes defined (i.e. a whnf) first.

Introduction rule:

$$\frac{A \parallel C \quad A \parallel \neg C}{{\downdownarrows}(A)}\ ({\downdownarrows}\text{-lem})$$

+ several other rules, all realisable.

Define $\mathbf{S}_2(x)$ coinductively to be the largest fixed point of the operator

$$\Phi_2(X, x) \stackrel{\mathrm{Def}}{=} \downdownarrows((\exists d)\, \mathbf{SD}(d) \wedge \mathbf{II}(d, x) \wedge X(2x - d)).$$

Theorem (Berger/Tsuiki)

$\mathbf{G} \subseteq \mathbf{S}_2$

The aim of the present talk is to do a similar thing for the space of nonempty compact subsets of $\mathbb{I}$.

3. The nonempty compact sets case

How to deal with the space of nonempty compact subsets of $\mathbb{I}$, where $\mathbb{I}$ is represented by the signed digit representation, has already studied in [Berger/Spreen, 2016]:

Let $\mathbf{I}_d \stackrel{\mathrm{Def}}{=} \{\, x \mid \mathbf{I}(d, x) \,\}$ and define $\mathbf{S_K}(K)$ coinductively as the largest fixed point of the operator

$$\begin{aligned}\Theta(X, K) \stackrel{\mathrm{Def}}{=} (\exists E \in \mathbf{P_{fin}}(\mathbf{SD}))\, K = \bigcup_{d \in E} K \cap \mathbf{I}_d \wedge \\ (\forall d \in E)\, (K \cap \mathbf{I}_d \neq \emptyset \wedge X(\{\, 2x - d \mid x \in K \cap \mathbb{I}_d \,\})\end{aligned}$$

For a definition of the Gray code of a nonempty compact set K we need to know whether K is contained in $[-1,0]$ or $[0,1]$, or in both. We use the minimum and maximum of K to this end.

Let $\mathbf{GC} = \{-1, 1\}$ and define $\mathbf{G_K}(K)$ coinductively to be the largest fixed point of the operator

$$\Omega(X, K) \stackrel{\mathrm{Def}}{=} \mathbf{G}(\min K) \land \mathbf{G}(\max K) \land \\ (\forall d \in \mathbf{GC})\,(K \cap \mathbb{I}_d \neq \emptyset \to X(\mathbf{t}[K \cap \mathbb{I}_d])$$

Proposition

$\mathbf{S_K} \subseteq \mathbf{G_K}$ *is derivable in IFP.*

For the converse implication we again need a concurrent version, this time of the predicate $\mathbf{S_K}$.

Note that in general, the concurrency modality $\downdownarrows$ is not a monad. We turn it into a monad by considering its finite iterative closure $\overset{*}{\downdownarrows}$, that is, $\overset{*}{\downdownarrows}(A)$ is inductively defined as the least fixed point of the operator

$$\Delta(X) \stackrel{\mathrm{Def}}{=} \downdownarrows(A \vee X(A))$$

<u>Rules:</u>

$$\frac{\overset{*}{\downdownarrows}(A) \quad \overset{*}{\downdownarrows}(B)}{\overset{*}{\downdownarrows}(A \wedge B)} \ (\overset{*}{\downdownarrows}\text{-}\wedge\text{-intro})$$

$$\frac{A \parallel B_1 \ldots A \parallel B_n}{\overset{*}{\downdownarrows}(A) \parallel (B_1 \vee \cdots \vee B_n)} \ (\overset{*}{\downdownarrows}\text{-}\parallel\text{-}\vee)$$

$+$ several other rules.

Now, let $\mathbf{S}^*_\mathbf{K}(K)$ coinductively be defined as the largest fixed point of the operator

$$\Theta_\mathbf{K}(X, K) \stackrel{\mathrm{Def}}{=} \overset{*}{\downdownarrows}((\exists E \in \mathbf{P_{fin}}(\mathbf{SD}))\, K = \bigcup_{d \in E} K \cap \mathbb{I}_d \wedge (\forall d \in E)\,(K \cap \mathbb{I}_d \neq \emptyset \wedge X(\{\, 2x - d \mid x \in K \cap \mathbb{I}_d \,\})))$$

Proposition

$\mathbf{G_K} \subseteq \mathbf{S}^*_\mathbf{K}$ *is derivable in CFP (+ new rules)*

The main step in the proof is

Lemma

$\mathbf{G_K}(K) \to \overset{*}{\downdownarrows}(A)$ *is derivable in CFP (+ additional rules), where*

$$A(K) \stackrel{\mathrm{Def}}{=} (\exists E \in \mathbf{P_{fin}}(\mathbf{SD}))\, K = \bigcup_{d \in E} K \cap \mathbb{I}_d \wedge (\forall d \in E)\,(K \cap \mathbb{I}_d \neq \emptyset)$$

Let

$$B_0^{\mathsf{min}} \stackrel{\mathrm{Def}}{=} \min K \neq 0 \qquad B_1^{\mathsf{min}} \stackrel{\mathrm{Def}}{=} \mathbf{t}(\min K) \neq 0$$

$$B_0^{\mathsf{max}} \stackrel{\mathrm{Def}}{=} \max K \neq 0 \quad B_1^{\mathsf{max}} \stackrel{\mathrm{Def}}{=} \mathbf{t}(\max K) \neq 0$$

and

$$C_{i,j} \stackrel{\mathrm{Def}}{=} B_i^{\mathsf{min}} \wedge B_j^{\mathsf{max}} \quad (i, j \in \{0, 1\})$$

Note that

$$\bigvee_{i,j=0}^{1} C_{i,j} \tag{1}$$

Because of Rule ($\overset{*}{\downdownarrows}$-$\|$-$\vee$) and a *modus ponens* rule for $\|$ it suffices to show that for all $i, j \in \{0, 1\}$

$$A(K) \parallel C_{i,j}$$

Case $i = j = 0$:

Since $\mathbf{G_K}(K)$ we have that $\mathbf{G}(\min K)$ and $\mathbf{G}(\max K)$. That is for $x \in \{\min K, \max K\}$

$$x \leq 0 \vee x \geq 0 \,\|\, x \neq 0 \tag{2}$$

As $\mathbf{G}(x) \to \mathbf{G}(\mathbf{t}(x))$ we also have that

$$\mathbf{t}(x) \leq 0 \vee \mathbf{t}(x) \geq 0 \,\|\, \mathbf{t}(x) \neq 0 \tag{3}$$

Now, note

$$\begin{gathered} \min K \geq 0 \leftrightarrow K \geq 0 \\ \min K \leq 0 \leftrightarrow K \cap \mathbb{I}_{-1} \neq \emptyset \\ \max K \leq 0 \leftrightarrow K \leq 0 \\ \max K \geq 0 \leftrightarrow K \cap \mathbb{I}_{1} \neq \emptyset \end{gathered} \tag{4}$$

Since

$$C_{0,0} = \min K \neq 0 \wedge \max K \neq 0$$

it follows with (2) that

$$(\min K \geq 0 \vee (\min K \leq 0 \wedge \max K \geq 0) \vee \max K \leq 0) \parallel C_{0,0}$$

Because of (4),

$$(\min K \geq 0 \vee (\min K \leq 0 \wedge \max K \geq 0) \vee \max K \leq 0) \to A(K)$$

So, we have that

$$A(K) \parallel C_{0,0}$$

The other cases follow similarly. Therefore we have

$$A(K) \parallel \bigvee_{i,j=0}^{1} C_{i,j}$$

and thus $A(K)$ because of (1).

So, we have that

$$\mathbf{S}_{\mathbf{K}} \subseteq \mathbf{G}_{\mathbf{K}} \subseteq \mathbf{S}^*_{\mathbf{K}},$$

which is quite unsatisfying as we want to compare the computational strength of both representations.

Let $\mathbf{G}^*$ coinductively be the largest fixed point of the operator

$$\Psi^*(X, x) \stackrel{\mathrm{Def}}{=} (x \neq 0 \to \overset{*}{\downdownarrows}(x \leq 0 \vee x \geq 0)) \wedge X(\mathbf{t}(x))$$

and $\mathbf{G}^*_{\mathbf{K}}$ coinductively be the largest fixed point of the operator

$$\Omega^*(X, K) \stackrel{\mathrm{Def}}{=} \mathbf{G}^*(\min K) \wedge \mathbf{G}^*(\max K) \wedge \\ (\forall d \in \mathbf{GC})\,(K \cap \mathbb{I}_d \neq \emptyset \to X(\mathbf{t}[K \cap \mathbb{I}_d])$$

Theorem

$\mathbf{S}^*_{\mathbf{K}} = \mathbf{G}^*_{\mathbf{K}}$ *is derivable in CFP (+ new rules)*