Definite Descriptions and Dijkstra’s Odd Powers of Odd Integers Problem

Hugh Gibbons

Computer Science Dept.,
Trinity College,
Dublin, Ireland

Abstract

The use of Frege-Russell style definite descriptions for giving meaning to functions has been long established and we investigate their use in the development of Functional Programs and from these to the development of correct imperative programs. In particular, we investigate the development of a functional program for a problem, "Odd powers of odd integers", discussed by Dijkstra. If the correctness of termination is not a concern then it is straightforward to develop a partially correct program. Further properties of the specification are needed to develop a totally correct program.

Keywords: definite descriptions, functional programming, assertions, partial and total correctness.

1 Introduction

The use of definite descriptions dates back to Frege and Russell [13] and also to further development by Quine [12] and Scott [14]. The use and definitions of definite descriptions are explained in Kalish and Montague [9]. In this article we consider reusing definite descriptions in the development of functional programs. As assertions have a central role in the development of imperative programs as promoted by Dijkstra [5] and Gries [8] and the Refinement Calculus [11], we consider the role of definite descriptions in the development of functional programs which can then be further developed to imperative programs.

In this article we investigate in detail the formal development of totally correct programs for a specification described by Dijkstra [6].

For $1 \leq p$ and odd $p$ and $1 \leq k$ and odd $r$ such that $1 \leq r < 2^k$, a value $x$ exists such that

$$1 \leq x < 2^k \land 2^k \mid (x^p - r) \land \text{odd } x$$

1 Email: hugh.gibbons@cs.tcd.ie
We are using ‘|’ for ‘divides’.

If proof of termination is not a concern then a very straightforward partially correct program can be easily developed. Proving termination uses induction and from the induction proof a simple functional program is derived. Based on this functional program, a totally correct imperative program is developed similar to that given by Dijkstra. Further properties of the specification are derived using the functional program and an alternative functional program is derived. While the alternative functional program is straightforward, its development into an imperative program is not. This development involves the transformation of linear recursion to an appropriate tail recursive form which can then be directly transformed to imperative programs with the tail recursive programs providing the invariants for the associated loops.

In the development of the functional versions of the specification we make use of the definite descriptors, ‘the’ and ‘least’.

1.1 Definite description, ‘the’

\[ y = \text{the one and only item satisfying } p \]
\[ y = (\text{the } x \cdot p \ x) \]
\{Russell\}
\[ \equiv (\forall x \cdot x = y \equiv p \ x) \]
\{Quine\}
\{y\} = \{x \cdot p \ x\}

1.2 Definite description, ‘least’

\[ y = (\text{least } x \cdot n \leq x \land p \ x) \]
\[ \equiv n \leq y \land p \ y \land (\forall x \cdot n \leq x < y \rightarrow \neg (p \ x)) \]

In particular,
\[ g \ n = (\text{least } x \cdot n \leq x \land p \ x) \]
\[ = (p \ n \rightarrow n) \land (\neg (p \ n) \rightarrow (\text{least } x \cdot (n + 1) \leq x \land p \ x)) \]
\[ = \text{if } p \ n \text{ then } n \text{ else } g \ (n + 1) \]

In terms of functional programming lists,
\[ y = (\text{least } x \cdot n \leq x \land p \ x) \]
\[ y = \text{head}[x \mid x \leftarrow [n..], p \ x] \]

1.3 Simple Floor Square Root

As an introductory application of definite descriptions we develop a simple program for finding the integer square root of a number.

For \( 0 \leq x \) we define the (positive) square root of \( x \), as
\[ \sqrt{x} = (\text{the } r \cdot 0 \leq r \land r^2 = x) \]
We can define the floor square root, \([\sqrt{x}]\) as
\[
\begin{align*}
r &= \lfloor \sqrt{x} \rfloor \\
\equiv & \ r \leq \sqrt{x} < r + 1 \\
\equiv & \ r^2 \leq x < (r + 1)^2
\end{align*}
\]
i.e. \([\sqrt{x}] = (\text{the } r \cdot 0 \leq r^2 \leq x < (r + 1)^2)\)

Show that
\([\sqrt{x}] = (\text{least } r \cdot 0 \leq r \land x < (r + 1)^2)\)

**Theorem 1.1**

\[y = (\text{least } r \cdot 0 \leq r \land x < (r + 1)^2) \Rightarrow y \in \{r \cdot 0 \leq r \land r^2 \leq x < (r + 1)^2\}\]

**Proof** Since
\[
\begin{align*}
y &= (\text{least } r \cdot 0 \leq r \land x < (r + 1)^2) \\
\Rightarrow & \ 0 \leq y \land x < (y + 1)^2
\end{align*}
\]
Need to just show that \(y^2 \leq x\)
\[
y = (\text{least } r \cdot 0 \leq r \land x < (r + 1)^2)
\Rightarrow \ (\forall r \cdot 0 \leq r < y \rightarrow (0 \leq r \land x < (r + 1)^2))
\equiv \ (\forall r \cdot 0 \leq r < y \rightarrow (0 > r \lor x \geq (r + 1)^2))
\equiv \ (\forall r \cdot 0 \leq r < y \rightarrow x \geq (r + 1)^2)
\{\text{witness } \hat{r} = y - 1\}
\Rightarrow x \geq y^2
\]
End proof. \(\square\)

Let
\[
fl_{\_sq}rt \ x \ n = (\text{least } r \cdot n \leq r \land x < (r + 1)^2)
\]
\[= \text{if } x < (n + 1)^2 \text{ then } n \text{ else } fl_{\_sq}rt \ x \ (n + 1)\]

therefore
\[
fl_{\_sq}rt \ x \ 0 = \lfloor \sqrt{x} \rfloor
\]

Writing this as a functional program:
\[
\lfloor \sqrt{x} \rfloor \equiv fl_{\_sq}rt \ x \ 0
\]

where
\[
fl_{\_sq}rt \ x \ n
|\ x < (n + 1)^2 \equiv n
|\ x \geq (n + 1)^2 \equiv fl_{\_sq}rt \ x \ (n + 1)
\]

We can rewrite this tail recursive functional program as an imperative program with the loop invariant based directly on the functional program.
\[
[\sqrt{-}] :: \text{Real} \rightarrow \text{Int}
\]
Here the tail recursive program, $\text{fl\\_sqrt}$, is used as a loop invariant. This connection between tail recursion and loop invariants is further developed in Gibbons [7] and in Broy and Krieg-Bruckner [3].

2 Dijkstra’s Odd Powers of Odd Integers

For clarity, we repeat the Dijkstra specification given above. For $1 \leq p$ and odd $p$ and $1 \leq k$ and odd $r$ such that $1 \leq r < 2^k$, a value $x$ exists such that

$$1 \leq x < 2^k \land 2^k \mid (x^p - r) \land \text{odd } x$$

**Example 2.1** 13 is a witness for the existential quantifier $x$ in

$$(\exists x \bullet 1 \leq x < 2^4 \land 2^4 \mid (x^3 - 5) \land \text{odd } x)$$

$$2^4 \mid (13^3 - 5) \equiv 16 \mid (2197 - 5)$$

$$\equiv 2192 = 137 \times 16$$

A witness for $x$ in $(\exists x \bullet 0 \leq x \land 2^k \mid (x^p - r))$ must be odd as if $2^k \mid (x^p - r)$ then $x^p - r$ is even, hence $x^p$ is odd since $r$ is odd, therefore $x$ is odd.

2.1 Definite Description function

Consider the following function, $f$, described by a definite description for finding a witness for $x$,

Let $\text{pre } p \ r \ k = 1 \leq p \land \text{odd } p \land 1 \leq k \land \text{odd } r \land 1 \leq r < 2^k$

$$\text{pre } p \ r \ k \rightarrow$$

$$f \ p \ r \ k \equiv (\text{least } x \bullet 1 \leq x < 2^k \land \text{odd } x \land 2^k \mid (x^p - r))$$

i.e. using a precondition

$$\{ \text{pre } p \ r \ k \}$$

$$f \ p \ r \ k \equiv (\text{least } x \bullet 1 \leq x < 2^k \land \text{odd } x \land 2^k \mid (x^p - r))$$
We rewrite \( fp r k \) as a functional program. using list comprehension,

\[
\{ \text{pre } p r k \}
fp r k \equiv \text{head}[x \mid x \leftarrow [1..2^k], \text{odd } x, 2^k \mid (x^p - r)]
\]

or using the higher order function, \( \text{filter} \)

\[
\{ \text{pre } p r k \}
f p r k \equiv \text{head}(\text{filter } b [1,3,\ldots])
\]

where
\[
b x \equiv x < 2^k \land 2^k \mid (x^p - r)
\]

Since in general,
\[
g n \equiv (\text{least } x \bullet n \leq x \land b x)
\equiv \text{if } b n \text{ then } n \text{ else } g(n + 1)
\]
we get an alternate (tail recursive) functional program, \( f_1 \),

\[
\{ \text{pre } p r k \}
f_1 p r k \equiv f_{loc} 1
\]

where
\[
f_{loc} x
| 2^k \mid (x^p - r) \land x < 2^k \equiv x
| \text{otherwise} \equiv f_{loc} (x + 2)
\]

We can use Quickcheck [4] to test if the functions \( f \) and \( f_1 \) are the same.

We can rewrite the functional program \( f_1 \) as an iterative imperative program:
see figure Algorithm 1 (Imperative \( f_1 \))

**Algorithm 1** Imperative \( f_1 \)

\[
f1 : \text{Int} \times \text{Int} \times \text{Int} \rightarrow \text{Int}
f1 (p,r,k) \equiv
\{\text{Pre: } 1 \leq p \land 1 \leq k \land 1 \leq r < 2^k \land \text{odd } r \}
local
\begin{array}{l}
x : \text{Int} \\
begin \\
\{\text{Inv: } f_{loc} 1 = f_{loc} x \}
\text{while } \neg(2^k \mid (x^p - r) \land x < 2^k) \text{ do}
x := x + 2
end \{f_{loc} 1 = x \}
\{f_1 p r k = x\}
\{2^k \mid (x^p - r) \land x < 2^k \land \text{odd } x \}
\text{Result} := x
\end{array}
end.
The loop in this imperative program iterates through the odd integers until it reaches an \( x \) such that \( 2^k | (x^p - r) \land x < 2^k \). When tested the program halts for the given inputs but testing is not enough to prove correctness. If the loop terminates then the program will give the correct result.

3 Alternative FP Version

To show that the loop terminates we are back to showing

\[
(\exists x \cdot \text{odd } x \land 1 \leq x < 2^k \land 2 | (x^p - r))
\]

under the assumption

\[
Pr e \ p r k : 1 \leq p \land \text{odd } p \land 1 \leq k \land \text{odd } r \land 1 \leq r < 2^k.
\]

A normal strategy in the context of the refinement calculus is to strengthen the precondition but here the precondition is weakened by dropping the conjunct, \( 1 \leq r < 2^k \) as it can be shown that \( (\exists x \cdot 1 \leq x \land 2^k | (x^p - r)) \) from the weaker assumption

\[
Pr e' r k : 1 \leq p \land \text{odd } p \land 1 \leq k \land \text{odd } r
\]

Whatever satisfies \( Pr e \) also satisfies \( Pr e' \), i.e. \( Pr e \Rightarrow Pr e' \).

Later we will show that the least witness, \( \hat{x} \), for \( (\exists x \cdot 1 \leq x \land 2^k | (x^p - r)) \) is such that \( \hat{x} < 2^k \).

**Theorem 3.1**

\[
1 \leq p \land \text{odd } p \land 1 \leq k \land \text{odd } r \Rightarrow (\exists x \cdot \text{odd } x \land 2^k | (x^p - r))
\]

**Proof** (By induction on \( k \))

Base case (\( k=1 \))

Let \( x = 1 \); since \( r \) is odd then \( 1^p - r \) is even therefore \( 2 | (1^p - r) \)

Also, \( x = 1 \) is the least such \( x \).

Induction step:

Assume \( x \) is the least \( x \) such that \( \text{odd } x \land 2^k | (x^p - r) \), determine least \( \text{odd } y \) such that \( 2^{k+1} | (y^p - r) \).

If \( 2^{k+1} | (x^p - r) \), let \( y = x \)

If \( \neg (2^{k+1} | (x^p - r)) \) then \( \frac{x^p - r}{2^k} \) is odd.

Let \( y = x + 2^k \),

\[
\frac{y^p - r}{2^k} = \frac{(x+2^k)^p - r}{2^k} = \frac{x^p + p x^{p-1} 2^k + \ldots + px (2^{(p-1)k} + 2^{(p-1)k}) - 2^k}{2^k} = \frac{x^p - r}{2^k} + px^{p-1} + \ldots + px 2^{(p-2)k} + 2^{(p-1)k}
\]

\[
\{ \frac{x^p - r}{2^k} \text{ and } px^{p-1} \text{ are odd } \}
\]

\[
\frac{y^p - r}{2^k} \text{ is even}
\]
Also, \( y = x + 2^k \) is the least such \( y \) as if \( y = x + n \) with (even \( n \)) and \( n < 2^k \) then

\[
(x + n)p - r = \frac{x^p - r}{2^k} + \frac{px^{p-1}n + \cdots + n^p}{2^k}
\]

\( 2^k \mid (x^p - r) \) but \( \neg (2^k \mid n (px^{p-1} + \cdots + n^{p-1})) \) as \( n < 2^k \) and \( px^{p-1} + \cdots + n^{p-1} \) is odd.

From this inductive proof, we get the recursive functional program, \( f_{2prk} \), for finding \( x \) such that \( \text{odd } x \land 2^k \mid (x^p - r) \)

\[
\{ \leq p \land \text{odd } p \land \leq k \land \text{odd } r \}
\]

\[
f_{2pr1} \equiv 1
\]

\[
f_{2pr(k+1)} \equiv \text{if } 2^{k+1} \mid (x^p - r) \text{ then } x + 2^k
\]

\text{where}

\[
x \equiv f_{2prk}
\]

It is clear this function terminates with respect to the precondition: \( 1 \leq k \).

**Theorem 3.2**

\( \text{pre } prk \Rightarrow f_{2prk} < 2^k \)

where

\( \text{pre } prk \equiv 1 \leq p \land \text{odd } p \land \leq k \land \text{odd } r \land \leq r < 2^k \)

**Proof** (By induction on \( k \))

Base case: \( (k=1) \)

\[
f_{2pr1} = 1 < 2
\]

Induction Step: \( (k > 1) \) Assume \( f_{2prk} < 2^k \)

Case \( 2^{k+1} \mid f_{2prk} \)

\[
f_{2pr(k+1)} = f_{2prk} < 2^k < 2^{k+1}
\]

Case \( \neg (2^{k+1} \mid f_{2prk}) \)

\[
f_{2pr(k+1)} = f_{2prk} + 2^k < 2^k + 2^k = 2^{k+1}
\]

End Proof.
The function, $f_{2 \, p \, r \, k}$, also satisfies the stronger specification:

$$1 \leq p \land \text{odd } p \land 1 \leq k \land \text{odd } r \land 1 \leq r < 2^k \rightarrow f_{2 \, p \, r \, k} \equiv (\text{least } x \bullet 1 \leq x < 2^k \land \text{odd } x \land x^p \text{ mod } 2^k = r)$$

and thus is a functional program that satisfies the specification given by Dijkstra.

Dijkstra provides an imperative solution based on the invariant

$$1 \leq x < 2^k \land 2^k | (x^p - r) \land \text{odd } x$$

Concerning his own imperative solution, Dijkstra states in [6]:

“I have evidence that, despite the existence of this very simple solution, the problem is not trivial: many computer scientists could not solve the programming problem within an hour. Try it on you colleagues, if you don’t believe me”

We derive an iterative solution from the recursive version $f_{2 \, p \, r \, k}$.

### 3.1 Iterative version

The imperative program, $f_1$ above, may be considered an imperative solution of the original $f$ once termination has been guaranteed.

A more direct version of an iterative program can be developed from the recursive program $f_2$. Consider the set

$$F = \{(p, r, k, y) \bullet 1 \leq k \land \text{odd } p \land 1 \leq p \land \text{odd } r \land y = f_{2 \, p \, r \, k}\}$$

Let $\text{pre } p \, r \, k = 1 \leq k \land \text{odd } p \land 1 \leq p \land \text{odd } r \land 1 \leq r$

For $k = 1$

$$((p, r, 1), 1) \in F.$$  

If $((p, r, k), x) \in F$ then

if $2^{k+1} | (x^p - r)$ then

$$((r, k + 1), x) \in F$$

else

$$((p, r, k + 1), x + 2^k) \in F$$

The set $F$ is an inductively defined set of ordered pairs such that

$$((p, r, k), y) \in F \Rightarrow y = f_{2 \, p \, r \, k}$$

Based on the inductive set $F$ we get the specification for an iterative function $f_t$

$$1 \leq k \land \text{odd } p, r \land 1 \leq p, r \rightarrow f_t \, p \, n \, r \, k \, x \equiv (\text{least } y \bullet k = n \land ((p, r, k), y) \in F \land x = y)$$

We write $f_t \, p \, n \, r \, k \, x$ as the functional program,

$$\{ \text{odd } p \land 1 \leq k \land \text{odd } r \}$$

$$f_t \, p \, n \, r \, k \, x \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad 

| $k = n$ | $\equiv x$ |
| $2^{k+1} | (x^p - r)$ | $\equiv f_t n r (k + 1) x$ |
| otherwise | $\equiv f_t p n r (k + 1) (x + 2^k)$ |

Rewriting this as an imperative program; see Algorithm 2 (Imperative ft),

**Algorithm 2** Imperative ft

```plaintext
ft::Int×Int×Int → Int
ft (p,r,k) ≡
{Pre: $1 \leq p \land \text{odd } p \land 1 \leq k \land \text{odd } r \land 1 \leq r < 2^k$ }
local
  j, x : Int
begin
  x := 1; j := 1
  {Inv: $2^k | (x^p - r) \land \text{odd } x \land 1 \leq j \leq k$}
  while $j \neq k$ do
    if $2^{j+1} | (x^p - r)$ then
      j := j+1
    else
      x := x + 2^j;
      j := j+1
    end
  end
  { $2^k | (x^p - r) \land \text{odd } x$ }
  Result := x
end.
```

Rather than explicitly using $2^k$ we can calculate it implicitly as in the following; see Algorithm 3 (Dijkstra version). This is the version similar to that developed by Dijkstra and like the version developed here does not make use of the restriction $1 \leq r < 2^k$ in the initial precondition.
Algorithm 3 Dijkstra version

\[
ft: \text{Int} \times \text{Int} \times \text{Int} \rightarrow \text{Int}
\]

\[
ft(p, r, k) \equiv
\]

\[
\{ \text{Pre: } 1 \leq p \land \text{odd } p \land 1 \leq k \land \text{odd } r \land 1 \leq r < 2^k \}
\]

\[
\text{local}
\]

\[
j, x, d : \text{Int}
\]

\[
\begin{align*}
j &:= 1 ; \quad x := 1 ; \quad d := 2 \\
\{ \text{Inv: } 2^j | (x^p - r) \land \text{odd } x \land 1 \leq j \leq n \land d = 2^j \}
\end{align*}
\]

\[
\text{while } j \neq k \text{ do}
\]

\[
\quad \text{if } \neg (2 \ast d | (x^p - r)) \text{ then}
\quad x := x + d
\quad \text{end}
\]

\[
\quad d := 2 \ast d
\quad j := j + 1
\quad \text{end}
\]

\[
\{ 2^k | (x^p - r) \land \text{odd } x \}
\]

\[
\text{Result } := x
\]

end.

4 Linear Recursion

As a consequence of the following theorem the restriction in the precondition of the specification that \(1 \leq r < 2^k\) is redundant. A linear recursive function results which also satisfies the Dijkstra specification and which then can be developed into an imperative program.

**Theorem 4.1**

\[
2^k | (x^p - r) \equiv 2^k | (x^p - (r \mod 2^k))
\]

**Proof** For some \(q_1\) and \(q_2\),

\[
2^k | (x^p - r)
\]

\[
\equiv (x^p - r) = q_1 2^k
\]

\[
\equiv \{ r = q_2 2^k + r \mod 2^k \}
\]

\[
(x^p - (q_2 2^k + r \mod 2^k)) = q_1 2^k
\]

\[
\equiv x^p - r \mod 2^k = q_1 2^k + q_2 2^k
\]

\[
\equiv x^p - r \mod 2^k = (q_1 + q_2)2^k
\]

\[
\equiv 2^k | (x^p - r \mod 2^k)
\]

End Proof. \(\square\)

From this theorem can conclude that

\[
f_2 p r k = f_2 p (r \mod 2^k) k
\]
Since \( r \mod 2^k < 2^k \) we also have,
\[
\{ 1 \leq p \land \text{odd } p \land 1 \leq r \land \text{odd } r \} \\
f_2 \ p \ r \ k < 2^k
\]
therefore, the restriction that \( r < 2^k \) is redundant.

If \( x = f_2 \ p \ r \ k \) then \( x < 2^k \land x^p \mod 2^k = r \mod 2^k \)

### 4.1 Alternative program

Taking advantage of the result that \( f_2 \ p \ r \ k = f_2 \ p \ (r \mod 2^k) \ k \) and without loss of generality fixing \( p \) to be the odd number 3 we can rewrite \( f_2 \ 3 \) as a new function \( f_3 \) where

\[
\{ 1 \leq k \land \text{odd } r \} \\
f_3 \ r \ 1 \equiv 1 \\
f_3 \ r \ (k + 1) \equiv \text{if } 2^{k+1} \mid (x^3 - r) \text{ then } x \text{ else } x + 2^k
\]

**where**

\[
\begin{align*}
r_1 &\equiv \mod r \ 2^k \\
x &\equiv f_3 \ r_1 \ k
\end{align*}
\]

This program, \( f_3 \) is more difficult to transform to an imperative/iterative version. In order to derive an imperative version we use the result that \( f_3 \) can be rewritten in a linear recursive form by progressive transformations.

Define auxiliary functions

\[
dv \ x \ r \ k \equiv \text{if } 2^k \mid (x^3 - r) \text{ then } 0 \text{ else } 1
\]

and

\[
next \ x \ r \ k \equiv x + (dv \ x \ r \ k) \ast 2^{k-1} \quad \text{-- finds the next terms after } x
\]

then we can rewrite \( f_3 \) as

\[
\{ 1 \leq k \land \text{odd } r \} \\
f_3 \ r \ k \equiv \text{if } k \neq 1 \text{ then } next (f_3 \ (mod r \ 2^{k-1}) \ (k - 1)) \ r \ k \\
else 1
\]

Writing this in an 'if - then - else' format we get

\[
\begin{align*}
&\{ 1 \leq k \land \text{odd } r \} \\
&f_3 \ r \ k \equiv \text{if } k \neq 1 \\
&\quad \text{then next } (f_3 \ (mod r \ 2^{k-1}) \ (k - 1)) \ r \ k \\
&\quad \text{else } 1
\end{align*}
\]

Using ordered pairs and auxillary functions

\[
nt \ (xr, \ xk) \ (yr, \ yk) \equiv (next \ xr \ yr \ yk, \ yk)
\]
we can reduce this further to a standard form.

\[ f_3 \equiv \text{if } bt \text{ then } nt \left( f_3 \left( gt \right) \right) \text{ else } x \]

### 4.2 Transforming Linear Recursion

Termination of the linear recursive function, \( lr \),

\[ lr \equiv \text{if } b \text{ then } n \left( lr \left( g \right) \right) \text{ else } x \]

depends on the existence of an number \( i \geq 0 \) such that \( \neg b \left( g^i \right) \) where \( g^0 x = x \) and \( g^{i+1} x = g \left( g^i x \right) \).

For a binary function \( f \), similar to definitions in Bird [2], we will use the following higher order function \( \backslash f \) ‘left-reduce’

\[
\begin{align*}
\backslash f \left[ \right] & = \[] \\
\backslash f \left[ x \right] & = x \\
\backslash f \left[ x_1 \ldots x_n \right] & = f \left( \backslash f \left[ x_1 \ldots x_{n-1} \right] \right) x_n
\end{align*}
\]

In particular,

\[ \backslash f \left[ x_1, x_2, x_3 \right] = f \left( f \left( x_1 x_2 \right) \right) x_3 \]

If we have an infix operator \( \circ \), not necessarily associative, then

\[ \circ \left[ x_1 \ldots x_n \right] = (\ldots (x_1 \circ x_2) \ldots) \circ x_n \]

Given the sequence or list

\[ gs = \left[ g^i x, g^{i-1} x, \ldots, g x, x \right] \text{ where } i = (\text{least } j \bullet \neg b \left( g^j \right)) \]
then the linear recursive function,

\[ lr x = \text{if } b x \text{ then } n \left( lr \left( g \right) \right) x \text{ else } x \]

can be implemented as

\[ lr x = \backslash n gs \]

A more general version of this result is proved in Gibbons [7] which is related to the approach of the Computer aided Intuition guided Programming (CIP) group in Munich Technical University led by Bauer [1].

**Theorem 4.2**

\[ lr x = \backslash n gs \]

where

\[
\begin{align*}
  i &= (\text{least } j \bullet \neg b \left( g^j \right)) \\
  gs &= \left[ g^i x, g^{i-1} x, \ldots, g x, x \right]
\end{align*}
\]
Proof (By Induction)

Notation:
If \( i < 0 \) then \([g^i x, g^{i-1} x, \ldots g x, x] = []\)
If \( i = 0 \) then \([g^i x, g^{i-1} x, \ldots g x, x] = [x]\)

end Notation

\( i = 0 \)

0 = (least \( j \bullet \neg b(g^j x)) \)

\( \neg b(x) \)

\( \neg \ n g s = x \)

\( \neg \ l r x = \neg \ n g s \)

\( i > 0 \), Assume true for \( i - 1 \), show true for \( i \).

\( i = (least \ j \bullet \neg b(g^j x)) \)

\( \l r x = (\neg \ n g s = x) \)

\( \neg b(g^j (g x)) \)

Let \( gs1 = [g^{i-1}(g x), g^{i-2}(g x), \ldots g x] \)

By induction,
\( \neg \ n gs1 = \l r (g x) \)

Since \( i > 0 \)

\( \l r x = n(\l r (g x)) x \)

\( = n(\neg \ n gs) x \)

(\text{def } \neg \ n \}

\( = \neg n gs \)

End proof.

4.2.1 Implementing \( l r x \)

Since \( \l r x = \neg n[g^i x, g^{i-1} x \ldots g x, x] \) where = (least \( j \bullet \neg b(g^j x)) \) we consider implementing \( \neg n(x : x s) \).

For an item \( x \) and a list \( x s \), define a function \( l r t \) via

\( l r t x x s = \neg n(x : x s) \)

\( \neg \ l r t x [] = \neg n[x] \)

\( = x \)

Also, for \( x s = y : y s \neq [] \),
\( l r t x x s = \neg n(x : (y : y s)) \)

\( \{ \text{prop. } \neg n \} \)

\( = \neg n((n x y) : y s) \)

\( = l r t (n x, y) y s \)
The function, \( lrt \), is the tail recursive function

\[
lrt \ x \ xs = \text{if } xs \neq [] \text{ then } lrt \ (n \ x \ (\text{head} \ xs)) \ (\text{tail} \ xs) \text{ else } x
\]

which can be rewritten as an imperative program which we can use to write an imperative program for \( lrt \). (Algorithm 4)

Algorithm 4
\[
\begin{align*}
lrti \ x \equiv & \{ \text{Pre: } gs = [g^i x, g^{i-1} x, \ldots g x, x] \} \\
& \text{local} \\
& y : \text{Int}; \\
& ys : [\text{Int}] \\
& \begin{align*}
& \text{begin} \\
& y := \text{head} \ gs; \ ys := \text{tail} \ gs \\
& \{ \text{Inv: } \\neg \exists \ n \ gs = \{n(y:ys)\} \} \\
& \text{while } ys \neq [] \text{ do} \\
& \quad y := n \ y \ (\text{head} \ ys) \\
& \quad ys := \text{tail} \ ys \\
& \text{end} \\
& \{y = lrt \ x\} \\
& \text{Result} := y \\
& \text{end lrti}
\end{align*}
\]

4.2.2 Finalising Implementation

What is still needed is a program to establish

\[
gs = [g^i x, g^{i-1} x, \ldots g x, x]
\]

where

\[
i = (\text{least } j \cdot \neg b(g^j x))
\]

Notation:

For lists \( xs, ys \)
\[
xs \ ++ \ ys \text{ is the concatenation of the lists.}
\]

In a similar way to implementing \( \\neg \exists \ gs \) we consider implementing the function

\[
p \ x \ xs = [g^{i-1} x, \ldots g x, x] ++ xs
\]

as for each \( 0 \leq j < i \) we have \( b(g^j x) \).

If \( \neg b \ x \) then \( i = 0 \) and therefore \( p \ x \ xs = xs \).

If \( b \ x \) then

\[
p (g x) (x : xs) = [g^{i-2} (g x), \ldots g x] ++ x : xs = [g^{i-1} x, \ldots g x, x] ++ xs = p \ x \ xs
\]
We can write $pxxs$ as a tail recursive function

$$pxxs \equiv \text{if } b x \text{ then } p(gx)(x : xs) \text{ else } xs$$

Based on this function we can write the following imperative program, init_lrt, (Algorithm 5) that will establish

$$gs = [g^i x, g^{i-1} x, \ldots g x, x]$$

where

$$i = \text{(least } j \bullet -b(g^j x))$$

### Algorithm 5

**init_lrt : Int -> [Int]**

**init_lrt x**

{ **Pre:** (∃i • i = (least j • -b(g^j x)) ) } local

y: Int;
gs: [Int]

begin

y := x; gs := []

while (b y) do 

{ **Inv:** $px[] = pygs$ }

gs := y:gs

y := g y

end 

{ $y = g^i x$ }

gs := y:gs

{ **Post:** gs = [g^i x, g^{i-1} x, \ldots g x, x] }

Result := gs

end init_lrt

### 5 Conclusion

Based on Dijkstra’s specification of the problem of ‘Odd Powers of Odd Integers’ this article applies the theory of definite descriptions and functional programming to first develop a correct functional program and from this to the development of a correct imperative program. If the correctness of termination is not a concern then it is straightforward to develop a partially correct imperative program. By developing functional programs many properties of the program are established and while Dijkstra develops a totally correct program via his own weakest precondition technique it is not clear how other properties could be established. Here it is shown that

$$fprk = fp(r \mod 2^k)k$$

and hence the restriction of $r < 2^k$ is redundant which is not noted by Dijkstra.

The development of the totally correct functional programs was done independently of Dijkstra’s article and it was the discovery of Dijkstra’s article that motivated
the more complete development presented here. Including the development of the functional programs clarifies the development of the imperative program and this article agrees with the view of Manna and Waldinger [10] who state that

“Recursion seem to be the ideal vehicle for systematic program construction”.

In this article recursion is also used as the vehicle for the development of the loop invariants of imperative programs and as a result integrates the development of imperative programs with that of functional programs.

References


