LOGIC FOR GRAY-CODE COMPUTATION

ULRICH BERGER AND KENJI MIYAMOTO AND HELMUT SCHWICHTENBERG
AND HIDEKI TSUIKI

Abstract. Gray-code is a well-known binary number system where neighboring values differ in one digit only. Tsuiki (2002) has introduced Gray code to the field of real number computation. He assigns to each number a unique $1\bot$-sequence, i.e., an infinite sequence of $\{-1, 1, \bot\}$ containing at most one copy of $\bot$ (meaning undefinedness). In this paper we take a logical and constructive approach to study real number computation based on Gray-code. Instead of Tsuiki's indeterministic multihead Type-2 machine, we use pre-Gray code, which is a representation of Gray-code as a sequence of constructors, to avoid the difficulty due to $\bot$ which prevents sequential access to a stream. We extract real number algorithms from proofs in an appropriate formal theory involving inductive and coinductive definitions. Examples are algorithms transforming pre-Gray code into signed digit code of real numbers, and conversely, the average for pre-Gray code and a translation of finite segments of pre-Gray code into its normal form. These examples are formalized in the proof assistant Minlog.

Keywords: Gray-code, real number computation, inductive and coinductive definitions, program extraction.

2010 Mathematics Subject Classification: 03D78, 03F60, 03B70, 03B35

1. Introduction

Gray-code (also called reflected binary code) is widely known in digital communication, due to its property that the Hamming distance between adjacent Gray-codes is always 1. Based on Gray-code, Di Gianantonio and Tsuiki studied independently an expansion of real numbers as infinite sequences of $\{0, 1, \bot\}$ each of which contains at most one $\bot$ standing for undefinedness [5, 12]. Tsuiki called it *modified Gray expansion*. He also studied computability of real numbers, and presented several algorithms to

This work was supported by the International Research Staff Exchange Scheme (IRSES) Nr. 612638 CORCON and Nr. 294962 COMPUTAL of the European Commission, the JSPS Core-to-Core Program, A. Advanced research Networks and JSPS KAKENHI Grant Number 15K00015.

do real number computation via Gray-code. The motivation of this paper is to shed light on the logical aspect of Gray-code computation from the constructive standpoint. We formalize Gray-code in the *Theory of Computable Functionals*, TCF in short, and also in the proof assistant Minlog[1], which is an implementation of TCF, by means of inductive and coinductive definitions [10]. In order to make use of Tsuiki's idea in TCF, we introduce pre-Gray code which is Gray-code represented as ordinary streams. Through the realizability interpretation we extract from proofs programs as terms in an extension T^+ of Gödel's T involving higher type recursion and corecursion operators. As case studies we extract real number algorithms in our setting of pre-Gray code. The correctness of the extracted programs is automatically ensured by the soundness theorem.

The rest of this paper is organized as follows. In Section 2 we investigate Gray-code and introduce pre-Gray code representation of real numbers. In Section 3 we describe realizability in our framework TCF, w.r.t. inductive and coinductive definitions. This provides a suitable setting to study logical aspects of signed digit streams and pre-Gray code. Section 4 presents proofs about coinductive representations that correspond to algorithms; the latter are described informally. 4.1 studies the average of two real numbers in signed digit code, and 4.4 directly for pre-Gray code. In 4.2 and 4.3 we give translators from pre-Gray into signed digit code, and vice versa. 4.5 studies a translation of finite segments of pre-Gray code into its normal form. Section 5 deals with the conversion of Gray-code to modified Gray expansion. In Section 6 we present and discuss the terms extracted from formalizations (in the proof assistant Minlog) of the proofs in Sections 4 and 5.

Related work. There are programming languages which can process modified Gray expansion directly. Tsuiki and Sugihara studied an extension of Haskell with the non-deterministic choice operator `gamb` which works as McCarthy's `amb` operator [14]. Tsuiki studied a logic programming language with guarded clauses and committed choice [13]. Terayama and Tsuiki studied an extension of PCF with parallelism [11]. In this paper we avoid using the above features by adopting pre-Gray code. Concerning stream based real arithmetic. Wiedmer [15, 16] used signed digit streams for real number computation. Its corecursive treatment was studied by Ciaffaglione and Di Gianantonio in Coq [4]. Berger and Seisenberger studied program extraction to obtain programs dealing with signed digit streams [2]. Some of

[1]See `http://www.minlog-system.de/`

their results are formalized by Miyamoto and Schwichtenberg in TCF and Minlog [7, 8]. Chuang studied the average and the multiplication of real numbers using coinduction in Agda via the Curry-Howard isomorphism [3].

2. Gray-code and its variations

2.1. **Expansions of real numbers.** We define binary expansion of the unit interval as the expansion of the unit[2] interval $\mathbb{I} = [-1, 1]$ as infinite sequences of $\mathbf{PSD} = \{-1, 1\}$ (proper signed digits) so that $v = a_1 a_2 \dots$ represents

$$\sum_{i=1}^{\infty} \frac{a_i}{2^i}. \tag{1}$$

With binary expansion, a finite sequence $a_1, a_2, \dots, a_n$ denotes the interval $f_{a_1}(f_{a_2} \dots (f_{a_n}(\mathbb{I}) \dots)$ for f_a the function

$$f_a(x) = \frac{x + a}{2},$$

and $a_1 a_2 \dots$ denotes the real number that belongs to the intersection of the intervals denoted by its finite truncations. Though binary expansion is simple and has little redundancy, it cannot be used for stream-based computation of the reals because, for example, the first digit of the number 0 cannot be determined by any arbitrary approximation information of the number. To remedy this, signed digit code is commonly used in real number computation. Signed digit code is a representation of the same interval with the same formula (1), but with three digits $\mathbf{SD} = \{-1, 0, 1\}$. In this paper, we view finite sequences of **SD** as a free algebra **I** with a nullary constructor $\mathsf{nil}_{\mathbf{I}}$ and three unary constructors $\mathrm{C}_{-1}, \mathrm{C}_0, \mathrm{C}_1$ of type $\mathbf{I} \to \mathbf{I}$. That is,

$$\mathbf{I} = \mathsf{nil}_{\mathbf{I}} + \mathrm{C}_{-1}\,\mathbf{I} + \mathrm{C}_0\,\mathbf{I} + \mathrm{C}_1\,\mathbf{I}.$$

Signed digit code has a lot of redundancy, as $\bar{1}1$ and $0\bar{1}$ represent the same interval $[-1/2, 0]$ and $1\bar{1}$ and 01 represent the same interval $[0, 1/2]$. Here, $\bar{1}$ is the notation of -1 in a sequence.

Modified Gray expansion is a unique representation of $\mathbb{I}$ that can be used for real number computation. It is based on Gray expansion which is another way of expanding $\mathbb{I}$ with **PSD**. In Gray expansion, the sequence is flipped after an appearance of 1. That is, let LR_a for $a \in \mathbf{PSD}$ be functions defined as

$$LR_a(x) = -a\frac{x - 1}{2} \tag{2}$$

[2]For simplicity we base our study on $[-1, 1]$ rather than $[0, 1]$.

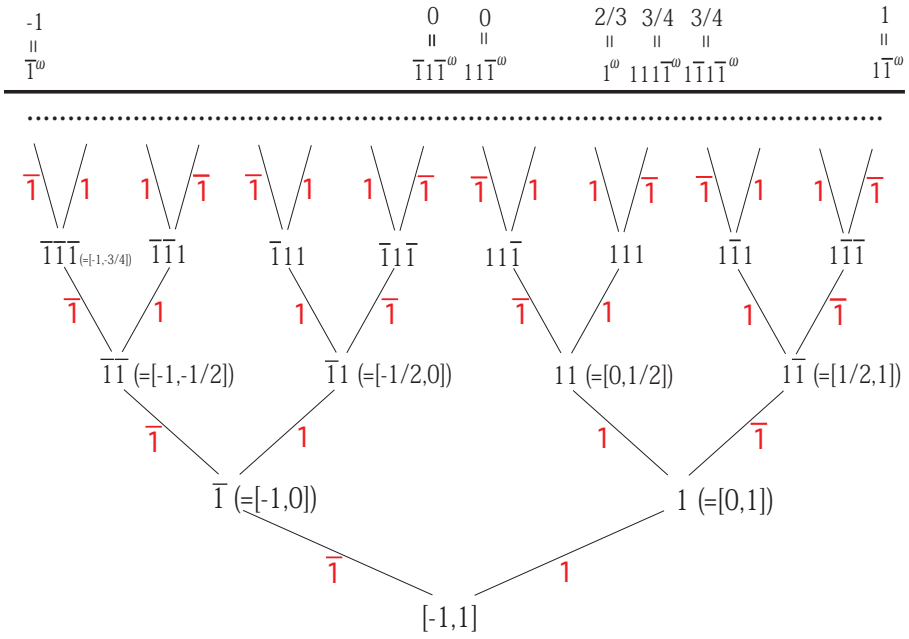

FIGURE 1. Gray expansion.

so that $LR_{-1} = f_{-1}$ but $LR_1(x) = f_1(-x)$ (Figure 2.1). Then, the number represented by a sequence $v = a_1 a_2 \dots$ is the limit of the shrinking intervals $LR_{a_1}(LR_{a_2} \dots (LR_{a_n}(\mathbb{I}) \dots)$ which is equal to

$$\sum_{i=1}^{\infty} \frac{-\prod_{j \le i}(-a_j)}{2^i}. \tag{3}$$

With Gray expansion, each dyadic rational number (i.e., $k/2^i$ for integers $-2^i \le k \le 2^i$) other than -1 and 1 is represented in two ways as is the case for the binary expansion. For example, 0 is expanded as $\bar{1}1\bar{1}^\omega$ and $11\bar{1}^\omega$. However, the two expansions differ only at one digit and the sequence after the digit they differ is always $1\bar{1}^\omega$. *Modified Gray expansion* assigns the $1\perp$-sequence $s\perp 1\bar{1}^\omega$ to a dyadic rational number which has two Gray expansions $s11\bar{1}^\omega$ and $s\bar{1}1\bar{1}^\omega$ for $s \in \{1, \bar{1}\}^*$ [12]. In this way, each real number in the unit interval is represented as a unique infinite $1\perp$-sequence, which is an infinite sequence of $\{-1, 1, \perp\}$ such that at most one copy of $\perp$ is contained in the sequence. In this paper, we consider its variant that assigns all three sequences $s11\bar{1}^\omega$, $s\bar{1}1\bar{1}^\omega$, and $s\perp 1\bar{1}^\omega$ to this dyadic rational number and

simply call it the *(infinite) Gray-code*. Gray-codes of real numbers in $[-1,1]$ range over the subset $\{1,\bar{1}\}^\omega \cup \{1,\bar{1}\}^*\bot 1\bar{1}^\omega$ of $\{-1,1,\bot\}^\omega$. We will also call each $1\bot$-sequence in this set an (infinite) Gray-code. The following table shows the difference of the three representations according to the character a allowed when a dyadic rational number is represented as $sa1\bar{1}^\omega$.

Gray expansion	$a \in \{-1,1\}$,
Modified Gray expansion	$a = \bot$,
Gray-code	$a \in \{-1,1,\bot\}$.

As we will study in Section 5, Gray-code and modified Gray expansion are equivalent in that a Gray-code can be coinductively converted to modified Gray expansion.

In order to define the meaning of Gray-codes more precisely, we introduce finite Gray-codes. A *finite* $1\bot$*-sequence* of length n is an infinite sequence $t = t_0t_1\ldots$ of $\{-1,1,\bot\}$ such that $t_{n-1} \neq \bot$, $t_k = \bot$ for $k \geq n$, and $t_k = \bot$ for at most one $k < n$. We sometime omit the suffix $\bot^\omega$ of a finite $1\bot$-sequence and write it as a sequence of $\{-1,1,\bot\}$ of length n. We call a finite $1\bot$-sequence in $\{1,\bar{1}\}^* \cup \{1,\bar{1}\}^*\bot 1\bar{1}^*$ a *finite Gray-code*. We define the order generated by $\bot \sqsubseteq -1$ and $\bot \sqsubseteq 1$ on $\{-1,1,\bot\}$, and its product order on $\{-1,1,\bot\}^\omega$. The set of finite/infinite $1\bot$-sequences form a Scott-Ershov domain BD with compact elements finite $1\bot$-sequences. Similarly, finite/infinite Gray-codes form a Scott-Ershov domain RD with compact elements finite Gray-codes. We say that a finite $1\bot$-sequence t approximates a $1\bot$-sequence s if $t \sqsubseteq s$.

We can define the meaning of Gray-code based on this domain structure. The meaning $[\![s]\!]$ of a finite Gray-code s is the same interval as the meaning of s with Gray expansion if $s \in \{\bar{1},1\}^*$, and is the union of $[\![s'\bar{1}1\bar{1}^n]\!]$ and $[\![s'11\bar{1}^n]\!]$ if s has the form $s'\bot 1\bar{1}^n$ for $s' \in \{\bar{1},1\}^*$. The meaning $[\![t]\!]$ of an infinite Gray-code t is the unique real number that belongs to the intersection of $[\![s]\!]$ for s finite Gray-codes that approximate t. The following proposition is immediate from the definition.

Proposition 2.1.

(a) For $t \in \{-1,1\}^\omega$, $[\![t]\!]$ is the same as the value obtained by (3).
(b) For $s\bot 10^\omega$ with $s \in \{-1,1\}^*$, $[\![s\bot 10^\omega]\!] = [\![s010^\omega]\!] = [\![s110^\omega]\!]$.

2.2. **An algebra of $\bot$-sequences.** Note that $\bot$ is not an ordinary character and a machine cannot read or write a $\bot$ on a tape. In [12] an IM2-machine (indeterministic multihead Type-2 machine) was introduced to input and output $1\bot$-sequences. An IM2-machine has two heads on each input/output tape so that it can skip a $\bot$ and access the rest the sequence.

In this paper, instead of such a direct manipulation of $1\bot$-sequences, we define pre-Gray code, which is a "representation" of Gray-code as sequences of constructors representing how an $1\bot$-sequence is obtained, and consider computation through usual stream programs instead of IM2-machines.

Before introducing pre-Gray code, we introduce an algebra $\mathbf{OB} = (|\mathbf{OB}|, C \cup \{\mathsf{nil}\})$ of finite $1\bot$-sequences. The carrier set $|\mathbf{OB}|$ is the set of finite $1\bot$-sequences. It is generated by four unary constructors in $C := \{\mathsf{cons}_1, \mathsf{cons}_{-1}, \mathsf{ins}_1, \mathsf{ins}_{-1}\}$ as well as a nullary constructor nil. Recall that an ordinary binary sequence is a term of a free algebra with two unary constructors cons_a for $a \in \{-1, 1\}$ which prepend a to a sequence as well as nil. On the other hand, a $1\bot$-sequence is generated by two additional constructors ins_a for $a \in \{-1, 1\}$ which insert a as the second character to a sequence.

Example 2.2. The term $\mathsf{ins}_1(\mathsf{ins}_{-1}(\mathsf{cons}_{-1}(\mathsf{ins}_1\,\mathsf{nil})))$ denotes $\bar{1}1\bar{1}\bot1$:

$$\begin{aligned}
\mathsf{nil} &\quad \text{denotes} \quad \bot^\omega,\\
(\mathsf{ins}_1\,\mathsf{nil}) &\quad \text{denotes} \quad \bot1\bot^\omega,\\
(\mathsf{cons}_{-1}(\mathsf{ins}_1\,\mathsf{nil})) &\quad \text{denotes} \quad \bar{1}\bot1\bot^\omega,\\
(\mathsf{ins}_{-1}(\mathsf{cons}_{-1}(\mathsf{ins}_1\,\mathsf{nil}))) &\quad \text{denotes} \quad \bar{1}\bar{1}\bot1\bot^\omega,\\
(\mathsf{ins}_1(\mathsf{ins}_{-1}(\mathsf{cons}_{-1}(\mathsf{ins}_1\,\mathsf{nil})))) &\quad \text{denotes} \quad \bar{1}1\bar{1}\bot1\bot^\omega.
\end{aligned}$$

When writing a term of $\mathbf{OB}$, we omit nil and write it as a sequence of C. Thus, we write $[\mathsf{ins}_1, \mathsf{ins}_{-1}, \mathsf{cons}_{-1}, \mathsf{ins}_1]$ for this term. One can calculate that $[\mathsf{cons}_{-1}, \mathsf{cons}_1, \mathsf{cons}_{-1}, \mathsf{ins}_1]$ also denotes the same $1\bot$-sequence.

We write $\varphi(p)$ for the $1\bot$-sequence denoted by $p \in C^*$. More precisely, $\varphi([c_1, \ldots, c_n]) = (c_1 \circ \cdots \circ c_n)(\bot^\omega)$.

For coalgebraic computation, one needs to read sequences of constructors from left to right. If a sequence of C is read from left to right, then it can be considered as a procedure to construct a $1\bot$-sequence as follows. We start with an infinite tape with the state $\bot^\omega$. We view cons_a as the operation to fill the leftmost $\bot$ with a and ins_a as the operation to fill the second $\bot$ from the left with a.

We write $\psi(p)$ for the $1\bot$-sequence obtained by this procedure. More precisely, if we define $c' \colon \{-1, 1, \bot\}^\omega \to \{-1, 1, \bot\}^\omega$ $(c \in C)$ by

$$\begin{aligned}
\mathsf{cons}'_a(s) &= \text{ filling in } s \text{ the first bottom from the left by } a\\
\mathsf{ins}'_a(s) &= \text{ filling in } s \text{ the second bottom from the left by } a
\end{aligned}$$

then $\psi([c_1, \ldots, c_n]) = (c'_n \circ \cdots \circ c'_1)(\bot^\omega)$.

Example 2.3. We construct $\bar{1}1\bar{1}\bot1$ according to $[\mathsf{cons}_{-1}, \mathsf{cons}_1, \mathsf{cons}_{-1}, \mathsf{ins}_1]$ as $\bot^\omega \to \bar{1}\bot^\omega \to \bar{1}1\bot^\omega \to \bar{1}1\bar{1}\bot^\omega \to \bar{1}1\bar{1}\bot1\bot^\omega$ and according to $[\mathsf{ins}_1, \mathsf{ins}_{-1}, \mathsf{cons}_{-1}, \mathsf{ins}_1]$ as $\bot^\omega \to \bot1\bot^\omega \to \bot1\bar{1}\bot^\omega \to \bar{1}1\bar{1}\bot^\omega \to \bar{1}1\bar{1}\bot1\bot^\omega$.

Proposition 2.4. *$\varphi(p) = \psi(p)$ for $p \in C^*$.*

Proof. We show that

$$(c_1 \circ \cdots \circ c_n)(\bot^\omega) = (c'_n \circ \cdots \circ c'_1)(\bot^\omega). \tag{4}$$

Note that c' satisfies the equations

$$\begin{aligned} c'(b : s) &= b : c'(s)\ (b \neq \bot), \\ \mathsf{cons}'_a(\bot : s) &= a : s, \\ \mathsf{ins}'_a(\bot : s) &= \bot : \mathsf{cons}'_a(s). \end{aligned}$$

Using the equations for c and c' one easily verifies that

$$c(\bot^\omega) = c'(\bot^\omega), \tag{5}$$

$$c \circ d' = d' \circ c. \tag{6}$$

From (6) one obtains

$$(c_1 \circ \cdots \circ c_n) \circ c' = c' \circ (c_1 \circ \cdots \circ c_n) \tag{7}$$

by induction on n. Now (7) and (5) yield (4), again by induction on n. □

Note that c' is increasing. That is, $s \sqsubseteq c'(s)$ for $c \in C$. Therefore, we can consider an infinite sequence $q \in C^\omega$ of the four constructors cons_1, $\mathsf{cons}\bar{1}$, ins_1, $\mathsf{ins}_{\bar{1}}$ as representing an infinite $1\bot$-sequence which is obtained as the least upper bound of $\{\, \varphi(p)(= \psi(p)) \mid p \text{ is a finite prefix of } q \,\}$. For example, $[\mathsf{ins}_1, \mathsf{ins}_{-1}, \mathsf{ins}_{-1}, \mathsf{ins}_{-1}, \dots]$ represents $\bot1\bar{1}^\omega$. We write $\varphi(q)$ for the $1\bot$-sequence represented by $q \in C^\omega$.

As we have noted, the algebra **OB** is not a free algebra and we have equations

$$\mathsf{ins}_a \circ \mathsf{cons}_b = \mathsf{cons}_b \circ \mathsf{cons}_a \tag{8}$$

for $a, b \in \mathbf{PSD}$. Actually, **OB** is the universal algebra in that the set of finite $1\bot$-sequences is equal to the quotient of C^* by these equations.

2.3. **An algebra of Gray-code and an auxiliary algebra.** Recall that finite Gray-codes form a subset $\{\bar{1}, 1\}^* \cup \{\bar{1}, 1\}^*\bot1\bar{1}^*$ of the set of finite $1\bot$-sequences. In order to represent only this set of finite Gray-codes, we define a subalgebra **G** of **OB** simultaneously with another subalgebra **H**. The

carrier set of $\mathbf{G}$ is the set of finite Gray-codes. A naive attempt is to define them as follows.

$$\begin{aligned}\mathbf{G} &= (\{\bar{1},1\}^* \cup \{\bar{1},1\}^*\bot 1\bar{1}^*,\\ &\qquad \{\,\mathsf{cons}_a\colon \mathbf{G}\to\mathbf{G} \mid a\in\mathbf{PSD}\,\}\cup\{\mathsf{ins}_1\colon \mathbf{H}\to\mathbf{G}, \mathsf{nil}_{\mathbf{G}}\colon \mathbf{G}\})\\ \mathbf{H} &= (\bot\bar{1}^*,\ \{\mathsf{ins}_{-1}\colon \mathbf{H}\to\mathbf{H}, \mathsf{nil}_{\mathbf{H}}\colon \mathbf{H}\})\end{aligned}$$

However, this definition does not allow filling a bottom with a digit by the cons_a constructor in the coinductive treatment of an $1\bot$-sequence. For this purpose, we need to add the constructors $\mathsf{cons}_a\colon \mathbf{G}\to\mathbf{H}$ for $a\in\mathbf{PSD}$ to the above definition. In order to distinguish the two constructors cons_a of types $\mathbf{G}\to\mathbf{G}$ and $\mathbf{G}\to\mathbf{H}$, we give them different names LR_a and Fin_a. We also rename ins_1 and ins_{-1} to U and D, respectively, and define the two algebras $\mathbf{G}$ and $\mathbf{H}$ with carrier sets $|\mathbf{G}| = \{\bar{1},1\}^*\cup\{\bar{1},1\}^*\bot 1\bar{1}^*$ and $|\mathbf{H}| = \{\bar{1},1\}^+\cup\{\bar{1},1\}^+\bot 1\bar{1}^*\cup\bot\bar{1}^*$ mutually recursively as follows.

$$\begin{aligned}\mathbf{G} &= (|\mathbf{G}|,\ \{\,\mathrm{LR}_a\colon \mathbf{G}\to\mathbf{G} \mid a\in\mathbf{PSD}\,\}\cup\{\mathrm{U}\colon \mathbf{H}\to\mathbf{G}, \mathsf{nil}_{\mathbf{G}}\colon \mathbf{G}\})\\ \mathbf{H} &= (|\mathbf{H}|,\ \{\,\mathrm{Fin}_a\colon \mathbf{G}\to\mathbf{H} \mid a\in\mathbf{PSD}\,\}\cup\{\mathrm{D}\colon \mathbf{H}\to\mathbf{H}, \mathsf{nil}_{\mathbf{H}}\colon \mathbf{H}\})\end{aligned}$$

Note that the carrier sets of both algebras are generated (but not freely) by their constructors. We call a term of type $\mathbf{G}$ a *finite pre-Gray code*.

In the coinductive treatment of an $1\bot$-sequence, $\mathrm{U}\colon \mathbf{H}\to\mathbf{G}$ means to leave the current cell *U*ndefined and fill the next cell with 1, $\mathrm{D}\colon \mathbf{H}\to\mathbf{H}$ means to *D*elay the determination of the value of the unfilled cell and add $\bar{1}$ to the end of the sequence, and Fin_a means to *Fin*ally fill the unfilled cell with a. Thus, both $\mathrm{U}(\mathrm{D}(\mathrm{Fin}_{-1}(\mathrm{U}(\mathsf{nil}_{\mathbf{H}}))))$ and $\mathrm{LR}_{-1}(\mathrm{LR}_1(\mathrm{LR}_{-1}(\mathrm{U}(\mathsf{nil}_{\mathbf{H}}))))$ are terms of type $\mathbf{G}$ representing the sequence $\bar{1}1\bar{1}\bot 1$.

We call an infinite sequence of these constructors all of whose finite truncations are term of type $\mathbf{G}$ an infinite term of type $\mathbf{G}$, and similary, define an infinite term of $\mathbf{H}$. An infinite term p of type $\mathbf{G}$ is representing an infinite Gray-code $\varphi(p)$ and thus representing a real number $[\![p]\!]\in\mathbb{I}$ defined as $[\![\varphi(p)]\!]$. For example, for $p=[\mathrm{U},\mathrm{D},\mathrm{D},\dots]$, $\varphi(p)=\bot 1\bar{1}^\omega$ and $[\![p]\!]=0$. We call an infinite term of type $\mathbf{G}$ an *(infinite) pre-Gray code*.

Since cons_a, and ins_a satisfy (8), the constructors of $\mathbf{G}$ and $\mathbf{H}$ satisfy the following equations for $a\in\mathbf{PSD}$.

$$\mathrm{U}\circ\mathrm{Fin}_a = \mathrm{LR}_a\circ\mathrm{LR}_1, \tag{9}$$

$$\mathrm{D}\circ\mathrm{Fin}_a = \mathrm{Fin}_a\circ\mathrm{LR}_{-1}. \tag{10}$$

We show that the set of finite Gray-codes is the quotient of the term algebra of $\mathbf{G}$ with these equations.

Proposition 2.5. *Let p be a term of type* **G** *and $a_i \in$* **PSD** *$(1 \le i \le m)$.*

(a) If $\varphi(p) = a_1 \dots a_m \bot 1\bar{1}^l$, the equation $p = [\mathrm{LR}_{a_1}, \dots, \mathrm{LR}_{a_m}, \mathrm{U}, \mathrm{D}^l]$ can be derived from (9) *and* (10).

(b) If $\varphi(p) = a_1 \dots a_m$, the equation $p = [\mathrm{LR}_{a_1}, \dots, \mathrm{LR}_{a_m}]$ can be derived from (9) *and* (10).

Proof. Let $p = [c_1, \dots, c_n]$. We have $n = l + m$ because each constructor adds one digit to a sequence. Suppose that the argument type of c_i is **H** for $i \ge k$ and the return type of c_k is **G**. Then, from the definition of **G** and **H**, we have $k = m + 1$ and $c_k, \dots, c_n$ are uniquely determined as $c_k = \mathrm{U}$ and $c_i = \mathrm{D}$ for $i > k$. Therefore, (a) is immediately derived from (b). We prove (b) by induction on m. If $m = 0$, then $p = \mathsf{nil}_{\mathbf{G}}$ and this statement holds. Suppose that $c_m = \mathrm{LR}_b$. Since $\varphi(p) = \psi(p)$ by Proposition 2.4, $a_m = b$ and $\varphi([c_1, \dots, c_{m-1}]) = a_1 \dots a_{m-1}$. Therefore, it holds by the induction hypothesis. Suppose that $c_m = \mathrm{Fin}_b$. Since the argument type of c_{m-1} is **H**, p has the form $[c_1, \dots, c_{m-k-2}, \mathrm{U}, \mathrm{D}^k, \mathrm{Fin}_b]$. By induction hypothesis, $[c_1, \dots, c_{m-k-2}] = [\mathrm{LR}_{a_1}, \dots, \mathrm{LR}_{a_{m-k-2}}]$ is derived. On the other hand, $[\mathrm{U}, \mathrm{D}^k, \mathrm{Fin}_b] = [\mathrm{LR}_b, \mathrm{LR}_1, \mathrm{LR}_{-1}^k]$ is derived by applying (10) k times and then applying (9). Thus, (b) is proved. □

2.4. **Pre-Gray code.** As we defined, Gray-codes are representations of $\mathbb{I}$ as $\{-1, 1, \bot\}$-sequences and pre-Gray codes are terms of the algebra **G** of Gray-codes. For our study of real number computation based on pre-Gray code, we redefine **G** and **H** as free algebras and assign affine functions f_c to unary constructors c of **G** and **H** so that one can directly define meanings of pre-Gray codes.

First, since $\mathsf{nil}_{\mathbf{G}}$ and $\mathsf{nil}_{\mathbf{H}}$ express the empty $1\bot$-sequence, they denote the unit interval $\mathbb{I}$. It is natural to define f_{LR_a} and f_{U} as

$$f_{\mathrm{LR}_a} = -a\frac{x-1}{2} \ (= LR_a \text{ in (2)}), \tag{11}$$

$$f_{\mathrm{U}}(x) = \frac{x}{2}. \tag{12}$$

Since (9) and (10) hold, f_{Fin_a} and f_{D} should satisfy

$$f_{\mathrm{U}} \circ f_{\mathrm{Fin}_a} = f_{\mathrm{LR}_a} \circ f_{\mathrm{LR}_1}, \tag{13}$$

$$f_{\mathrm{D}} \circ f_{\mathrm{Fin}_a} = f_{\mathrm{Fin}_a} \circ f_{\mathrm{LR}_{-1}}. \tag{14}$$

From (13), we have

$$f_{\mathrm{Fin}_a}(x) = a\frac{x+1}{2} = f_{\mathrm{LR}_a}(-x), \tag{15}$$

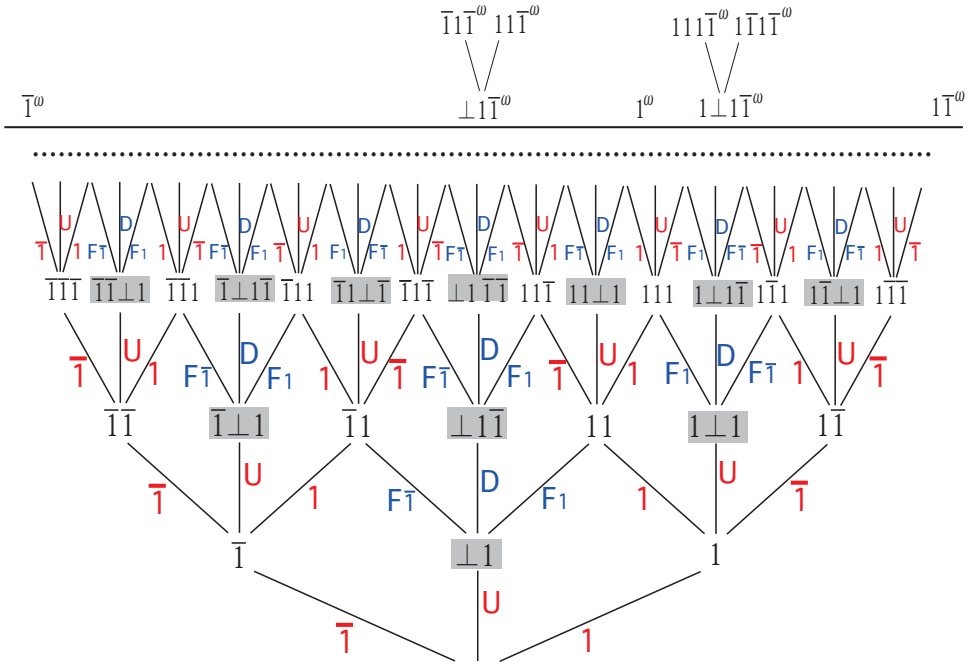

FIGURE 2. The domain RD and constructors of pre-Gray code. Here, $\mathrm{LR}_{-1}, \mathrm{LR}_1, \mathrm{U}, \mathrm{Fin}_{-1}, \mathrm{Fin}_1$, and D are written as $\overline{1}, 1, \mathrm{U}, \mathrm{F}\overline{1}, \mathrm{F}1$, and D, respectively.

and therefore from (14), we have

$$f_{\mathrm{D}}(x) = \frac{x}{2}. \tag{16}$$

Equations (11), (12), (15), and (16) define the meanings of constructors as affine functions, and they define the meaning $F_{\mathbf{G}}(p)$ of a term $p = [c_1, \ldots, c_n]$ of type $\mathbf{G}$ as

$$F_{\mathbf{G}}(p) = f_{c_1}(f_{c_2}(\ldots f_{c_n}(\mathbb{I})\ldots)). \tag{17}$$

They also define the meaning $F_{\mathbf{H}}(q)$ of a term q of type $\mathbf{H}$ similarly. Therefore, they define meanings $F_{\mathbf{G}}(p)$ and $F_{\mathbf{H}}(q)$ of infinite terms p of type $\mathbf{G}$ and q of type $\mathbf{H}$, respectively, as the unique elements which belong to intersections of the meanings of their finite prefixes (Figure 2).

Proposition 2.6. *For a (possibly infinite) term p of type $\mathbf{G}$, we have $[\![p]\!] = F_{\mathbf{G}}(p)$.*

Proof. We first prove the statement for the case that p is finite. Since equations (13) and (14) hold, we only need to consider the cases $p = [\mathrm{LR}_{a_1}, \ldots, \mathrm{LR}_{a_m}, \mathrm{U}, \mathrm{D}^n]$ and $p = [\mathrm{LR}_{a_1}, \ldots, \mathrm{LR}_{a_m}]$ by Proposition 2.5. The latter case is immediate from the definition. In the former case, we have $\varphi(p) = a_1 \ldots a_m \bot 1\bar{1}^n$. Let $g = f_{\mathrm{LR}_{a_1}} \circ \cdots \circ f_{\mathrm{LR}_{a_m}}$. We have

$$\begin{aligned}
[\![p]\!] &= [\![a_1 \ldots a_m \bar{1} 1 \bar{1}^n]\!] \cup [\![a_1 \ldots a_m 1 1 \bar{1}^n]\!] \\
&= g(f_{\mathrm{LR}_{-1}} \circ f_{\mathrm{LR}_1} \circ f^n_{\mathrm{LR}_{-1}}(\mathbb{I})) \cup g(f_{\mathrm{LR}_1} \circ f_{\mathrm{LR}_1} \circ f^n_{\mathrm{LR}_{-1}}(\mathbb{I})) \\
&= g([-1/2^{n+1}, 0]) \cup g([0, 1/2^{n+1}]) \\
&= g([-1/2^{n+1}, 1/2^{n+1}]) \\
&= (g \circ f_{\mathrm{U}} \circ f^n_{\mathrm{D}})(\mathbb{I}) \\
&= F_{\mathbf{G}}([\mathrm{LR}_{a_1}, \ldots, \mathrm{LR}_{a_m}, \mathrm{U}, \mathrm{D}^n]).
\end{aligned}$$

The case p is infinite is immediately derived from the finite case. □

Note that the meaning $F_{\mathbf{H}}(p)$ of a term p of type $\mathbf{H}$ is also defined. If p is a term of type $\mathbf{H}$, then $\varphi(p)$ may not be a finite Gray-code and even if it is, $F_{\mathbf{H}}(p)$ is different from $[\![\varphi(p)]\!]$ in general. For example, $\varphi([\mathrm{D}]) = \bot\bar{1}$ and $[\![\bar{1}\bar{1}]\!] \cup [\![1\bar{1}]\!] = [-1, -1/2] \cup [1/2, 1]$ is not an interval, and $[\![\varphi([\mathrm{Fin}_1, \mathrm{LR}_1])]\!] = [\![11]\!] = [0, 1/2]$ whereas $F_{\mathbf{H}}([\mathrm{Fin}_1, \mathrm{LR}_1]) = [1/2, 1]$.

The meaning $F_{\mathbf{H}}$ of $\mathbf{H}$ defines another representation of $\mathbb{I}$ which is obtained by flipping the second digit of Gray code (Figure 3). We extract conversion programs between these two representations from the proof of Lemma 4.10 in Section 4.4.

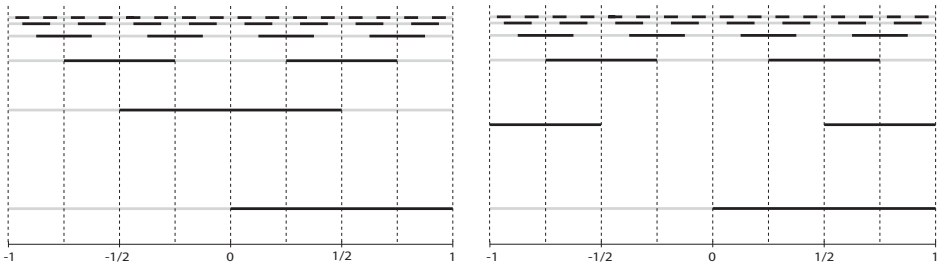

FIGURE 3. Expansion by G (i.e., Gray expansion) and expansion by H.

We defined an infinite term of type $\mathbf{G}$ as an infinite sequence of constructors of $\mathbf{G}$ and $\mathbf{H}$ such that any truncation of the sequence forms a finite

term of type **G**. In TCF, infinite structures like this can be treated as cototal ideals. Each algebra definition of TCF generates a basic domain of the Scott-Ershov model of partial continuous functionals. Among the ideals of such a domain we single out the total and cototal ones, which are our well-founded and non-well-founded objects, respectively. For the details, please consult [10]. For our algebras **I**, **G**, and **H**, every total ideal is a finite term and every cototal ideal is an infinite term of the algebra.

The notion of a cototal ideal also makes sense when the underlying algebra does *not* have nullary constructors. Since we will only be concerned with cototal ideals we take advantage of this fact and from now on omit the nullary constructor from our algebras. This will simplify the arguments below considerably (for instance in comparison with [8]). We also redefine our free algebras **I**, **G** and **H** so that **I** has a binary constructor C of type $\mathbf{SD} \to \mathbf{I} \to \mathbf{I}$ and so on; the intention is $\mathrm{LR}_a(p) = \mathrm{LR}(a, p)$. To sum up, our algebras have the following definitions.

$$\begin{aligned}\mathbf{I} &= \mathrm{C}\ \mathbf{SD}\ \mathbf{I},\\ \mathbf{G} &= \mathrm{LR}\ \mathbf{PSD}\ \mathbf{G}\ +\ \mathrm{U}\ \mathbf{H},\\ \mathbf{H} &= \mathrm{Fin}\ \mathbf{PSD}\ \mathbf{G}\ +\ \mathrm{D}\ \mathbf{H}.\end{aligned}$$

3. Coinductive representation of Gray-code via realizability

A constructive proof of a formula A can be viewed as a solution to the problem posed by A [6]. Such a solution is a (computable) function of a certain type $\tau(A)$ determined by the formula A. For example, $\forall_n \exists_m(\mathrm{Prime}(m) \wedge m > n)$ has type $\mathbf{N} \to \mathbf{N}$. Sometimes the solution is only a verification, like for $\forall_{n_1,n_2,n_3>0,m>2}(n_1^m + n_2^m \neq n_3^m)$. In such cases a solution has no computational content and the formula A is called non-computational (n.c., or Harrop); the other ones are called computationally relevant (c.r.). The only way c.r. formulas can arise is via inductively defined predicates, like I or ${}^{\mathrm{co}}I$ below (we consider $\exists_x A$ and $A \vee B$ as inductively defined). The clauses of the inductive definition determine the data type (free algebra) of a solution or "realizer". It is essential that we allow non-computational universal quantifiers $\forall^{\mathrm{nc}}$ [1] to obtain the desired data type. For instance, in the clause $\forall_x^{\mathrm{nc}} \forall_d(I(x) \to I(\frac{x+d}{2}))$ $(d \in \{-1, 0, 1\})$ for I one is not interested in the real number x as input, but only in how the digit d gives rise to a new element of I. Here we work in such a constructive arithmetical theory with realizability (called TCF in [10]).

We want to extract algorithms for real number computation from proofs in an appropriate formal theory involving coinductive definitions. The idea

is to leave infinite streams implicit, as realizers of atomic propositions on reals. For example, consider the problem to compute the average of two real numbers coded by infinite streams. We will coinductively define a unary predicate ${}^{\mathrm{co}}I$ and prove

$$\forall^{\mathrm{nc}}_{x,x'}({}^{\mathrm{co}}I(x) \to {}^{\mathrm{co}}I(x') \to {}^{\mathrm{co}}I(\frac{x+x'}{2})) \tag{18}$$

(recall that $\forall^{\mathrm{nc}}$ indicates that the reals x, x' have no computational significance, only the assumptions ${}^{\mathrm{co}}I(x)$, ${}^{\mathrm{co}}I(x')$ have). Associated with ${}^{\mathrm{co}}I$ is its "realizability extension" $({}^{\mathrm{co}}I)^{\mathbf{r}}$, a relation between streams v of signed digits and real numbers x. We can understand $({}^{\mathrm{co}}I)^{\mathbf{r}}(v,x)$ as saying that v is a stream representation of x witnessing ${}^{\mathrm{co}}I(x)$. The soundness theorem gives

$$({}^{\mathrm{co}}I)^{\mathbf{r}}(v,x) \to ({}^{\mathrm{co}}I)^{\mathbf{r}}(v',x') \to ({}^{\mathrm{co}}I)^{\mathbf{r}}(f(v,v'), \frac{x+x'}{2})$$

for some function f extracted from the proof. The function is the stream transformer for the average, and it is obtained (together with a proof of its correctness) from the proof of (18), which never mentions streams.

Now what is the predicate ${}^{\mathrm{co}}I$? Consider the operator

$$\Phi(X) := \{\, x \mid \exists^{\mathrm{r}}_{x' \in X} \exists_d (x = \frac{x'+d}{2}) \,\},$$

where d ranges over $\mathbf{SD} := \{-1, 0, 1\}$. The ${}^{\mathrm{r}}$ in $\exists^{\mathrm{r}}$ (not to be confused with the $^{\mathbf{r}}$ in $({}^{\mathrm{co}}I)^{\mathbf{r}}$) indicates that the quantified variable x' has no computational significance, only the kernel of the existential formula has. Since $\Phi(X)$ is stricly positive in X, our underlying theory provides us with unary predicates (or sets; they are not distinguished) I and ${}^{\mathrm{co}}I$ for the least and greatest fixed point of Φ:

$$\begin{aligned} I &:= \mu_X \Phi(X) && \text{least fixed point} \\ {}^{\mathrm{co}}I &:= \nu_X \Phi(X) && \text{greatest fixed point} \end{aligned}$$

satisfying the (strengthened) axioms

$$\begin{aligned} \Phi(I \cap X) \subseteq X \to I \subseteq X && \quad \text{induction} \\ X \subseteq \Phi({}^{\mathrm{co}}I \cup X) \to X \subseteq {}^{\mathrm{co}}I && \quad \text{coinduction} \end{aligned}$$

(they are called "strengthened" because their hypotheses are weaker than the fixed point property $\Phi(X) = X$).

The realizability extensions $I^{\mathbf{r}}$ and $({}^{\mathrm{co}}I)^{\mathbf{r}}$ are binary predicates on streams v of signed digits (coming from $\exists_d$ in the definition of $\Phi(X)$) and real numbers x. Consider the operator

$$\Phi^{\mathbf{r}}(Y) := \{\, (v,x) \mid \exists^{\mathrm{u}}_{(v',x')\in Y} \exists_d (x = \frac{x'+d}{2} \wedge v = \mathrm{C}_d(v'))\,\}$$

(the $^{\mathrm{u}}$ in $\exists^{\mathrm{u}}$ indicates that neither the quantified variable nor the kernel has computational significance). Since $\Phi^{\mathbf{r}}(Y)$ is strictly positive in Y, again our underlying theory provides us with binary predicates (or relations) $I^{\mathbf{r}}$ and $({}^{\mathrm{co}}I)^{\mathbf{r}}$ for the least and greatest fixed point of $\Phi^{\mathbf{r}}$:

$$\begin{aligned} I^{\mathbf{r}} &:= \mu_Y \Phi^{\mathbf{r}}(Y) && \text{least fixed point} \\ ({}^{\mathrm{co}}I)^{\mathbf{r}} &:= \nu_Y \Phi^{\mathbf{r}}(Y) && \text{greatest fixed point} \end{aligned}$$

satisfying the (strengthened) axioms

$$\begin{aligned} \Phi^{\mathbf{r}}(I^{\mathbf{r}} \cap Y) \subseteq Y \to I^{\mathbf{r}} \subseteq Y && \text{induction} \\ Y \subseteq \Phi^{\mathbf{r}}(({}^{\mathrm{co}}I)^{\mathbf{r}} \cup Y) \to Y \subseteq ({}^{\mathrm{co}}I)^{\mathbf{r}} && \text{coinduction.} \end{aligned}$$

The following proposition states that the definition of ${}^{\mathrm{co}}I$ is correct in the sense that the realizers of ${}^{\mathrm{co}}I(x)$ are exactly the signed digit representations of x.

Proposition 3.1. *For $v = a_1 a_2 \ldots \in \mathbf{SD}^\omega$ and $x \in \mathbb{I}$*

$$({}^{\mathrm{co}}I)^{\mathbf{r}}(v,x) \leftrightarrow x \in \bigcap_{n=1}^{\infty} f_{a_1}(f_{a_2}(\ldots f_{a_n}(\mathbb{I})\ldots))$$

Proof. For the direction from left to right we show

$$\forall_{v,x}(({}^{\mathrm{co}}I)^{\mathbf{r}}(v,x) \to v = a_1 a_2 \ldots \wedge x \in f_{a_1}(f_{a_2}(\ldots f_{a_n}(\mathbb{I})\ldots)))$$

by induction on n. For $n = 0$ this holds since $x \in \mathbb{I}$. For $n+1$ suppose that $({}^{\mathrm{co}}I)^{\mathbf{r}}(v,x)$ holds. Then, since $({}^{\mathrm{co}}I)^{\mathbf{r}}$ is a fixed point of $\Phi^{\mathbf{r}}$,

$$\exists_{v',x',a_1}(({}^{\mathrm{co}}I)^{\mathbf{r}}(v',x') \wedge x = f_{a_1}(x') \wedge v = \mathrm{C}_{a_1}(v')).$$

Let $v' = a_2 a_3 \ldots$. By induction hypothesis, $x' \in f_{a_2}(f_{a_3}(\ldots f_{a_{n+1}}(\mathbb{I})\ldots))$. We have $v = \mathrm{C}_{a_1}(v') = a_1 a_2 \ldots$ and $x \in f_{a_1}(f_{a_2} \ldots (f_{a_{n+1}}(\mathbb{I}))\ldots)$.

The direction from right to left is shown by coinduction. Setting

$$\{\, (v,x) \mid v = a_1 a_2 \ldots,\ x \in f_{a_1}(f_{a_2}(\ldots f_{a_n}(\mathbb{I})\ldots)) \text{ for every } n \,\}$$

it suffices to show $P \subseteq \Phi^{\mathbf{r}}(P)$. Assume $(v,x) \in P$. Set $x' := 2x - a_1$ and $v' := a_2 a_3 \ldots$. Then clearly $P(v',x')$, $x = \frac{x'+a_1}{2}$ and $v = a_1 v' = \mathrm{C}_{a_1}(v')$. Hence $(v,x) \in \Phi^{\mathbf{r}}(P)$. □

For Gray-code we proceed similarly; for brevity only for the infinite case. We now need two predicates ${}^{\mathrm{co}}G$ and ${}^{\mathrm{co}}H$ instead of ${}^{\mathrm{co}}I$. The corresponding operators Γ, Δ are defined by

$$\Gamma(X,Y) := \{\, y \mid \exists^{\mathrm{r}}_{x\in X}\exists_a(y = -a\frac{x-1}{2}) \vee \exists^{\mathrm{r}}_{x\in Y}(y = \frac{x}{2}) \,\},$$
$$\Delta(X,Y) := \{\, y \mid \exists^{\mathrm{r}}_{x\in X}\exists_a(y = a\frac{x+1}{2}) \vee \exists^{\mathrm{r}}_{x\in Y}(y = \frac{x}{2}) \,\}$$

and we define $({}^{\mathrm{co}}G, {}^{\mathrm{co}}H) := \nu_{(X,Y)}(\Gamma(X,Y),\Delta(X,Y))$. This is understood as the greatest fixed point of (Γ,Δ), expressed by the (strengthened) simultaneous coinduction axiom

$$(X,Y) \subseteq (\Gamma({}^{\mathrm{co}}G \cup X, {}^{\mathrm{co}}H \cup Y), \Delta({}^{\mathrm{co}}G \cup X, {}^{\mathrm{co}}H \cup Y)) \to (X,Y) \subseteq ({}^{\mathrm{co}}G, {}^{\mathrm{co}}H),$$

where inclusion $\subseteq$ is meant component-wise.

For later use we note immediate consequences of the fact that $({}^{\mathrm{co}}G, {}^{\mathrm{co}}H)$ is a (simultaneous) fixed point of (Γ,Δ), CoGClause and CoGClauseInv:

$$\forall^{\mathrm{nc}}_x({}^{\mathrm{co}}G(x) \to \exists^{\mathrm{r}}_{x'\in {}^{\mathrm{co}}G}\exists_a(x = -a\frac{x'-1}{2}) \vee \exists^{\mathrm{r}}_{x'\in {}^{\mathrm{co}}H}(x = \frac{x'}{2})), \tag{19}$$

$$\forall^{\mathrm{nc}}_x(\exists^{\mathrm{r}}_{x'\in {}^{\mathrm{co}}G}\exists_a(x = -a\frac{x'-1}{2}) \vee \exists^{\mathrm{r}}_{x'\in {}^{\mathrm{co}}H}(x = \frac{x'}{2}) \to {}^{\mathrm{co}}G(x)). \tag{20}$$

The realizability extensions $({}^{\mathrm{co}}G)^{\mathbf{r}}$ and $({}^{\mathrm{co}}H)^{\mathbf{r}}$ are binary predicates on cototal ideals p in $\mathbf{G}$ or q in $\mathbf{H}$ (respectively) and real numbers x. Consider the operators

$$\Gamma^{\mathbf{r}}(Z,W) := \{\, (p,x) \mid \exists_{(p',x')\in Z}\exists_a(x = -a\frac{x'-1}{2} \wedge p = \mathrm{LR}_a(p')) \vee^{\mathrm{u}}$$
$$\exists_{(q',x')\in W}(x = \frac{x'}{2} \wedge p = \mathrm{U}(q')) \,\},$$
$$\Delta^{\mathbf{r}}(Z,W) := \{\, (q,x) \mid \exists_{(p',x')\in Z}\exists_a(x = a\frac{x'+1}{2} \wedge q = \mathrm{Fin}_a(p')) \vee^{\mathrm{u}}$$
$$\exists_{(q',x')\in W}(x = \frac{x'}{2} \wedge q = \mathrm{D}(q')) \,\}$$

(the ${}^{\mathrm{u}}$ in $\vee^{\mathrm{u}}$ indicates that the disjunction has no computational significance). Since both $\Gamma^{\mathbf{r}}(Z,W)$ and $\Delta^{\mathbf{r}}(Z,W)$ are strictly positive in Z,W, our underlying theory provides us with a pair of binary predicates $({}^{\mathrm{co}}G)^{\mathbf{r}}$, $({}^{\mathrm{co}}H)^{\mathbf{r}}$ for the greatest fixed point of $(\Gamma^{\mathbf{r}},\Delta^{\mathbf{r}})$:

$$(({}^{\mathrm{co}}G)^{\mathbf{r}}, ({}^{\mathrm{co}}H)^{\mathbf{r}}) := \nu_{(Z,W)}(\Gamma^{\mathbf{r}}(Z,W),\Delta^{\mathbf{r}}(Z,W))$$

satisfying the (strengthened) simultaneous coinduction axiom

$$(Z, W) \subseteq (\Gamma^{\mathbf{r}}((^{\mathrm{co}}G)^{\mathbf{r}} \cup Z, (^{\mathrm{co}}H)^{\mathbf{r}} \cup W), \Delta^{\mathbf{r}}((^{\mathrm{co}}G)^{\mathbf{r}} \cup Z, (^{\mathrm{co}}H)^{\mathbf{r}} \cup W)) \to$$
$$(Z, W) \subseteq ((^{\mathrm{co}}G)^{\mathbf{r}}, (^{\mathrm{co}}H)^{\mathbf{r}})$$

where again inclusion $\subseteq$ is meant component-wise.

Similar to Proposition 3.1, we show that $^{\mathrm{co}}G$ is correct in the sense that the realizers of $^{\mathrm{co}}G(x)$ are exactly the pre-Gray codes of x.

Proposition 3.2. *For $x \in \mathbb{I}$ and cototal ideals p in $\mathbf{G}$ and q in $\mathbf{H}$*

$$(^{\mathrm{co}}G)^{\mathbf{r}}(p, x) \leftrightarrow x = F_{\mathbf{G}}(p),$$
$$(^{\mathrm{co}}H)^{\mathbf{r}}(q, x) \leftrightarrow x = F_{\mathbf{H}}(q).$$

Proof. Recall that if $p = [c_1, c_2, \ldots]$ is a cototal ideal in $\mathbf{G}$, then

$$F_{\mathbf{G}}(p) = \bigcap_{n=1}^{\infty} f_{c_1}(f_{c_2}(\ldots f_{c_n}(\mathbb{I})\ldots))$$

and similary for $F_{\mathbf{H}}(q)$. The proof is similar to the case of signed digits, but slightly more involved because of the simultaneous definition of $(^{\mathrm{co}}G)^{\mathbf{r}}$ and $(^{\mathrm{co}}H)^{\mathbf{r}}$. □

Remark 3.3 (Nested definition). As an alternative to the above simultaneous definition of $^{\mathrm{co}}G$ and $^{\mathrm{co}}H$, we can take the nested definition $^{\mathrm{co}}G' = \nu_X \Gamma(X, {}^{\mathrm{co}}H'(X))$ where $^{\mathrm{co}}H'_X = \nu_Y \Delta(X, Y)$. The witnessing algebras would also be changed. In this paper we adopt the simultaneous one, since the extracted programs are simpler.

4. Proofs about coinductive representations that correspond to algorithms

In each of the examples below, after the proof we state the rules (equations) expressing the algorithm implicit in this proof. Such an "informal program extraction" can be difficult and error-prone. In Section 6 this will be done precisely, using Minlog to extract a program (i.e., a term in an extension of Gödel's T) from a formalization of this proof.

4.1. **Average for signed digit code.** As a warm-up we prove the average property (18), following [2]. Consider two sets of averages, the second one with a "carry" $i \in \mathbf{SD}_2 := \{-2, -1, 0, 1, 2\}$:

$$P := \{\, \frac{x+y}{2} \mid x, y \in {}^{\mathrm{co}}I \,\}, \qquad Q := \{\, \frac{x+y+i}{4} \mid x, y \in {}^{\mathrm{co}}I, i \in \mathbf{SD}_2 \,\},$$

where $\mathbf{SD}_2$ are the "extended signed digits" $\{-2,-1,0,1,2\}$; let i,j range over $\mathbf{SD}_2$. Recall that ${}^{\mathrm{co}}I$ is a fixed point of Φ. Hence ${}^{\mathrm{co}}I \subseteq \Phi({}^{\mathrm{co}}I)$, i.e.

$$\forall^{\mathrm{nc}}_{x\in{}^{\mathrm{co}}I}\exists^{\mathrm{r}}_{x'\in{}^{\mathrm{co}}I}\exists_d(x=\frac{x'+d}{2}) \qquad {}^{\mathrm{co}}I\text{-clause.} \tag{21}$$

It suffices to show that Q satisfies (21), for then by the greatest-fixed-point axiom for ${}^{\mathrm{co}}I$ we have $Q \subseteq {}^{\mathrm{co}}I$. Since we also have $P \subseteq Q$ we then obtain $P \subseteq {}^{\mathrm{co}}I$, which is our claim.

Lemma 4.1 (CoIAvToAvc)**.**

$$\forall^{\mathrm{nc}}_{x,y\in{}^{\mathrm{co}}I}\exists^{\mathrm{r}}_{x',y'\in{}^{\mathrm{co}}I}\exists_i(\frac{x+y}{2}=\frac{x'+y'+i}{4}).$$

Proof. Immediate from (21). □

Lemma 4.2 (CoIAvcSatCoICl)**.**

$$\forall_i\forall^{\mathrm{nc}}_{x,y\in{}^{\mathrm{co}}I}\exists^{\mathrm{r}}_{x',y'\in{}^{\mathrm{co}}I}\exists_{j,d}(\frac{x+y+i}{4}=\frac{\frac{x'+y'+j}{4}+d}{2}).$$

Proof. We need functions $J\colon \mathbf{SD}\to\mathbf{SD}\to\mathbf{SD}_2\to\mathbf{SD}_2$ and $K\colon \mathbf{SD}\to\mathbf{SD}\to\mathbf{SD}_2\to\mathbf{SD}$ such that $d+e+2i = J(d,e,i)+4K(d,e,i)$. They can be defined easily by cases on d, e and i. Using these we can relate the functions $\frac{x+d}{2}$ and $\frac{x+y+i}{4}$ by

$$\frac{\frac{x+d}{2}+\frac{y+e}{2}+i}{4}=\frac{\frac{x+y+J(d,e,i)}{4}+K(d,e,i)}{2}. \tag{22}$$

Now (21) gives the claim. □

By coinduction from Lemma 4.2 we obtain

Lemma 4.3 (CoIAvcToCoI)**.**

$$\forall^{\mathrm{nc}}_z(\exists^{\mathrm{r}}_{x,y\in{}^{\mathrm{co}}I}\exists_i(z=\frac{x+y+i}{4})\to{}^{\mathrm{co}}I(z)).$$

Proposition 4.4 (CoIAverage)**.**

$$\forall^{\mathrm{nc}}_{x,y}({}^{\mathrm{co}}I(x)\to{}^{\mathrm{co}}I(y)\to{}^{\mathrm{co}}I(\frac{x+y}{2})).$$

Proof. Immediate from Lemmata 4.1 and 4.3. □

Implicit algorithm. Lemma 4.1 computes the first "carry" $i\in\mathbf{SD}_2$ and the tails of the inputs. Then $f\colon \mathbf{SD}_2\times\mathbf{I}\times\mathbf{I}\to\mathbf{I}$ defined corecursively by

$$f(i,\mathrm{C}_d(v),\mathrm{C}_e(w))=\mathrm{C}_{K(d,e,i)}(f(J(d,e,i),v,w))$$

is called repeatedly in order to compute the average step by step.

4.2. **From pre-Gray to signed digit code.** We prove ${}^{\mathrm{co}}G \subseteq {}^{\mathrm{co}}I$. However, to be able to do this by coinduction we need to generalize our goal to

Lemma 4.5 (CoGToCoIAux)**.** $\forall_x^{\mathrm{nc}}(\exists_a({}^{\mathrm{co}}G(ax) \vee {}^{\mathrm{co}}H(ax)) \to {}^{\mathrm{co}}Ix)$.

Proof. For $P := \{\, x \mid \exists_a({}^{\mathrm{co}}G(ax) \vee {}^{\mathrm{co}}H(ax))\,\}$ we must show $P \subseteq {}^{\mathrm{co}}I$. By coinduction it suffices to prove $P \subseteq \Phi({}^{\mathrm{co}}I \cup P)$. Let $x_1 \in P$. We show $x_1 \in \Phi({}^{\mathrm{co}}I \cup P)$:

$$\exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}I \cup P} \exists_d (x_1 = \frac{x+d}{2}). \tag{23}$$

Since $x_1 \in P$ we have a such that ${}^{\mathrm{co}}G(ax_1) \vee {}^{\mathrm{co}}H(ax_1)$.

Case ${}^{\mathrm{co}}G(ax_1)$. The ${}^{\mathrm{co}}G$-clause ${}^{\mathrm{co}}G \subseteq \Gamma({}^{\mathrm{co}}G, {}^{\mathrm{co}}H)$ applied to $ax_1 \in {}^{\mathrm{co}}G$ gives us

$$\exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}G} \exists_b (ax_1 = -b\frac{x-1}{2}) \vee \exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}H} (ax_1 = \frac{x}{2}).$$

If the left hand side holds, we have $x_2 \in {}^{\mathrm{co}}G$ and b such that $ax_1 = -b\frac{x_2-1}{2}$. Then (23) holds for $x := -abx_2$ and $d := ab$, since $-abx_2 \in P$ (by $x_2 \in {}^{\mathrm{co}}G$ and the definition of P), and

$$x_1 = a^2 x_1 = -ab\frac{x_2-1}{2} = \frac{-abx_2+ab}{2} = \frac{x+d}{2}.$$

If the right hand side holds, we have $x_2 \in {}^{\mathrm{co}}H$ such that $ax_1 = \frac{x_2}{2}$. Then (23) holds for $x := ax_2$ and $d := 0$, since $ax_2 \in P$ (by $x_2 \in {}^{\mathrm{co}}H$ and the definition of P), and

$$x_1 = a^2 x_1 = a\frac{x_2}{2} = \frac{ax_2+0}{2} = \frac{x+d}{2}.$$

Case ${}^{\mathrm{co}}H(ax_1)$. The ${}^{\mathrm{co}}H$-clause ${}^{\mathrm{co}}H \subseteq \Delta({}^{\mathrm{co}}G, {}^{\mathrm{co}}H)$ applied to $ax_1 \in {}^{\mathrm{co}}H$ gives

$$\exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}G} \exists_b (ax_1 = b\frac{x+1}{2}) \vee \exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}H} (ax_1 = \frac{x}{2}).$$

If the left hand side holds, we have $x_2 \in {}^{\mathrm{co}}G$ and b such that $ax_1 = b\frac{x_2+1}{2}$. Then (23) holds for $x := abx_2$ and $d := ab$, since $abx_2 \in P$ (by $x_2 \in {}^{\mathrm{co}}G$ and the definition of P), and

$$x_1 = a^2 x_1 = ab\frac{x_2+1}{2} = \frac{abx_2+ab}{2} = \frac{x+d}{2}.$$

If the right hand side holds, we have $x_2 \in {}^{\mathrm{co}}H$ such that $ax_1 = \frac{x_2}{2}$. Then (23) holds for $x := ax_2$ and $d := 0$, since $ax_2 \in P$ (by $x_2 \in {}^{\mathrm{co}}H$ and the definition of P), and

$$x_1 = a^2 x_1 = a\frac{x_2}{2} = \frac{ax_2+0}{2} = \frac{x+d}{2}.$$

□

Implicit algorithm. $[f,g]\colon \mathbf{PSD}\times\mathbf{G}+\mathbf{PSD}\times\mathbf{H}\to\mathbf{I}$ defined by

$$\begin{aligned} f(a,\mathrm{LR}_b(p)) &= \mathrm{C}_{ab}(f(-ab,p)), & g(a,\mathrm{Fin}_b(p)) &= \mathrm{C}_{ab}(f(ab,p)),\\ f(a,\mathrm{U}(q)) &= \mathrm{C}_0(g(a,q)), & g(a,\mathrm{D}(q)) &= \mathrm{C}_0(g(a,q)). \end{aligned}$$

An immediate consequence is

Proposition 4.6 (CoGToCoI)**.** $\forall^{\mathrm{nc}}_x({}^{\mathrm{co}}G(x)\to{}^{\mathrm{co}}I(x))$.

4.3. **From signed digit to pre-Gray code.** Conversely we also have ${}^{\mathrm{co}}I\subseteq{}^{\mathrm{co}}G$. Again, to be able to prove this by coinduction we need to generalize our goal to

Lemma 4.7 (CoIToCoGAux)**.**

$$\forall^{\mathrm{nc}}_x(\exists_a{}^{\mathrm{co}}I(ax)\to{}^{\mathrm{co}}Gx),$$
$$\forall^{\mathrm{nc}}_x(\exists_a{}^{\mathrm{co}}I(ax)\to{}^{\mathrm{co}}Hx).$$

Proof. For $P:=\{\,x\mid\exists_a(ax\in{}^{\mathrm{co}}I)\,\}$ we show $P\subseteq{}^{\mathrm{co}}G$ simultaneously with $P\subseteq{}^{\mathrm{co}}H$. By coinduction it suffices to prove (i) $P\subseteq\Gamma({}^{\mathrm{co}}G\cup P,{}^{\mathrm{co}}H\cup P)$ and (ii) $P\subseteq\Delta({}^{\mathrm{co}}G\cup P,{}^{\mathrm{co}}H\cup P)$. For (i), let $x_1\in P$. We show $x_1\in\Gamma({}^{\mathrm{co}}G\cup P,{}^{\mathrm{co}}H\cup P)$:

$$\exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}G\cup P}\exists_a(x_1=-a\frac{x-1}{2})\vee\exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}H\cup P}(x_1=\frac{x}{2}). \tag{24}$$

Since $x_1\in P$ we have a_1 such that ${}^{\mathrm{co}}I(a_1x_1)$. The ${}^{\mathrm{co}}I$-clause ${}^{\mathrm{co}}I\subseteq\Phi({}^{\mathrm{co}}I)$ applied to $a_1x_1\in{}^{\mathrm{co}}I$ gives us

$$\exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}I}\exists_d(a_1x_1=\frac{x+d}{2}).$$

Hence we have $x_2\in{}^{\mathrm{co}}I$ and d such that $a_1x_1=\frac{x_2+d}{2}$.

Case $d=-1$. Then the left hand of (24) holds for $x:=x_2$ and $a:=-a_1$, since $x_2\in P$ (by $x_2\in{}^{\mathrm{co}}I$ and the definition of P), and

$$x_1=a_1a_1x_1=a_1\frac{x_2+d}{2}=a_1\frac{x_2-1}{2}.$$

Case $d=1$. Then the left hand of (24) holds for $x:=-x_2$ and $a:=a_1$, since $-x_2\in P$ (by $x_2\in{}^{\mathrm{co}}I$ and the definition of P), and

$$x_1=a_1a_1x_1=a_1\frac{x_2+d}{2}=a_1\frac{x_2+1}{2}=-a_1\frac{-x_2-1}{2}.$$

Case $d=0$. Then the right hand of (24) holds for $x:=a_1x_2$, since $a_1x_2\in P$ (by $x_2\in{}^{\mathrm{co}}I$ and the definition of P), and

$$x_1=a_1a_1x_1=a_1\frac{x_2+d}{2}=\frac{a_1x_2}{2}.$$

This finishes the proof of (i). The proof of (ii) is similar, and we omit it. □

Implicit algorithm. $g\colon \tau \to \mathbf{G}$ and $h\colon \tau \to \mathbf{H}$ with $\tau := \mathbf{PSD} \times \mathbf{I}$, defined by

$$\begin{aligned} g(b, \mathrm{C}_{-1}(v)) &= \mathrm{LR}_{-b}(g(1, v)), & h(b, \mathrm{C}_{-1}(v)) &= \mathrm{Fin}_{-b}(g(-1, v)), \\ g(b, \mathrm{C}_1(v)) &= \mathrm{LR}_b(g(-1, v)), & h(b, \mathrm{C}_1(v)) &= \mathrm{Fin}_b(g(1, v)), \\ g(b, \mathrm{C}_0(v)) &= \mathrm{U}(h(b, v)), & h(b, \mathrm{C}_0(v)) &= \mathrm{D}(h(b, v)). \end{aligned}$$

An immediate consequence is

Proposition 4.8 (CoIToCoG)**.** $\forall_x^{\mathrm{nc}}({}^{\mathrm{co}}I(x) \to {}^{\mathrm{co}}G(x))$.

4.4. **Average for pre-Gray code.** We consider the problem to compute the average of two real numbers given in pre-Gray code directly, without going via signed digit code.

As a preparation we treat the unary minus function. Here we make use of the fact that our coinduction axioms are in strengthened form (that is $X \subseteq \Phi({}^{\mathrm{co}}I \cup X) \to X \subseteq {}^{\mathrm{co}}I$ instead of $X \subseteq \Phi(X) \to X \subseteq {}^{\mathrm{co}}I$, for example).

Lemma 4.9 (CoGMinus)**.**

$$\begin{aligned} &\forall_x^{\mathrm{nc}}({}^{\mathrm{co}}G(-x) \to {}^{\mathrm{co}}Gx), \\ &\forall_x^{\mathrm{nc}}({}^{\mathrm{co}}H(-x) \to {}^{\mathrm{co}}Hx). \end{aligned}$$

Proof. For $P := \{\, x \mid -x \in {}^{\mathrm{co}}G) \,\}$ and $Q := \{\, x \mid -x \in {}^{\mathrm{co}}H) \,\}$ we show $P \subseteq {}^{\mathrm{co}}G$ simultaneously with $Q \subseteq {}^{\mathrm{co}}H$. By coinduction it suffices to prove (i) $P \subseteq \Gamma({}^{\mathrm{co}}G \cup P, {}^{\mathrm{co}}H \cup Q)$ and (ii) $Q \subseteq \Delta({}^{\mathrm{co}}G \cup P, {}^{\mathrm{co}}H \cup Q)$. For (i), let $x_1 \in P$. We show $x_1 \in \Gamma({}^{\mathrm{co}}G \cup P, {}^{\mathrm{co}}H \cup Q)$:

$$\exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}G \cup P} \exists_a (x_1 = -a\frac{x-1}{2}) \vee \exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}H \cup Q} (x_1 = \frac{x}{2}). \tag{25}$$

The ${}^{\mathrm{co}}G$-clause applied to $-x_1 \in {}^{\mathrm{co}}G$ gives us

$$\exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}G} \exists_a (-x_1 = -a\frac{x-1}{2}) \vee \exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}H} (-x_1 = \frac{x}{2}).$$

In the first case we have $x_2 \in {}^{\mathrm{co}}G$ and a with $-x_1 = -a\frac{x_2-1}{2}$. Then the left hand side of (25) holds for x_2 and $-a$ (here we use that our coinduction axiom is in strengthened form). In the second case we have $x_2 \in {}^{\mathrm{co}}H$ with $-x_1 = \frac{x_2}{2}$. Then the right hand side of (25) holds for $-x_2$. This finishes the proof of (i). The proof of (ii) is similar, and we omit it. □

Implicit algorithm. $f\colon \mathbf{G} \to \mathbf{G}$ and $f'\colon \mathbf{H} \to \mathbf{H}$ defined by

$$\begin{aligned} f(\mathrm{LR}_a(p)) &= \mathrm{LR}_{-a}(p), & f'(\mathrm{Fin}_a(p)) &= \mathrm{Fin}_{-a}(p), \\ f(\mathrm{U}(q)) &= \mathrm{U}(f'(q)), & f'(\mathrm{D}(q)) &= \mathrm{D}(f'(q)). \end{aligned}$$

Using Lemma 4.9 we prove that ${}^{\mathrm{co}}\mathcal{G}$ and ${}^{\mathrm{co}}H$ are in fact equivalent.

Lemma 4.10 (CoHToCoG)**.**

$$\forall_x^{\mathrm{nc}}({}^{\mathrm{co}}Hx \to {}^{\mathrm{co}}\mathcal{G}x),$$
$$\forall_x^{\mathrm{nc}}({}^{\mathrm{co}}\mathcal{G}x \to {}^{\mathrm{co}}Hx).$$

Proof. We show ${}^{\mathrm{co}}H \subseteq {}^{\mathrm{co}}\mathcal{G}$ simultaneously with ${}^{\mathrm{co}}\mathcal{G} \subseteq {}^{\mathrm{co}}H$. By coinduction it suffices to prove (i) ${}^{\mathrm{co}}H \subseteq \Gamma({}^{\mathrm{co}}\mathcal{G} \cup {}^{\mathrm{co}}H, {}^{\mathrm{co}}H \cup {}^{\mathrm{co}}\mathcal{G})$ and (ii) ${}^{\mathrm{co}}\mathcal{G} \subseteq \Delta({}^{\mathrm{co}}\mathcal{G} \cup {}^{\mathrm{co}}H, {}^{\mathrm{co}}H \cup {}^{\mathrm{co}}\mathcal{G})$. For (i), let $x_1 \in {}^{\mathrm{co}}H$. We show $x_1 \in \Gamma({}^{\mathrm{co}}\mathcal{G} \cup {}^{\mathrm{co}}H, {}^{\mathrm{co}}H \cup {}^{\mathrm{co}}\mathcal{G})$:

$$\exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}\mathcal{G} \cup {}^{\mathrm{co}}H} \exists_a (x_1 = -a\frac{x-1}{2}) \vee \exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}H \cup {}^{\mathrm{co}}\mathcal{G}} (x_1 = \frac{x}{2}). \tag{26}$$

The ${}^{\mathrm{co}}H$-clause applied to $x_1 \in {}^{\mathrm{co}}H$ gives us

$$\exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}\mathcal{G}} \exists_a (x_1 = a\frac{x+1}{2}) \vee \exists^{\mathrm{r}}_{x \in {}^{\mathrm{co}}H} (x_1 = \frac{x}{2}).$$

In the first case we have $x_2 \in {}^{\mathrm{co}}\mathcal{G}$ and a with $x_1 = a\frac{x_2+1}{2}$. Then the left hand side of (26) holds for $-x_2$ and a, using Lemma 4.9 and (again) that our coinduction axiom is in strengthened form. In the second case we have $x_2 \in {}^{\mathrm{co}}H$ with $x_1 = \frac{x_2}{2}$. Then the right hand side of (25) holds for x_2. This finishes the proof of (i). The proof of (ii) is similar, and we omit it. □

Implicit algorithm. $g\colon \mathbf{H} \to \mathbf{G}$ and $h\colon \mathbf{G} \to \mathbf{H}$:

$$g(\mathrm{Fin}_a(p)) = \mathrm{LR}_a(f^-(p)), \qquad h(\mathrm{LR}_a(p)) = \mathrm{Fin}_a(f^-(p)),$$
$$g(\mathrm{D}(q)) = \mathrm{U}(q), \qquad h(\mathrm{U}(q)) = \mathrm{D}(q)$$

where $f^- :=$ cCoGMinus (cL denotes the function extracted from the proof of a lemma L). Notice that no corecursive call is involved.

The direct proof of the existence of the average w.r.t. Gray-coded reals is similar to the proof in Section 4.1 of the existence of the average w.r.t. signed digit stream coded reals. It proceeds as follows. To prove

$$\forall_{x,y}^{\mathrm{nc}}({}^{\mathrm{co}}\mathcal{G}(x) \to {}^{\mathrm{co}}\mathcal{G}(y) \to {}^{\mathrm{co}}\mathcal{G}(\frac{x+y}{2}))$$

consider again two sets of averages, the second one with a "carry":

$$P := \{\, \frac{x+y}{2} \mid x, y \in {}^{\mathrm{co}}\mathcal{G} \,\}, \qquad Q := \{\, \frac{x+y+i}{4} \mid x, y \in {}^{\mathrm{co}}\mathcal{G},\ i \in \mathbf{SD}_2 \,\}.$$

It suffices to show that Q satisfies the clause coinductively defining ${}^{\mathrm{co}}\mathcal{G}$, for then by the greatest-fixed-point axiom for ${}^{\mathrm{co}}\mathcal{G}$ we have $Q \subseteq {}^{\mathrm{co}}\mathcal{G}$. Since we also have $P \subseteq Q$ we then obtain $P \subseteq {}^{\mathrm{co}}\mathcal{G}$, which is our claim.

Lemma 4.11 (CoGAvToAvc)**.**

$$\forall^{\mathrm{nc}}_{x,y\in {}^{\mathrm{co}}G}\exists^{\mathrm{r}}_{x',y'\in {}^{\mathrm{co}}G}\exists_i(\frac{x+y}{2}=\frac{x'+y'+i}{4}).$$

Proof. Immediate from CoGClause (19). □

Implicit algorithm. We use f^* for cCoGPsdTimes and s for cCoHToCoG.

$$\begin{aligned} f(\mathrm{LR}_a(p),\mathrm{LR}_{a'}(p')) &= (a+a', f^*(-a,p), f^*(-a',p')),\\ f(\mathrm{LR}_a(p),\mathrm{U}(q)) &= (a, f^*(-a,p), s(q)),\\ f(\mathrm{U}(q),\mathrm{LR}_a(p)) &= (a, s(q), f^*(-a,p)),\\ f(\mathrm{U}(q),\mathrm{U}(q')) &= (0, s(q), s(q')). \end{aligned}$$

Lemma 4.12 (CoGAvcSatCoICl)**.**

$$\forall_i\forall^{\mathrm{nc}}_{x,y\in {}^{\mathrm{co}}G}\exists^{\mathrm{r}}_{x',y'\in {}^{\mathrm{co}}G}\exists_{j,d}(\frac{x+y+i}{4}=\frac{\frac{x'+y'+j}{4}+d}{2}).$$

Proof. As in Lemma 4.2 we need the functions J, K with their property (22). Then (19) gives the claim. □

Implicit algorithm.

$$\begin{aligned} f(i,\mathrm{LR}_a(p),\mathrm{LR}_{a'}(p')) &= (J(a,a',i), K(a,a',i), f^*(-a,p), f^*(-a',p')),\\ f(i,\mathrm{LR}_a(p),\mathrm{U}(q)) &= (J(a,0,i), K(a,0,i), f^*(-a,p), s(q)),\\ f(i,\mathrm{U}(q),\mathrm{LR}_a(p)) &= (J(0,a,i), K(0,a,i), s(q), f^*(-a,p)),\\ f(i,\mathrm{U}(q),\mathrm{U}(q')) &= (J(0,0,i), K(0,0,i), s(q), s(q')). \end{aligned}$$

Lemma 4.13 (CoGAvcToCoG)**.**

$$\begin{aligned} &\forall^{\mathrm{nc}}_z(\exists^{\mathrm{r}}_{x,y\in {}^{\mathrm{co}}G}\exists_i(z=\frac{x+y+i}{4})\to {}^{\mathrm{co}}G(z)),\\ &\forall^{\mathrm{nc}}_z(\exists^{\mathrm{r}}_{x,y\in {}^{\mathrm{co}}G}\exists_i(z=\frac{x+y+i}{4})\to {}^{\mathrm{co}}H(z)). \end{aligned}$$

Proof. We show $Q\subseteq {}^{\mathrm{co}}G$ simultaneously with $Q\subseteq {}^{\mathrm{co}}H$. By coinduction it suffices to prove (i) $Q\subseteq\Gamma({}^{\mathrm{co}}G\cup Q, {}^{\mathrm{co}}H\cup Q)$ and (ii) $Q\subseteq\Delta({}^{\mathrm{co}}G\cup Q, {}^{\mathrm{co}}H\cup Q)$. For (i), let $z_1\in Q$. We show $z_1\in\Gamma({}^{\mathrm{co}}G\cup Q, {}^{\mathrm{co}}H\cup Q)$:

$$\exists^{\mathrm{r}}_{z\in {}^{\mathrm{co}}G\cup Q}\exists_a(z_1=-a\frac{z-1}{2})\vee\exists^{\mathrm{r}}_{z\in {}^{\mathrm{co}}H\cup Q}(z_1=\frac{z}{2}). \tag{27}$$

Lemma 4.12 applied to $z_1\in Q$ gives us $x_1, y_1\in {}^{\mathrm{co}}G$ and i_1, d_1 such that

$$z_1=\frac{\frac{x_1+y_1+i_1}{4}+d_1}{2}.$$

Case $d_1 = 0$. Go for the right hand side of (27) with $z := (x_1 + y_1 + i_1)/4 \in Q$. *Case* $d_1 = \pm 1$. Go for the left hand side of (27) with $a := d_1$ and $z := (-ax_1 - ay_1 - ai_1)/4 \in Q$. Then

$$-a\frac{z-1}{2} = -a\frac{4z-4}{8} = \frac{x_1 + y_1 + i_1 + 4a}{8} = z_1.$$

This finishes the proof of (i). The proof of (ii) is similar, and we omit it. □

Implicit algorithm. In the proof we used SdDisj: $\forall_d(d = 0 \vee \exists_a(d = a))$.

$$\begin{aligned}
g(i,p,p') &= \text{let } (i_1,d,p_1,p_1') = \text{cCoGAvcSatCoICl}(i,p,p') \text{ in}\\
&\quad \text{case cSdDisj}(d) \text{ of}\\
&\quad\quad 0 \to \mathrm{U}(h(i,p_1,p_1'))\\
&\quad\quad a \to \mathrm{LR}_a(g(-ai, f^*(-a,p_1), f^*(-a,p_1'))),\\
h(i,p,p') &= \text{let } (i_1,d,p_1,p_1') = \text{cCoGAvcSatCoICl}(i,p,p') \text{ in}\\
&\quad \text{case cSdDisj}(d) \text{ of}\\
&\quad\quad 0 \to \mathrm{D}(h(i,p_1,p_1'))\\
&\quad\quad a \to \mathrm{Fin}_a(g(-ai, f^*(-a,p_1), f^*(-a,p_1'))).
\end{aligned}$$

Proposition 4.14 (CoGAverage)**.**

$$\forall^{\mathrm{nc}}_{x,y}({}^{\mathrm{co}}G(x) \to {}^{\mathrm{co}}G(y) \to {}^{\mathrm{co}}G(\frac{x+y}{2})).$$

Proof. Compose Lemmata 4.11 and 4.13. □

4.5. **A bounded translation from pre-Gray code to its normal form.** For pre-Gray code there are many ways of expressing the same real number as we noted in Section 2. In particular, the two terms $\mathrm{U}(\mathrm{D}^k(\mathrm{Fin}_a\ p)))$ and $\mathrm{LR}_a(\mathrm{LR}_1(\mathrm{LR}^k_{-1}\ p))))$ denote the same number as Proposition 2.5 says (D^k and LR^k_{-1} denote k-times repetition of the same constructor). Here we extract a program which transfers the former pattern in the first n elements of a pre-Gray code into the latter pattern.

Similar to G we inductively define a binary relation ${}^{\mathrm{z}}G$ between real and natural numbers (used as bounds), this time with an initial clause. The definition is no longer simultaneous with H, but the latter can be defined independently in advance:

$${}^{\mathrm{z}}\Delta(Z) := \{\,(y,m) \mid m = 0 \vee \exists^{\mathrm{r}}_{x\in Z}(y = \frac{x}{2} \wedge m = n+1)\,\}.$$

With ${}^{\mathrm{z}}H = \mu_Z {}^{\mathrm{z}}\Delta(Z)$ we can now define

$$ {}^{\mathrm{z}}\Gamma(X) := \{\, (y,m) \mid m = 0 \vee \exists^{\mathrm{r}}_{(x,n)\in X} \exists_a (y = -a\frac{x-1}{2} \wedge m = n+1) \vee \exists^{\mathrm{r}}_{(x,n)\in {}^{\mathrm{z}}H} (y = \frac{x}{2} \wedge m = n+1) \,\} $$

and ${}^{\mathrm{z}}G = \mu_X {}^{\mathrm{z}}\Gamma(X)$. From a proof of $\{\, (x,n) \mid {}^{\mathrm{co}}G(x) \,\} \subseteq {}^{\mathrm{z}}G$, we extract the desired program to compute a prefix of a pre-Gray code of x of length n which does not contain a subsequence of the form $\mathrm{UD}^k\mathrm{Fin}_a$ from a pre-Gray code of x. The associated algebra for ${}^{\mathrm{z}}H$ it is just the natural numbers $\mathbf{N}$, and for ${}^{\mathrm{z}}G$ it is ${}^{\mathrm{z}}\mathbf{G}$ with constructors

$$ \mathrm{Nz}\colon {}^{\mathrm{z}}\mathbf{G}, \qquad \mathrm{LRz}\colon \mathbf{PSD} \to {}^{\mathrm{z}}\mathbf{G} \to {}^{\mathrm{z}}\mathbf{G}, \qquad \mathrm{Uz}\colon \mathbf{N} \to {}^{\mathrm{z}}\mathbf{G}. $$

Lemma 4.15 (GenCoGLR)**.** $\forall^{\mathrm{nc}}_x \forall_a ({}^{\mathrm{co}}G(x) \to {}^{\mathrm{co}}G(-a\frac{x-1}{2}))$.

Proof. Easy by coinduction. □

Lemma 4.16 (CoGToBGAux)**.**

$$ \forall_n \forall^{\mathrm{nc}}_x ({}^{\mathrm{co}}G(x) \to {}^{\mathrm{z}}G(x,n)), $$

$$ \forall_n \forall^{\mathrm{nc}}_x ({}^{\mathrm{co}}H(x) \to {}^{\mathrm{z}}H(x,n) \vee \exists^{\mathrm{r}}_{y\in {}^{\mathrm{co}}G} \exists_a ({}^{\mathrm{z}}G(y,n-1) \wedge x = a\frac{y+1}{2})). $$

Proof. We prove both statements simultaneously by induction on n. The case $n = 0$ is trivial. For the step case, we first assume ${}^{\mathrm{co}}G(x_1)$ and prove $(x_1, n+1) \in {}^{\mathrm{z}}G$. We have

$$ \exists^{\mathrm{r}}_{x_2\in {}^{\mathrm{co}}G} \exists_a (x_1 = -a\frac{x_2-1}{2}) \vee \exists^{\mathrm{r}}_{x_2\in {}^{\mathrm{co}}H} (x_1 = \frac{x_2}{2}). $$

(Case A) Suppose that the left hand side holds. Then, by induction hypothesis applied to x_2, we have ${}^{\mathrm{z}}G(x_2, n)$. Therefore $(x_1, n+1) \in {}^{\mathrm{z}}\Gamma({}^{\mathrm{z}}G) = {}^{\mathrm{z}}G$ because

$$ \exists^{\mathrm{r}}_{(x_2,n)\in {}^{\mathrm{z}}G} \exists_a (x_1 = -a\frac{x_2-1}{2}). $$

(Case B) Suppose that the right hand side holds. Then, $x_1 = \frac{x_2}{2}$ for $x_2 \in {}^{\mathrm{co}}H$. Therefore, by induction hypothesis,

$$ {}^{\mathrm{z}}H(x_2, n) \vee \exists^{\mathrm{r}}_{x_3\in {}^{\mathrm{co}}G} \exists_a ({}^{\mathrm{z}}G(x_3, n-1) \wedge x_2 = a\frac{x_3+1}{2}). $$

(Case B1) Suppose that the left hand side holds. Then, since ${}^{\mathrm{z}}H(x_2, n)$ and $x_1 = \frac{x_2}{2}$, ${}^{\mathrm{z}}G(x_1, n+1)$ holds.

(Case B2) Suppose that the right hand side holds. Then,

$$ x_1 = \frac{x_2}{2} = a_3\frac{x_3+1}{4} = -a_3\frac{-\frac{x_3-1}{2}-1}{2} = -a_3\frac{x_4-1}{2} $$

for some a_3, $x_3 \in {}^{\mathrm{co}}\mathcal{G}$ and $x_4 := -\frac{x_3-1}{2}$. Since $x_1 = -a_3\frac{x_4-1}{2}$, for our goal ${}^{\mathrm{z}}\mathcal{G}(x_1, n+1)$ it suffices to prove ${}^{\mathrm{z}}\mathcal{G}(x_4, n)$. In case $n = 0$ this follows from the initial clause for ${}^{\mathrm{z}}\mathcal{G}$, and in case $n = m+1$ it follows from ${}^{\mathrm{z}}\mathcal{G}(x_3, n-1)$ by the first generating clause for ${}^{\mathrm{z}}\mathcal{G}$, since $x_4 = -\frac{x_3-1}{2}$.

Next, we suppose that ${}^{\mathrm{co}}H(x_1)$ and prove

$$ {}^{\mathrm{z}}H(x_1, n+1) \vee \exists^{\mathrm{r}}_{y\in{}^{\mathrm{co}}G}\exists_a({}^{\mathrm{z}}\mathcal{G}(y, n) \wedge x_1 = a\frac{y+1}{2}). $$

The argument is almost the same as above. Since ${}^{\mathrm{co}}H(x_1)$, we have

$$ \exists^{\mathrm{r}}_{x_2\in{}^{\mathrm{co}}G}\exists_a(x_1 = a\frac{x_2+1}{2}) \vee \exists^{\mathrm{r}}_{x_2\in{}^{\mathrm{co}}H}(x_1 = \frac{x_2}{2}). $$

(Case A) Suppose that the left hand side holds. We have $x_1 = a_2\frac{x_2+1}{2}$ for a_2 and $x_2 \in {}^{\mathrm{co}}\mathcal{G}$. By induction hypothesis, ${}^{\mathrm{z}}\mathcal{G}(x_2, n)$. Therefore

$$ \exists^{\mathrm{r}}_{y\in{}^{\mathrm{co}}G}\exists_a({}^{\mathrm{z}}\mathcal{G}(y, n) \wedge x_1 = a\frac{y+1}{2}). $$

(Case B) Suppose that the right hand side holds. We have $x_1 = \frac{x_2}{2}$ for $x_2 \in {}^{\mathrm{co}}H$. By induction hypothesis,

$$ {}^{\mathrm{z}}H(x_2, n) \vee \exists^{\mathrm{r}}_{x_3\in{}^{\mathrm{co}}G}\exists_a({}^{\mathrm{z}}\mathcal{G}(x_3, n-1) \wedge x_2 = a\frac{x_3+1}{2}). $$

(Case B1) Suppose that the left hand side holds. Then, since ${}^{\mathrm{z}}H(x_2, n)$ and $x_1 = \frac{x_2}{2}$, we have ${}^{\mathrm{z}}H(x_1, n+1)$.

(Case B2) Suppose that the right hand side holds. Then,

$$ x_1 = \frac{x_2}{2} = a\frac{x_3+1}{4} = a\frac{\frac{x_3-1}{2}+1}{2} = a\frac{x_4+1}{2} $$

for $x_4 := \frac{x_3-1}{2}$. We prove the right hand side of our goal for x_4 and a. Since $x_1 = a\frac{x_4+1}{2}$ it suffices to prove $x_4 \in {}^{\mathrm{co}}\mathcal{G}$ and ${}^{\mathrm{z}}\mathcal{G}(x_4, n)$. From $x_3 \in {}^{\mathrm{co}}\mathcal{G}$ we obtain $x_4 \in {}^{\mathrm{co}}\mathcal{G}$ by Lemma 4.15. To prove ${}^{\mathrm{z}}\mathcal{G}(x_4, n)$ we argue by cases on n. In case $n = 0$ this follows from the initial clause for ${}^{\mathrm{z}}\mathcal{G}$, and in case $n = m+1$ it follows from ${}^{\mathrm{z}}\mathcal{G}(x_3, n-1)$ by the first generating clause for ${}^{\mathrm{z}}\mathcal{G}$, since $x_4 = \frac{x_3-1}{2}$. □

Implicit algorithm. $f\colon \mathbf{N} \to \mathbf{G} \to {}^{\mathrm{z}}\mathbf{G}$ and $g\colon \mathbf{N} \to \mathbf{H} \to \mathbf{N} + \mathbf{PSD} \times \mathbf{G} \times {}^{\mathrm{z}}\mathbf{G}$ are defined by simultaneous recursion

$$ \begin{aligned} &f(0, p) = 0 \qquad g(0, q) = 0 \\ &f(n+1, \mathrm{LR}_a(p)) = \mathrm{LRz}_a(f(n, p)) \\ &f(n+1, \mathrm{U}(q)) = \text{case } g(n, q) \text{ of} \\ &\qquad\qquad m \to m \end{aligned} $$

$$\begin{aligned}
&(a,p,r) \to \mathrm{LRz}_a(\text{case } n \text{ of}\\
&\qquad\qquad 0 \to 0\\
&\qquad\qquad m+1 \to \mathrm{LRz}_1(r))\\
&g(n+1,\mathrm{Fin}_a(p)) = (a,p,f(n,p)))\\
&g(n+1,\mathrm{D}(q)) = \text{case } g(n,q) \text{ of}\\
&\qquad\qquad m \to m+1\\
&\qquad\qquad (a,p,r) \to (a,\mathrm{LR}_{-1}(p), f(n,\mathrm{LR}_{-1}(p)))
\end{aligned}$$

An immediate consequence is

Proposition 4.17 (CoGToBG)**.** $\forall_n \forall_x^{\mathrm{nc}} ({}^{\mathrm{co}}G(x) \to {}^{\mathrm{z}}G(x,n))$.

5. Conversion from Gray-code to modified Gray expansion

As we studied in Section 2.1, each dyadic rational number has three representations of the forms $s11\bar{1}^\omega$, $s\bar{1}1\bar{1}^\omega$ and $s\bot1\bar{1}^\omega$ in Gray-code, and only the last one in modified Gray expansion. We show that Gray-code can be converted to modified Gray expansion. We denote by $K(RD)$ and $L(RD)$ the sets of compact and non-compact elements of RD, which coincide with the sets of finite Gray-codes and infinite Gray-codes, respectively. We also denote by $M(L(RD))$ the set of minimal elements of $L(RD)$, which coincides with the set of modified Gray expansions.

We say that s is a predecessor of t if $s \sqsubseteq t$ and no $u \in K(RD)$ satisfies $s \sqsubseteq u \sqsubseteq t$. $\bot^\omega$ have no predecessor, $s'\bot1\bar{1}^k$, $\bar{1}^k$ and $1\bar{1}^k$ have one predecessor, and the other elements of $K(RD)$ have two predecessors (see Figure 2). We define a function ρ on $K(RD)$ so that $\rho(s)$ is the meet of the predecessors of s for $s \neq \bot$. In the following definition, $a \in \{\bar{1},1\}$, $k \geq 0$, $s' \in \{\bar{1},1\}^*$, and $a\bar{1}^{k-1}$ means $\bot^\omega$ if $k = 0$.

$$\rho(s) = \begin{cases} \bot^\omega & (s = \bot^\omega)\\ s'\bot1\bar{1}^{k-1} & (s = s'\bot1\bar{1}^k)\\ a\bar{1}^{k-1} & (s = a\bar{1}^k)\\ s'\bot1\bar{1}^{k-1} & (s = s'a1\bar{1}^k) \end{cases}$$

Since $\rho(s) \sqsubseteq s$, we have $[\![\rho(s)]\!] \supseteq [\![s]\!]$. Moreover, $[\![\rho(s)]\!]$ is the smallest standard interval whose interior contains $[\![s]\!]$.

One can verify that ρ is monotonic. Therefore, ρ can be extended to a continuous function from RD to RD because RD is a Scott-Ershov domain. It is obvious that $\rho(L(RD)) \subseteq L(RD)$. The following proposition says that ρ is a conversion function from Gray-code to modified Gray expansion.

Proposition 5.1. *ρ is a retract function from $L(RD)$ to $M(L(RD))$. That is, $\rho(t) \in M(L(RD))$ and $\rho(t) \sqsubseteq t$ for $t \in L(RD)$. In particular, $\rho(t) = t$ for $t \in M(L(RD))$.*

Proof. Since $\rho(s) \sqsubseteq s$ for $s \in K(RD)$, $\rho(t) \sqsubseteq t$ for $t \in L(RD)$, and therefore $\rho(t) = t$ for $t \in M(L(RD))$. We show $\rho(L(RD)) \subseteq M(L(RD))$. Suppose that $t \in L(RD) \setminus M(L(RD))$ and let $t = sa1\bar{1}^\omega$ for some $s \in \{\bar{1}, 1\}^*$ and $a \in \{\bar{1}, 1\}$. Since $\rho(sa1\bar{1}^k) = s\bot 1\bar{1}^{k-1}$ for every $k \geq 0$, $\rho(t) = s\bot 1\bar{1}^\omega \in M(L(RD))$. □

We develop an algorithm to compute the function ρ at the level of pre-Gray code, i.e. we transform a pre-Gray code p to a pre-Gray code p' such that $\varphi(p') = \rho(\varphi(p))$, in particular p' will be the modified Gray-expansion of the real number denoted by p.

In the following, we sometimes write a for LR_a for simplicity. Since $\rho(a1\bar{1}) = \bot 1$ for $a \in \mathbf{PSD}$, if the sequence begins with $[\mathrm{LR}_a, \mathrm{LR}_1, \mathrm{LR}_{-1}]$, then we apply Equation (9) from right to left and replace it with $[\mathrm{U}, \mathrm{Fin}_a, \mathrm{LR}_{-1}]$ and fix U. We write this rule simply as

$$a\ 1\ \bar{1}\ \mapsto\ \mathrm{U} \mid \mathrm{Fin}_a\ \bar{1}.$$

On the other hand, since $\rho(a11){=}a$, if the sequence begins with $[\mathrm{U}, \mathrm{Fin}_a, \mathrm{LR}_1]$, we apply Equation (9) from left to right and replace it with $[\mathrm{LR}_a, \mathrm{LR}_1, \mathrm{LR}_1]$ and fix LR_a. Therefore, we have

$$\mathrm{U}\ \mathrm{Fin}_a\ 1\ \mapsto\ a\ 1\ 1.$$

Similarly, we have the following rules

$$\mathrm{Fin}_a\ \bar{1}\ \bar{1}\ \mapsto\ \mathrm{D} \mid \mathrm{Fin}_a\ \bar{1},$$
$$\mathrm{D}\ \mathrm{Fin}_a\ 1\ \mapsto\ \mathrm{Fin}_a \mid \bar{1}\ 1.$$

If the sequence does not match to these four patterns, then we fix the first character. We repeat this procedure to the rest of the sequence. One can verify that the implicit algorithm extracted from the proof of Proposition 5.5 behaves in this way.

We extract a program that converts Gray-code to modified Gray expansion. To this end we define variants ${}^{\mathrm{co}}M$ of ${}^{\mathrm{co}}G$ and ${}^{\mathrm{co}}N$ of ${}^{\mathrm{co}}H$. Recall that the predicate $({}^{\mathrm{co}}G)^{\mathbf{r}}(p, y)$ expresses that p is a pre-Gray code of y by Proposition 3.2, and it is defined (as greatest fixed point) to mean that $p = \mathrm{LR}_a(p')$, $y = -a\frac{x-1}{2}$ and $({}^{\mathrm{co}}G)^{\mathbf{r}}(p', x)$ or else $p = \mathrm{U}(q)$, $y = \frac{x}{2}$ and $({}^{\mathrm{co}}H)^{\mathbf{r}}(q, x)$. In this definition, $p = \mathrm{LR}_{-1}(p')$ happens only if $y \leq 0$, $p = \mathrm{LR}_1(p')$ happens only if $y \geq 0$ and $p = \mathrm{U}(q)$ happens only if $-\frac{1}{2} \leq y \leq \frac{1}{2}$. Modified Gray expansion is obtained by restricting these three cases to $y < 0$, $y > 0$, and

$-\frac{1}{2} < y < \frac{1}{2}$. Therefore, ${}^{\mathrm{co}}M$ is defined so that the left clause of ${}^{\mathrm{co}}G$ is restricted to $y \neq 0$ and the right clause of ${}^{\mathrm{co}}G$ is restricted to $y \neq \pm\frac{1}{2}$. A similar restriction must be imposed on ${}^{\mathrm{co}}H$. Accordingly we define variants Γ', Δ' of the operators Γ, Δ by

$$\Gamma'(X,Y) := \{\, y \mid \exists^{\mathrm{r}}_{x\in X}\exists_a(y = -a\frac{x-1}{2} \wedge y \neq 0) \vee \exists^{\mathrm{r}}_{x\in Y}(y = \frac{x}{2} \wedge y \neq \pm\frac{1}{2}) \,\},$$
$$\Delta'(X,Y) := \{\, y \mid \exists^{\mathrm{r}}_{x\in X}\exists_a(y = a\frac{x+1}{2} \wedge y \neq 0) \vee \exists^{\mathrm{r}}_{x\in Y}(y = \frac{x}{2} \wedge y \neq \pm\frac{1}{2}) \,\}$$

and we define $({}^{\mathrm{co}}M, {}^{\mathrm{co}}N) := \nu_{(X,Y)}(\Gamma'(X,Y), \Delta'(X,Y))$.

The corresponding realizability predicates are defined by the operators

$$(\Gamma')^{\mathbf{r}}(Z,W) := \{\, (p,x) \mid \exists_{(p',x')\in Z}\exists_a(x = -a\frac{x'-1}{2} \wedge p = \mathrm{LR}_a(p') \wedge x \neq 0) \vee^{\mathrm{u}}$$
$$\exists_{(q',x')\in W}(x = \frac{x'}{2} \wedge p = \mathrm{U}(q')) \wedge x \neq \pm\frac{1}{2} \,\},$$
$$(\Delta')^{\mathbf{r}}(Z,W) := \{\, (q,x) \mid \exists_{(p',x')\in Z}\exists_a(x = a\frac{x'+1}{2} \wedge q = \mathrm{Fin}_a(p') \wedge x \neq 0) \vee^{\mathrm{u}}$$
$$\exists_{(q',x')\in W}(x = \frac{x'}{2} \wedge q = \mathrm{D}(q')) \wedge x \neq \pm\frac{1}{2} \,\}$$

as $(({}^{\mathrm{co}}M)^{\mathbf{r}}, ({}^{\mathrm{co}}N)^{\mathbf{r}}) := \nu_{(Z,W)}((\Gamma')^{\mathbf{r}}(Z,W), (\Delta')^{\mathbf{r}}(Z,W))$.

The following proposition shows that ${}^{\mathrm{co}}M$ is correct in the sense that the realizers of ${}^{\mathrm{co}}M(x)$ are exactly the pre-Gray codes of x that are mapped by φ to a modified Gray-expansion of x.

Proposition 5.2. *For cototal ideals p in $\mathbf{G}$ and $x \in \mathbb{I}$*

$$({}^{\mathrm{co}}M)^{\mathbf{r}}(p,x) \leftrightarrow \varphi(p) \textit{ is a modified Gray-expansion of } x.$$

Proof. This is a direct consequence of the following lemma, because the modified Gray expansion of -1 and 1 are $\bar{1}^\omega$ and $1\bar{1}^\omega$, respectively, and they are the only cases modified Gray expansion has the form $s\bar{1}^\omega$ for $s \in \{\bar{1}, 1\}^*$. □

Lemma 5.3. *For $x \in \mathbb{I}$ and cototal ideals p in $\mathbf{G}$ and q in $\mathbf{H}$*

$$({}^{\mathrm{co}}M)^{\mathbf{r}}(p,x) \leftrightarrow x = F_{\mathbf{G}}(p) \wedge (x \in \{-1,1\} \vee \varphi(p) \neq s\bar{1}^\omega \textit{ for } s \in \{\bar{1},1\}^*),$$
$$({}^{\mathrm{co}}N)^{\mathbf{r}}(q,x) \leftrightarrow x = F_{\mathbf{H}}(q) \wedge (x \in \{-1,1\} \vee \varphi(q) \neq s\bar{1}^\omega \textit{ for } s \in \{\bar{1},1\}^*).$$

Proof. (From left to right). First, obviously, $({}^{\mathrm{co}}M)^{\mathbf{r}}(p,x) \to ({}^{\mathrm{co}}G)^{\mathbf{r}}(p,x)$ and $({}^{\mathrm{co}}N)^{\mathbf{r}}(q,x) \to ({}^{\mathrm{co}}H)^{\mathbf{r}}(q,x)$. Therefore, $({}^{\mathrm{co}}M)^{\mathbf{r}}(p,x) \to x = F_{\mathbf{G}}(p)$ and $({}^{\mathrm{co}}N)^{\mathbf{r}}(q,x) \to x = F_{\mathbf{H}}(q)$ holds by Proposition 3.2. We show

$$\forall_{s,p,x}(({}^{\mathrm{co}}M)^{\mathbf{r}}(p,x) \to x \in \{-1,1\} \vee \varphi(p) \neq s\bar{1}^\omega) \tag{28}$$

$$\forall_{s,q,x}((^{\mathrm{co}}N)^{\mathbf{r}}(q,x) \to x \in \{-1,1\} \vee \varphi(q) \neq s\bar{1}^{\omega}) \tag{29}$$

by induction on the length $|s|$ of $s \in \{\bar{1},1\}^*$. As the base case, (28) holds for $|s| = 0$ because $\varphi(p) = \bar{1}^{\omega} \wedge x = F_{\mathbf{G}}(p)$ implies $x = -1$. We study (29) for $|s| = 0$. We show that there is no pair (q,x) such that $\varphi(q) = \bar{1}^{\omega}$ and $(^{\mathrm{co}}N)^{\mathbf{r}}(q,x)$. Suppose that such a pair exists. We have $x = F_{\mathbf{H}}(q)$ and $F_{\mathbf{H}}(q) = 0$ (cf. Figure 3 on page 11). Since $(^{\mathrm{co}}N)^{\mathbf{r}}$ is a fixed point of $(\Delta')^{\mathbf{r}}$,

$$\exists_{p',x',a}((^{\mathrm{co}}M)^{\mathbf{r}}(p',x') \wedge x = a\frac{x'+1}{2} \wedge p = \mathrm{Fin}_a(p') \wedge x \neq 0)$$

or

$$\exists_{q',x'}((^{\mathrm{co}}N)^{\mathbf{r}}(q',x') \wedge x = \frac{x'}{2} \wedge p = \mathrm{D}(q') \wedge x \neq \pm\frac{1}{2}).$$

Since $x = 0$, we have the latter case and $p = \mathrm{D}(q')$ and $(^{\mathrm{co}}N)^{\mathbf{r}}(q',0)$. Again for q', we have $q' = \mathrm{D}(q'')$ and $(^{\mathrm{co}}N)^{\mathbf{r}}(q'',0)$. In this way, we have $q = \mathrm{D}^{\omega}$ and $\varphi(q) = \perp\bar{1}^{\omega}$, and we have contradiction. Thus, (29) holds for $|s| = 0$.

Suppose that (28) and (29) hold for $|s| = n$ and prove (28) for $|s| = n+1$. Suppose that $(^{\mathrm{co}}M)^{\mathbf{r}}(p,x)$. Since $(^{\mathrm{co}}M)^{\mathbf{r}}$ is a fixed point of $(\Gamma')^{\mathbf{r}}$,

$$\exists_{p',x',a}((^{\mathrm{co}}M)^{\mathbf{r}}(p',x') \wedge x = -a\frac{x'-1}{2} \wedge p = \mathrm{LR}_a(p') \wedge x \neq 0)$$

or

$$\exists_{q',x'}((^{\mathrm{co}}N)^{\mathbf{r}}(q',x') \wedge x = \frac{x'}{2} \wedge p = \mathrm{U}(q') \wedge x \neq \pm\frac{1}{2}.$$

In the former case, by induction hypothesis, $x' \in \{-1,1\}$ or else $\varphi(p') \neq s\bar{1}^{\omega}$ for any $s \in \{\bar{1},1\}^n$. The case $x' = 1$ does not happen because $x \neq 0$. If $x' = -1$, then $x \in \{-1,1\}$. If $\varphi(p') \neq s\bar{1}^{\omega}$ for any $s \in \{\bar{1},1\}^n$, then $\varphi(p) = \varphi(\mathrm{LR}_a(p')) = a : \varphi(p') \neq s'\bar{1}^{\omega}$ for any $s' \in \{\bar{1},1\}^{n+1}$.

In the latter case, by induction hypothesis, $x' \in \{-1,1\}$ or else $\varphi(q') \neq s\bar{1}^{\omega}$ for any $s \in \{\bar{1},1\}^n$. The case $x' \in \{-1,1\}$ does not happen because $x \neq \pm\frac{1}{2}$. Suppose that $\varphi(q') \neq s\bar{1}^{\omega}$ for any $s \in \{\bar{1},1\}^n$. We have, for $a : t = \varphi(q')$, $\varphi(p) = \varphi(\mathrm{U}(q')) = a : 1 : t$ and $a : 1 : t \neq s'\bar{1}^{\omega}$ for any $s' \in \{\bar{1},1\}^{n+1}$.

The step case of (29) is similar and we omit it.

(From right to left). Easily proved by coinduction. □

Remark 5.4. From $^{\mathrm{co}}G = \Gamma(^{\mathrm{co}}G, ^{\mathrm{co}}H)$ and $^{\mathrm{co}}H = \Delta(^{\mathrm{co}}G, ^{\mathrm{co}}H)$ we know that $\gamma_a(x) := -a\frac{x-1}{2} \in {}^{\mathrm{co}}G$ $(x \in {}^{\mathrm{co}}H)$ and $\delta_a(x) := a\frac{x+1}{2} \in {}^{\mathrm{co}}H$ $(x \in {}^{\mathrm{co}}G)$.

Proposition 5.5 (CoGToCoM)**.**

$$\forall_x^{\mathrm{nc}}({}^{\mathrm{co}}G(x) \to {}^{\mathrm{co}}M(x)),$$
$$\forall_x^{\mathrm{nc}}({}^{\mathrm{co}}H(x) \to {}^{\mathrm{co}}N(x)).$$

Proof. For $P := {}^{\mathrm{co}}G$ and $Q := {}^{\mathrm{co}}H$ we show $P \subseteq {}^{\mathrm{co}}M$ simultaneously with $Q \subseteq {}^{\mathrm{co}}N$. By coinduction it suffices to prove (i) $P \subseteq \Gamma'({}^{\mathrm{co}}M \cup P, {}^{\mathrm{co}}N \cup Q)$ and (ii) $Q \subseteq \Delta'({}^{\mathrm{co}}M \cup P, {}^{\mathrm{co}}N \cup Q)$. For (i), let $x_0 \in P$. We show $x_0 \in \Gamma'({}^{\mathrm{co}}M \cup P, {}^{\mathrm{co}}N \cup Q)$:

$$(30)\quad \exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}M\cup P}\exists_a(x_0 = -a\frac{x-1}{2} \land x_0 \neq 0) \lor \exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}N\cup Q}(x_0 = \frac{x}{2} \land x_0 \neq \pm\frac{1}{2}).$$

The ${}^{\mathrm{co}}G$-clause applied to $x_0 \in {}^{\mathrm{co}}G$ gives us

$$(31)\qquad \exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}G}\exists_a(x_0 = -a\frac{x-1}{2}) \lor \exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}H}(x_0 = \frac{x}{2}).$$

Case ga. The lhs of (31) holds. We have $x_1 \in {}^{\mathrm{co}}G$ and a_1 with $x_0 = -a_1\frac{x_1-1}{2}$. The ${}^{\mathrm{co}}G$-clause applied to $x_1 \in {}^{\mathrm{co}}G$ gives us

$$(32)\qquad \exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}G}\exists_a(x_1 = -a\frac{x-1}{2}) \lor \exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}H}(x_1 = \frac{x}{2}).$$

Case gaa. The lhs of (32) holds. We have $x_2 \in {}^{\mathrm{co}}G$ and a_2 with $x_1 = -a_2\frac{x_2-1}{2}$.

Case ga$\bar{1}$. Assume $a_2 = -1$. Go for the lhs of (30) with $x_1 \in P$ and a_1. The goal $x_0 = -a_1\frac{x_1-1}{2}$ holds by the choice of x_1, a_1. Since $x_2 \in [-1, 1]$, $x_1 = \frac{x_2-1}{2} \neq 1$. Thus, $x_0 = -a_1\frac{x_1-1}{2} \neq 0$.

*Case ga*1. Assume $a_2 = 1$. The ${}^{\mathrm{co}}G$-clause applied to $x_2 \in {}^{\mathrm{co}}G$ gives us

$$(33)\qquad \exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}G}\exists_a(x_2 = -a\frac{x-1}{2}) \lor \exists^{\mathrm{r}}_{x\in{}^{\mathrm{co}}H}(x_2 = \frac{x}{2}).$$

*Case ga*1*a.* The lhs of (33) holds. We have $x_3 \in {}^{\mathrm{co}}G$ and a_3 with $x_2 = -a_3\frac{x_3-1}{2}$.

*Case ga*1$\bar{1}$. Assume $a_3 = -1$. Go for the rhs of (30) with $x = \delta_{a_1}(x_2) := a_1\frac{x_2+1}{2} \in Q$ (since $x_2 \in {}^{\mathrm{co}}G$ implies $\delta_a(x_2) \in {}^{\mathrm{co}}H$). The goal $x_0 = \frac{x}{2}$ holds since

$$x_0 = -a_1\frac{x_1-1}{2} = -a_1\frac{-a_2\frac{x_2-1}{2}-1}{2} = a_1\frac{x_2-1+2}{4} = \frac{x}{2}.$$

On the other hand, since $x_3 \in [-1, 1]$, $x_2 = \frac{x_3-1}{2} \in [-1, 0]$ and therefore, $x_0 = a_1\frac{x_2+1}{4} \in [-\frac{1}{4}, \frac{1}{4}]$. Thus, $x_0 \neq \pm\frac{1}{2}$.

*Case ga*11. Assume $a_3 = 1$. Go for the lhs of (30) with $x_1 \in P$ and a_1. The goal $x_0 = -a_1\frac{x_1-1}{2}$ holds by the choice of x_1, a_1. Since $x_3 \in [-1, 1]$, $x_2 = -\frac{x_3-1}{2} \in [0, 1]$ and hence $x_1 = -\frac{x_2-1}{2} \neq 1$. Thus, $x_0 = -a_1\frac{x_1-1}{2} \neq 0$.

*Case ga*1U. The rhs of (33) holds. We have $x_3 \in {}^{\mathrm{co}}H$ with $x_2 = \frac{x_3}{2}$. Go for the lhs of (30) with $x = x_1 \in Q$ and a_1. The goal $x_0 = -a_1\frac{x_1-1}{2}$ holds by the choice of x_1, a_1. Since $x_3 \in [-1, 1]$, $x_2 \in [-\frac{1}{2}, \frac{1}{2}]$ and therefore $x_1 = -\frac{x_2-1}{2} \neq 1$. Thus, $x_0 = -a_1\frac{x_1-1}{2} \neq 0$.

Case gaU. The rhs of (32) holds. We have $x_2 \in {}^{\mathrm{co}}H$ with $x_1 = \frac{x_2}{2}$. Go for the lhs of (30) with $x = x_1 \in Q$ and a_1. The goal $x_0 = -a_1\frac{x_1-1}{2}$ holds by the choice of x_1, a_1. Since $x_2 \in [-1, 1]$, $x_1 = \frac{x_2}{2} \neq 1$. Thus, $x_0 = -a_1\frac{x_1-1}{2} \neq 0$.

Case gU. The rhs of (31) holds. We have $x_1 \in {}^{\mathrm{co}}H$ with $x_0 = \frac{x_1}{2}$. We now proceed as above, applying the ${}^{\mathrm{co}}H$-clause to $x_1 \in {}^{\mathrm{co}}H$, and complete the proof of (i). The proof for (ii) is similar, and we omit it. □

Implicit algorithm. $g\colon \mathbf{G} \to \mathbf{G}$ and $h\colon \mathbf{H} \to \mathbf{H}$, defined by (with a for LR_a)

$$
\begin{array}{llll}
g(a(\bar{1}(p))) & = a(g(\bar{1}(p))) & h(\mathrm{Fin}_a(\bar{1}(\bar{1}(p)))) & = \mathrm{D}(h(\mathrm{Fin}_a(\bar{1}(p)))) \\
g(a(1(\bar{1}(p)))) & = \mathrm{U}(h(\mathrm{Fin}_a(\bar{1}(p)))) & h(\mathrm{Fin}_a(\bar{1}(1(p)))) & = \mathrm{Fin}_a(g(\bar{1}(1(p)))) \\
g(a(1(1(p)))) & = a(g(1(1(p)))) & h(\mathrm{Fin}_a(\bar{1}(\mathrm{U}(q)))) & = \mathrm{Fin}_a(g(\bar{1}(\mathrm{U}(q)))) \\
g(a(1(\mathrm{U}(q)))) & = a(g(1(\mathrm{U}(q)))) & h(\mathrm{Fin}_a(1(p))) & = \mathrm{Fin}_a(g(1(p))) \\
g(a(\mathrm{U}(q))) & = a(g(\mathrm{U}(q))) & h(\mathrm{Fin}_a(\mathrm{U}(q))) & = \mathrm{Fin}_a(g(\mathrm{U}(q))) \\
g(\mathrm{U}(\mathrm{Fin}_a(\bar{1}(p)))) & = \mathrm{U}(h(\mathrm{Fin}_a(\bar{1}(p)))) & h(\mathrm{D}(\mathrm{Fin}_a(\bar{1}(p)))) & = \mathrm{D}(h(\mathrm{Fin}_a(\bar{1}(p)))) \\
g(\mathrm{U}(\mathrm{Fin}_a(1(p)))) & = a(g(1(1(p)))) & h(\mathrm{D}(\mathrm{Fin}_a(1(p)))) & = \mathrm{Fin}_a(g(\bar{1}(1(p)))) \\
g(\mathrm{U}(\mathrm{Fin}_a(\mathrm{U}(q)))) & = \mathrm{U}(h(\mathrm{Fin}_a(\mathrm{U}(q)))) & h(\mathrm{D}(\mathrm{Fin}_a(\mathrm{U}(q)))) & = \mathrm{D}(h(\mathrm{Fin}_a(\mathrm{U}(q)))) \\
g(\mathrm{U}(\mathrm{D}(q))) & = \mathrm{U}(h(\mathrm{D}(q))) & h(\mathrm{D}(\mathrm{D}(q))) & = \mathrm{D}(h(\mathrm{D}(q)))
\end{array}
$$

Modified Gray expansion is a more desirable representation of real numbers than Gray-code in that it gives the unique code to each real number. However, a program which input and output modified Gray expansion is usually not easy to write, as the above conversion program indicates.

When the above program cCoGToModCoG is composed with a program which inputs and outputs Gray-code, one obtains a program that inputs and outputs modified Gray expansion since a modified Gray expansion is itself a Gray-code. For example, cCoGAverage ∘ cCoGToModCoG is an average program on modified Gray expansion. Therefore, by constructing a program which inputs and outputs Gray-code, one automatically obtains a program which inputs and outputs modified Gray expansion.

6. Minlog and program extraction

Minlog is a proof assistant designed to study constructive proofs and their realizers, or more precisely the theory TCF [10]. All proofs in Sections 4 and 5 have been formalized in Minlog[3] and their realizers extracted, as terms in an extension of Gödel's T. In this section we present the extracted terms and

[3]See `http://www.minlog-system.de/`, which gives instructions on how to download (or clone) the system and the necessary software (Scheme in this case). The formalizations can be found in the directory `minlog/examples/analysis/gray.scm`.

discuss how they operate. They involve recursion and corecursion operators where the original proofs used induction or coinduction axioms, and the conversion rules for these operators determine how the extracted terms can be used as programs. The results of such an analysis have been shown in Sections 4 and 5 under the label "implicit algorithm".

6.1. **Corecursion.** Recall the type of the corecursion operator for $\mathbf{I}$:

$$ {}^{\mathrm{co}}\mathcal{R}^{\tau}_{\mathbf{I}} \colon \tau \to (\tau \to \mathbf{SD} \times (\mathbf{I} + \tau)) \to \mathbf{I}. \tag{34} $$

The type $\mathbf{SD} \times (\mathbf{I} + \tau)$ appears since $\mathbf{I}$ has the single constructor C of type $\mathbf{SD} \to \mathbf{I} \to \mathbf{I}$. The meaning of ${}^{\mathrm{co}}\mathcal{R}^{\tau}_{\mathbf{I}} NM$ is defined by the conversion rule

$$ {}^{\mathrm{co}}\mathcal{R}^{\tau}_{\mathbf{I}} NM \mapsto \mathrm{C}_{\pi_1(MN)}([\mathrm{id}^{\mathbf{I}\to\mathbf{I}}, \lambda_y({}^{\mathrm{co}}\mathcal{R}^{\tau}_{\mathbf{I}} yM)]\pi_2(MN)). $$

We have used π_1, π_2 for the two projections of type $\rho \times \sigma$, and the notation $[f, g] \colon \rho + \sigma \to \tau$ (for $f \colon \rho \to \tau$ and $g \colon \sigma \to \tau$) defined by

$$ [f, g](z) := \begin{cases} f(x) & \text{if } z = \mathrm{inl}(x), \\ g(y) & \text{if } z = \mathrm{inr}(y). \end{cases} $$

We will also need the simultaneous corecursion operators ${}^{\mathrm{co}}\mathcal{R}^{(\mathbf{G},\mathbf{H}),(\sigma,\tau)}_{\mathbf{G}}$ and ${}^{\mathrm{co}}\mathcal{R}^{(\mathbf{G},\mathbf{H}),(\sigma,\tau)}_{\mathbf{H}}$ for $\mathbf{G}$, $\mathbf{H}$, of type

$$ \begin{aligned} {}^{\mathrm{co}}\mathcal{R}^{(\mathbf{G},\mathbf{H}),(\sigma,\tau)}_{\mathbf{G}} &\colon \sigma \to \delta_{\mathbf{G}} \to \delta_{\mathbf{H}} \to \mathbf{G} \\ {}^{\mathrm{co}}\mathcal{R}^{(\mathbf{G},\mathbf{H}),(\sigma,\tau)}_{\mathbf{H}} &\colon \tau \to \delta_{\mathbf{G}} \to \delta_{\mathbf{H}} \to \mathbf{H} \end{aligned} \tag{35} $$

with step types

$$ \begin{aligned} \delta_{\mathbf{G}} &:= \sigma \to \mathbf{PSD} \times (\mathbf{G} + \sigma) + (\mathbf{H} + \tau), \\ \delta_{\mathbf{H}} &:= \tau \to \mathbf{PSD} \times (\mathbf{G} + \sigma) + (\mathbf{H} + \tau). \end{aligned} $$

The type $\mathbf{PSD} \times (\mathbf{G} + \sigma) + (\mathbf{H} + \tau)$ appears since $\mathbf{G}$ has the two constructors $\mathrm{LR} \colon \mathbf{PSD} \to \mathbf{G} \to \mathbf{G}$ and $\mathrm{U} \colon \mathbf{H} \to \mathbf{G}$, and $\mathbf{H}$ has the two constructors $\mathrm{Fin} \colon \mathbf{PSD} \to \mathbf{G} \to \mathbf{H}$ and $\mathrm{D} \colon \mathbf{H} \to \mathbf{H}$. Omitting the upper indices of ${}^{\mathrm{co}}\mathcal{R}$, the terms ${}^{\mathrm{co}}\mathcal{R}_{\mathbf{G}} NMM'$ and ${}^{\mathrm{co}}\mathcal{R}_{\mathbf{H}} N'MM'$ are defined by the conversion rules

$$ {}^{\mathrm{co}}\mathcal{R}_{\mathbf{G}} NMM' \mapsto \begin{cases} \mathrm{LR}_{\pi_1(u)}([\mathrm{id}, \lambda_y({}^{\mathrm{co}}\mathcal{R}_{\mathbf{G}} yMM')]\pi_2(u)) & \text{if } MN = \mathrm{inl}(u) \\ \mathrm{U}([\mathrm{id}, \lambda_z({}^{\mathrm{co}}\mathcal{R}_{\mathbf{H}} zMM')]v) & \text{if } MN = \mathrm{inr}(v) \end{cases} $$

$$ {}^{\mathrm{co}}\mathcal{R}_{\mathbf{H}} N'MM' \mapsto \begin{cases} \mathrm{Fin}_{\pi_1(u)}([\mathrm{id}, \lambda_y({}^{\mathrm{co}}\mathcal{R}_{\mathbf{G}} yMM')]\pi_2(u)) & \text{if } M'N' = \mathrm{inl}(u) \\ \mathrm{D}([\mathrm{id}, \lambda_z({}^{\mathrm{co}}\mathcal{R}_{\mathbf{H}} zMM')]v) & \text{if } M'N' = \mathrm{inr}(v) \end{cases} $$

6.2. **Notational conventions of Minlog.** Types:

`iv, ag, ah, bg`	base types for the algebra **I**, **G**, **H**, $^{z}\mathbf{G}$
`rho=>sigma`	function type
`rho@@sigma`	product type
`rho ysum sigma`	sum type

Variables (with fixed types)

`v, p, q`	of type **I**, **G** and **H**
`d, a, i`	of type **SD**, **PSD**, $\mathbf{SD}_2$
`ivw`	of type $\mathbf{SD}_2 \times \mathbf{I} \times \mathbf{I}$
`jdvw`	of type $\mathbf{SD}_2 \times \mathbf{SD} \times \mathbf{I} \times \mathbf{I}$
`ap`	of type $\mathbf{PSD} \times \mathbf{G}$
`apq`	of type $\mathbf{PSD} \times (\mathbf{G} + \mathbf{H})$
`bv`	of type $\mathbf{PSD} \times \mathbf{I}$
`ipp`	of type $\mathbf{SD}_2 \times \mathbf{G} \times \mathbf{G}$
`idpp`	of type $\mathbf{SD}_2 \times \mathbf{SD} \times \mathbf{G} \times \mathbf{G}$
`psf`	of type $(\mathbf{G} \to {}^{z}\mathbf{G} \times {}^{z}\mathbf{G}) \times (\mathbf{H} \to (\mathbf{N} + \mathbf{PSD} \times \mathbf{G} \times {}^{z}\mathbf{G})^2)$
`apbg`	of type $\mathbf{PSD} \times \mathbf{G} \times {}^{z}\mathbf{G}$

Constants

`Rec, CoRec`	recursion, corecursion
`Des`	destructor
`PsdToSd`	embedding of **PSD** into **SD**
`plus, times, inv`	arithmetic in **SD**
`cL`	realizer for lemma L

Terms

`[x]r`	lambda abstraction $\lambda_x r$
`r@s`	product term
`left r, right r`	components (prefix, binding strongest)
`InL, InR`	injections into a sum type

6.3. **CoIAverage.** We analyze the term in Figure 4 extracted from CoIAverage. The first argument N of the corecursion operator destructs `v`, `v0`

```
[v,v0](CoRec sdtwo@@iv@@iv=>iv)
 (left Des v plus left Des v0@right Des v@right Des v0)
 ([ivw][let jdvw
     (J left Des left right ivw
        left Des right right ivw
        left ivw@
     K left Des left right ivw
       left Des right right ivw
       left ivw@
     right Des left right ivw@
     right Des right right ivw)
     (left right jdvw@InR(left jdvw@right right jdvw))])
```

FIGURE 4. Extracted term for CoIAverage.

into their components (d, v), (e, w) and forms $(d + e, v, w)$. The step function M, when applied to an argument `ivw` of type $\tau = \mathbf{SD}_2 \times \mathbf{I} \times \mathbf{I}$, M gives a result of type $\mathbf{SD} \times (\mathbf{I} + \tau)$, as follows. Destruct `ivw` into the form $(i, (d, v), (e, w))$, and let `jdvw` be the quadruple $(J(d, e, i), K(d, e, i), v, w)$. Return $(K(d, e, i), \mathrm{inr}(J(d, e, i), v, w))$.

Hence we can write ${\lambda_y}^{\mathrm{co}}\mathcal{R}^{\tau}_{\mathbf{I}} yM$ as a function $f\colon \tau \to \mathbf{I}$ defined by

$$f(i, \mathrm{C}_d(v), \mathrm{C}_e(w)) = \mathrm{C}_{K(d,e,i)}(f(J(d, e, i), v, w)).$$

6.4. **CoGToCoI.** Consider the term in Figure 5 extracted from Lemma 4.5 (CoGToCoIAux). We analyze the second argument M of the corecursion operator (the "step term"). When applied to an argument N of type $\tau = \mathbf{PSD} \times (\mathbf{G} + \mathbf{H})$, M returns a result of type $\mathbf{SD} \times (\mathbf{I} + \tau)$; it will be in the right part of $\mathbf{I} + \tau$ (i.e., here we do not use the fact that our coinductive definitions are in "strengthened" form). Consider the right hand side N_2 of N, of type $\mathbf{G} + \mathbf{H}$.

Case 1. If N_2 is of the form $\mathrm{inl}(p)$ with p of type $\mathbf{G}$, destruct p. Recall that $\mathbf{G}$ has two constructors, LR and U. If p is of the form $\mathrm{LR}_b(p')$, the result is $(ab, \mathrm{inr}(-ab, \mathrm{inl}(p')))$. If p is of the form $\mathrm{U}(q)$, the result is $(0, \mathrm{inr}(a, \mathrm{inr}(q)))$.

Case 2. If N_2 is of the form $\mathrm{inr}(q)$ with q of type $\mathbf{H}$, destruct q. Recall that $\mathbf{H}$ has two constructors, Fin and D. If q is of the form $\mathrm{Fin}_b(p)$, the result is $(ab, \mathrm{inr}(ab, \mathrm{inl}(p)))$. If q is of the form $\mathrm{D}(q')$, the result is $(0, \mathrm{inr}(a, \mathrm{inr}(q')))$. Hence ${\lambda_y}^{\mathrm{co}}\mathcal{R}^{\tau}_{\mathbf{I}} yM$ is a function $[f, g]\colon \mathbf{PSD} \times \mathbf{G} + \mathbf{PSD} \times \mathbf{H} \to \mathbf{I}$ defined by

$$f(a, \mathrm{LR}_b(p)) = \mathrm{C}_{ab}(f(-ab, p)), \qquad g(a, \mathrm{Fin}_b(p)) = \mathrm{C}_{ab}(f(ab, p)),$$

```
[apq](CoRec psd@@(ag ysum ah)=>iv)apq
 ([apq0][case (right apq0)
     (InL p -> [case (Des p)
       (InL ap ->
       PsdToSd(left apq0 times left ap)@
       InR(inv(left apq0 times left ap)@InL right ap))
       (InR q -> Mid@InR(left apq0@InR q))])
     (InR q -> [case (Des q)
       (InL ap ->
       PsdToSd(left apq0 times left ap)@
       InR(left apq0 times left ap@InL right ap))
       (InR q0 -> Mid@InR(left apq0@InR q0))])])
```

FIGURE 5. Extracted term for CoGToCoIAux.

$$f(a, \mathrm{U}(q)) \quad = \mathrm{C}_0(g(a,q)), \qquad\qquad g(a, \mathrm{D}(q)) \quad = \mathrm{C}_0(g(a,q)).$$

6.5. **CoIToCoG.** For Lemma 4.7 (CoIToCoGAux) we obtain the extracted term in Figure 6.

```
[bv](CoRec psd@@iv=>ag psd@@iv=>ah)bv
 ([bv0][case (left Des right bv0)
     (Lft -> InL(inv left bv0@InR(PRht@right Des right bv0)))
     (Rht -> InL(left bv0@InR(PLft@right Des right bv0)))
     (Mid -> InR(InR(left bv0@right Des right bv0)))])
 ([bv0][case (left Des right bv0)
     (Lft -> InL(inv left bv0@InR(PLft@right Des right bv0)))
     (Rht -> InL(left bv0@InR(PRht@right Des right bv0)))
     (Mid -> InR(InR(left bv0@right Des right bv0)))])
```

FIGURE 6. Extracted term for CoIToCoGAux.

To understand this term recall the type (35) of the simultaneous corecursion operators ${}^{\mathrm{co}}\mathcal{R}^{(\mathbf{G},\mathbf{H}),(\tau,\tau)}_{\mathbf{G}}$ and ${}^{\mathrm{co}}\mathcal{R}^{(\mathbf{G},\mathbf{H}),(\tau,\tau)}_{\mathbf{H}}$, or shortly ${}^{\mathrm{co}}\mathcal{R}_{\mathbf{G}}$ and ${}^{\mathrm{co}}\mathcal{R}_{\mathbf{H}}$, with $\tau := \mathbf{PSD} \times \mathbf{I}$ and step types $\delta := \tau \to \mathbf{PSD} \times (\mathbf{G} + \tau) + (\mathbf{H} + \tau)$. We again analyze the particular step functions M, M' extracted from our proof. When applied to an argument N of type $\tau = \mathbf{PSD} \times \mathbf{I}$, M returns a result of type $\mathbf{PSD} \times (\mathbf{G} + \tau) + (\mathbf{H} + \tau)$, in the right part of $\mathbf{G} + \tau$ or $\mathbf{H} + \tau$. Let $N = (b, v)$ with v of type $\mathbf{I}$, of the form $\mathrm{C}_d(v')$. The result is

$$\mathrm{inl}(-b, \mathrm{inr}(1, v')) \quad \text{if } d = -1,$$

$$\begin{cases} \mathrm{inl}(b, \mathrm{inr}(-1, v')) & \text{if } d = 1, \\ \mathrm{inr}(\mathrm{inr}(b, v')) & \text{if } d = 0. \end{cases}$$

Similarly, when applied to an argument N of type $\tau = \mathbf{PSD} \times \mathbf{I}$, M' returns a result of type $\mathbf{PSD} \times (\mathbf{G} + \tau) + (\mathbf{H} + \tau)$. Let $N = (b, v)$ with v of type $\mathbf{I}$, of the form $\mathrm{C}_d(v')$. The result is

$$\begin{cases} \mathrm{inl}(-b, \mathrm{inr}(-1, v')) & \text{if } d = -1, \\ \mathrm{inl}(b, \mathrm{inr}(1, v')) & \text{if } d = 1, \\ \mathrm{inr}(\mathrm{inr}(b, v')) & \text{if } d = 0. \end{cases}$$

Hence we can write the two functions $\lambda_y {}^{\mathrm{co}}\mathcal{R}_{\mathbf{G}} y M M'$ and $\lambda_y {}^{\mathrm{co}}\mathcal{R}_{\mathbf{H}} y M M'$ as $g\colon \tau \to \mathbf{G}$ and $h\colon \tau \to \mathbf{H}$ defined by

$$\begin{aligned} g(b, \mathrm{C}_{-1}(v)) &= \mathrm{LR}_{-b}(g(1, v)), & h(b, \mathrm{C}_{-1}(v)) &= \mathrm{Fin}_{-b}(g(-1, v)), \\ g(b, \mathrm{C}_1(v)) &= \mathrm{LR}_b(g(-1, v)), & h(b, \mathrm{C}_1(v)) &= \mathrm{Fin}_b(g(1, v)), \\ g(b, \mathrm{C}_0(v)) &= \mathrm{U}(h(b, v)), & h(b, \mathrm{C}_0(v)) &= \mathrm{D}(h(b, v)). \end{aligned}$$

6.6. **CoGAverage.** For Lemma 4.9 (CoGMinus) the extracted term is shown in Figure 7.

```
[p](CoRec ag=>ag ah=>ah)p
 ([p0][case (Des p0)
     (InL ap -> InL(inv left ap@InL right ap))
     (InR q -> InR(InR q))])
 ([q][case (Des q)
     (InL ap -> InL(inv left ap@InL right ap))
     (InR q0 -> InR(InR q0))])
```

FIGURE 7. Extracted term for CoGMinus.

We need simultaneous corecursion operators ${}^{\mathrm{co}}\mathcal{R}_{\mathbf{G}}^{(\mathbf{G},\mathbf{H}),(\sigma,\tau)}$, ${}^{\mathrm{co}}\mathcal{R}_{\mathbf{H}}^{(\mathbf{G},\mathbf{H}),(\sigma,\tau)}$ of type (35). By analyzing the particular step functions M, M' extracted from our proof we see that we can write $\lambda_y {}^{\mathrm{co}}\mathcal{R}_{\mathbf{G}} y M M'$ and $\lambda_z {}^{\mathrm{co}}\mathcal{R}_{\mathbf{H}} z M M'$ as functions $f\colon \sigma \to \mathbf{G}$ and $f'\colon \tau \to \mathbf{H}$ defined by

$$\begin{aligned} f(\mathrm{LR}_a(p)) &= \mathrm{LR}_{-a}(p), & f'(\mathrm{Fin}_a(p)) &= \mathrm{Fin}_{-a}(p), \\ f(\mathrm{U}(q)) &= \mathrm{U}(f'(q)), & f'(\mathrm{D}(q)) &= \mathrm{D}(f'(q)). \end{aligned}$$

Lemma 4.9 (CoGMinus) gave us Lemma 4.10 (CoHToCoG).

The extracted term in Figure 8 clearly represents the functions shown as implicit algorithm in Section 4.4.

```
[q](CoRec ah=>ag ag=>ah)q
 ([q0][case (Des q0)
     (InL ap -> InL(left ap@InL(cCoGMinus right ap)))
     (InR q1 -> InR(InL q1))])
 ([p][case (Des p)
     (InL ap -> InL(left ap@InL(cCoGMinus right ap)))
     (InR q0 -> InR(InL q0))])
```

FIGURE 8. Extracted term for CoHToCoG.

We now come to the average for Gray-code. As a preparation we need an easy consequence of CoGMinus, a lemma CoGPsdTimes with extracted term `[a,p][case a (PLft -> cCoGMinus p) (PRht -> p)]`.

For Lemma 4.11 (CoGAvToAvc) the extracted term in Figure 9 again clearly represents the function shown as implicit algorithm in Section 4.4.

```
[p,p0][case (Des p)
   (InL ap ->
   [case (Des p0)
     (InL ap0 -> left ap plus left ap0@
                 cCoGPsdTimes inv left ap right ap@
                 cCoGPsdTimes inv left ap0 right ap0)
     (InR q -> left ap plus Mid@
               cCoGPsdTimes inv left ap right ap@
               cCoHToCoG q)])
   (InR q ->
   [case (Des p0)
     (InL ap -> Mid plus left ap@
                cCoHToCoG q@
                cCoGPsdTimes inv left ap right ap)
     (InR q0 -> MT@cCoHToCoG q@cCoHToCoG q0)])]
```

FIGURE 9. Extracted term for CoGAvToAvc.

For Lemma 4.12 (CoGAvcSatCoICl) the extracted term is shown in Figure 10. It is rather easy to parse into how it is written in Section 4.4.

For Lemma 4.13 (CoGAvcToCoG) we need as a preparation an easy lemma SdDisj: $\forall_d(d = 0 \vee \exists_a(d = a))$, with extracted term

```
[d][case d (Lft -> Inr PLft) (Rht -> Inr PRht) (Mid -> DummyL)]
```

```
[i,p,p0][case (Des p)
   (InL ap ->
   [case (Des p0)
     (InL ap0 -> J(PsdToSd left ap)(PsdToSd left ap0)i@
                 K(PsdToSd left ap)(PsdToSd left ap0)i@
                 cCoGPsdTimes inv left ap right ap@
                 cCoGPsdTimes inv left ap0 right ap0)
     (InR q ->   J(PsdToSd left ap)Mid i@
                 K(PsdToSd left ap)Mid i@
                 cCoGPsdTimes inv left ap right ap@
                 cCoHToCoG q)])
   (InR q ->
   [case (Des p0)
     (InL ap -> J Mid(PsdToSd left ap)i@
                K Mid(PsdToSd left ap)i@
                cCoHToCoG q@
                 cCoGPsdTimes inv left ap right ap)
     (InR q0 -> J Mid Mid i@K Mid Mid i@
                cCoHToCoG q@cCoHToCoG q0)])]
```

FIGURE 10. Extracted term for CoGAvcSatCoICl.

It is easy to see that the extracted term for Lemma 4.13 (in Figure 11) gives the algorithm in Section 4.4.

Now for Proposition 4.14 (CoGAverage) the extracted term is obtained just by composition of those for Lemmata 4.11 and 4.13:

```
[p,p0]cCoGAvcToCoG(cCoGAvToAvc p p0)
```

6.7. **CoGToBG.** For Lemma 4.16 again the extracted term (see Figure 12) represents the algorithms given in Section 4.5

6.8. **CoGToCoM.** Finally Figure 13 gives the term extracted from our proof of Proposition 5.5.

REFERENCES

[1] U. Berger. Program extraction from normalization proofs. In M. Bezem and J. Groote, editors, *Typed Lambda Calculi and Applications*, volume 664 of *LNCS*, pages 91–106. Springer Verlag, Berlin, Heidelberg, New York, 1993.

```
[ipp](CoRec sdtwo@@ag@@ag=>ag sdtwo@@ag@@ag=>ah)ipp
 ([ipp0]
   [let idpp (cCoGAvcSatCoICl
               left ipp0 left right ipp0 right right ipp0)
     [case (cSdDisj left right idpp)
      (DummyL -> InR(InR(left idpp@right right idpp)))
      (Inr a ->
      InL(a@InR
       (a times inv left idpp@
        cCoGPsdTimes inv a left right right idpp@
        cCoGPsdTimes inv a right right right idpp)))]])
 ([ipp0][let idpp (cCoGAvcSatCoICl
                    left ipp0 left right ipp0 right right ipp0)
     [case (cSdDisj left right idpp)
      (DummyL -> InR(InR(left idpp@right right idpp)))
      (Inr a ->
      InL(a@InR
       (a times left idpp@
        cCoGPsdTimes a left right right idpp@
        cCoGPsdTimes a right right right idpp)))]])
```

FIGURE 11. Extracted term for CoGAvcToCoG.

[2] U. Berger and M. Seisenberger. Proofs, programs, processes. In F. Ferreira et al., editors, *Proceedings CiE 2010*, volume 6158 of *LNCS*, pages 39–48. Springer Verlag, Berlin, Heidelberg, New York, 2010.

[3] C. M. Chuang. *Extraction of Programs for Exact Real Number Computation Using Agda*. PhD thesis, Swansea University, Wales, UK, 2011.

[4] A. Ciaffaglione and P. D. Gianantonio. A co-inductive approach to real numbers. In *Proc. of the workshop "Types 1999"*, volume 1956 of *LNCS*, pages 114–130. Springer Verlag, Berlin, Heidelberg, New York, 1999.

[5] P. D. Gianantonio. An abstract data type for real numbers. *Theoretical Computer Science*, 221(1-2):295–326, 1999.

[6] A. N. Kolmogorov. Zur Deutung der intuitionistischen Logik. *Math. Zeitschr.*, 35:58–65, 1932.

[7] K. Miyamoto. *Program extraction from coinductive proofs and its application to exact real arithmetic*. PhD thesis, Mathematisches Institut der Universität München, 2013.

[8] K. Miyamoto and H. Schwichtenberg. Program extraction in exact real arithmetic. *Mathematical Structures in Computer Science*, FirstView:1–13, 9 2015.

[9] S. Sagiv, editor. *Programming Languages and Systems, 14th European Symposium on Programming,ESOP 2005, Held as Part of the Joint European Conferences on Theory*

```
[n](Rec nat=>(ag=>bg@@bg)@@
             (ah=>(nat ysum psd@@ag@@bg)@@
                  (nat ysum psd@@ag@@bg)))
 n
 (([p]Nz@[case (Des p) (InL ap -> LRz left ap Nz)
                       (InR q -> Uz Zero)])@
  ([q]InL Zero@
    [case (Des q)
      (InL ap -> InR(left ap@right ap@Nz))
      (InR q0 -> InL(Succ Zero))]))
 ([n0,psf]
   ([p]right(left psf p)@
     [case (Des p)
       (InL ap -> LRz left ap right(left psf right ap))
       (InR q ->
       [case (right(right psf q))
         (InL n -> Uz n)
         (InR apbg -> LRz left apbg
                       (LRz PRht right right apbg))])])@
   ([q]right(right psf q)@
     [case (Des q)
       (InL ap -> InR(left ap@right ap@
                      right(left psf right ap)))
       (InR q0 ->
       [case (right(right psf q0))
         (InL n1 -> InL(Succ n1))
         (InR apbg ->
         InR
         (left apbg@
          cCoGClauseInv(InL(PLft@left right apbg))@
          right(left psf(cCoGClauseInv
                         (InL(PLft@left right apbg))))))])]))
```

FIGURE 12. Extracted term for CoGToBGAux.

and Practice of Software, ETAPS 2005, Edinburgh, UK, April 4-8, 2005, Proceedings, volume 3444 of *Lecture Notes in Computer Science*. Springer, 2005.

[10] H. Schwichtenberg and S. S. Wainer. *Proofs and Computations*. Perspectives in Logic. Association for Symbolic Logic and Cambridge University Press, 2012.

[11] K. Terayama and H. Tsuiki. A stream calculus of bottomed sequences for real number computation. *Electr. Notes Theor. Comput. Sci.*, 298:383–402, 2013.
[12] H. Tsuiki. Real number computation through Gray code embedding. *Theoretical Computer Science*, 284:467–485, 2002.
[13] H. Tsuiki. Real number computation with committed choice logic programming languages. *J. Log. Algebr. Program.*, 64(1):61–84, 2005.
[14] H. Tsuiki and K. Sugihara. Streams with a bottom in functional languages. In Sagiv [9], pages 201–216.
[15] E. Wiedmer. *Exaktes Rechnen mit reellen Zahlen und anderen unendlichen Objekten.* PhD thesis, ETH Zürich, 1977.
[16] E. Wiedmer. Computing with infinite objects. *Theoretical Comput. Sci.*, 10:133–155, 1980.

```
[p](CoRec ag=>ag ah=>ah)p
 ([p0][case (Des p0)
     (InL ap -> [case (Des right ap)
       (InL ap0 -> [case (left ap0)
         (PLft -> InL(left ap@InR right ap))
         (PRht -> [case (Des right ap0)
           (InL ap1 -> [case (left ap1)
             (PLft -> InR(InR(cCoHClauseInv
                              (InL(left ap@right ap0)))))
             (PRht -> InL(left ap@InR right ap))])
           (InR q -> InL(left ap@InR right ap))])])
       (InR q -> InL(left ap@InR right ap))])
     (InR q -> [case (Des q)
       (InL ap -> [case (Des right ap)
         (InL ap0 -> [case (left ap0)
           (PLft -> InR(InR(cCoHClauseInv(InL ap))))
           (PRht -> InL(left ap@InR(cCoGClauseInv
                     (InR(cCoHClauseInv(InL(PRht@right ap0)))))))])
         (InR q0 -> InR(InR(cCoHClauseInv(InL ap))))])
       (InR q0 -> InR(InR q))])])
 ([q][case (Des q)
     (InL ap -> [case (Des right ap)
       (InL ap0 -> [case (left ap0)
         (PLft -> [case (Des right ap0)
           (InL ap1 -> [case (left ap1)
             (PLft -> InR(InR(cCoHClauseInv
                              (InL(left ap@right ap)))))
             (PRht -> InL(left ap@InR right ap))])
           (InR q0 -> InL(left ap@InR right ap))])
         (PRht -> InL(left ap@InR right ap))])
       (InR q0 -> InL(left ap@InR right ap))])
     (InR q0 -> [case (Des q0)
       (InL ap -> [case (Des right ap)
         (InL ap0 -> [case (left ap0)
           (PLft -> InR(InR(cCoHClauseInv(InL ap))))
           (PRht -> InL(left ap@InR(cCoGClauseInv
                     (InR(cCoHClauseInv(InL(PLft@right ap0)))))))])
         (InR q1 -> InR(InR(cCoHClauseInv(InL ap))))])
       (InR q1 -> InR(InR q0))])])
```

FIGURE 13. Extracted term for CoGToCoM.