GENERATING THE GREATEST COMMON DIVISOR, AND LIMITATIONS OF PRIMITIVE RECURSIVE ALGORITHMS

L. VAN DEN DRIES

ABSTRACT. The greatest common divisor of two integers cannot be generated in a uniformly bounded number of steps from those integers using arithmetic operations. The proof uses an elementary model-theoretic construction that enables us to focus on "integers with transcendental ratio". This unboundedness result is part of the solution of a problem posed by Y. Moschovakis on limitations of primitive recursive algorithms for computing the greatest common divisor function.

1. INTRODUCTION

Consider gcd as the function $\mathbf{Z}^2 \to \mathbf{Z}$ given by

$$\gcd(a,b) = c \iff c \geq 0 \text{ and } a\mathbf{Z} + b\mathbf{Z} = c\mathbf{Z}.$$

We shall prove among other things that $\gcd(a,b)$ cannot be obtained in a uniformly bounded number of steps starting from the integers a and b by means of the usual arithmetic operations: addition, subtraction, multiplication, and division with remainder. Here is some notation that will enable us to formulate results of this kind in a precise way. In this introduction a and b range over integers. Throughout we let $m, n \in \mathbf{N} = \{0, 1, \dots\}$.

For real x we let $\lfloor x \rfloor$ be the largest integer $\leq x$. We define the functions $\mathrm{qu}, \bmod : \mathbf{Z}^2 \to \mathbf{Z}$ by

$$\mathrm{qu}(a,b) := \lfloor a/b \rfloor \text{ if } b \neq 0, \quad \mathrm{qu}(a,0) := a$$
$$a \bmod b := a - \mathrm{qu}(a,b)b, \text{ in particular } a \bmod 0 = a.$$

Note that $a = \mathrm{qu}(a,b)b + a \bmod b$; moreover, $0 \leq a \bmod b < b$ if $b > 0$ and $b < a \bmod b \leq 0$ if $b < 0$. Thus we may think of $\mathrm{qu}(a,b)$ as the quotient and $a \bmod b$ as the remainder when a is divided by b; together these operations amount to "division with remainder".

We define recursively for any a, b an increasing sequence of finite subsets $G_0(a,b) \subseteq G_1(a,b) \subseteq G_2(a,b) \subseteq \dots$ of $\mathbf{Z}$:

$$G_0(a,b) := \{a, b\}$$
$$G_{n+1}(a,b) := G_n(a,b) \cup \{x + y, x - y, \mathrm{qu}(x,y), x \bmod y : x, y \in G_n(a,b)\}.$$

(If $0 < a < b$, then $a - a = \mathrm{qu}(a,b) = 0$, $\mathrm{qu}(a,a) = 1$, $a \bmod b = a$, so

$$G_1(a,b) = \{0, 1, a, b, 2a, 2b, a + b, a - b, b - a, \mathrm{qu}(b,a), b \bmod a\}.)$$

Date: October 2002.

We put

$$g(a,b) := \text{least } n \text{ such that } \gcd(a,b) \in G_n(a,b).$$

Thus $g(a,b)$ is the number of steps needed to get $\gcd(a,b)$ from a,b using addition, subtraction, and division with remainder, where in each step these operations are applied to all numbers obtained in earlier steps. The Euclidean algorithm shows that there is a positive constant $C > 0$ such that $g(a,b) \leq C \log \min(|a|,|b|)$ for all a,b. But $g(a,b)$ is often much smaller than the number of "remainder" steps taken by the Euclidean algorithm: for example, $1 \in G_1(a,b)$ (unless $a = b = 0$), hence $g(a,b) \leq 1$ whenever $\gcd(a,b) = 1$.

Our first result, in Section 2, is that the function g is *unbounded*. This is unsurprising, and was known, see the **Comment** below. The novelty is the method used in our proof: a simple model-theoretic construction enables us to focus on "integers with irrational ratio". Varying this construction opens the door to other results in this paper.

In Section 3 we obtain a triple logarithmic lower bound for the growth of the function g on suitable sequences. In Section 4 we strengthen the unboundedness of g in another way, by including multiplication in the generation process, and in Section 5 we obtain a quadruple logarithmic lower bound for the growth of the corresponding function $g^\times$.

In Section 6 we consider *primitive recursive* algorithms that use the arithmetic operations as givens. These algorithms are shown to be subject to severe limitations in efficiency. In combination with the unboundedness of g this yields a solution to a problem of Moschovakis [6] on primitive recursive algorithms that compute the gcd using arithmetic operations as givens.

The methods of this paper appear to be new in solving problems of this kind; they might be fruitful also in dealing with related issues.

I thank Yiannis Moschovakis for explaining his "Problem 1", and for email correspondence on the topics of this paper.

Comment. While this paper was being considered for publication Marek Karpinski kindly informed me of an article by Y. Mansour, B. Schieber and P. Tiwari, "A lower bound for integer greatest common divisor computations", Journal of the ACM **38** (1991), 453–571. Its results imply the boundedness of the functions g and $g^\times$ in Propositions 2.1 and 4.1 below. The methods used are quite different from ours and do not yield the parts of Propositions 2.1 and 2.4 that involve irrationality and transcendence, as needed in Section 6 below. The article cited also implies a quadruple logarithmic lower bound for the function $g^\times$ on some sequence, but does not lend itself to an explicit definition of such a sequence as in Section 5 below.

2. Unboundedness and Irrationality

The table below gives an impression of the slowness of the growth of g. It lists the lexicographically smallest pairs (a, b) in the ranges indicated with g-values $0, 1, 2, 3, 4$. For g-values 3 and 4 these pairs were found by Victor DeLorenzo using a computer search. This search showed also that $g(a, b) \leq 4$ for all a, b with $1 \leq a, b \leq 20,000$.

$g(a,b)$	(a,b)	range	$\gcd(a,b)$
0	(1, 1)	$a, b \geq 1$	1
1	(2, 3)	$a, b \geq 1$	1
2	(6, 10)	$a, b \geq 1$	2
3	(21, 225)	$1 \leq a, b \leq 10^8$	3
4	(1044,1812)	$1 \leq a, b \leq 20,000$	12

Proposition 2.1. *The function g is unbounded. More precisely, if (a_n) and (b_n) are sequences of positive integers such that $a_n/b_n \to r$ as $n \to \infty$, where r is irrational, then $g(n!a_n, n!b_n) \to \infty$ as $n \to \infty$.*

The multipliers $n!$ cannot be omitted: it may happen that $\gcd(a_n, b_n) = 1$ for all n, in which case also $g(a_n, b_n) \leq 1$ for all n. The irrationality of r in this proposition is essential: if $r = a/b$ where a, b are positive integers, then the set $\{g(\kappa a, \kappa b) : \kappa \in \mathbf{Z}\}$ is bounded.

Proof. We prove the more precise statement. Let ${}^*\mathbf{Z}$ be an $\aleph_1$-saturated elementary extension of the ring of integers $\mathbf{Z}$, let ${}^*\mathbf{Q}$ be the ordered fraction field of ${}^*\mathbf{Z}$. (Those unfamiliar with these notions but acquainted with ultraproducts can take for ${}^*\mathbf{Z}$ an ultrapower of the ring $\mathbf{Z}$ with respect to a non-principal ultrafilter on some index set.) The binary operations gcd, qu and mod on $\mathbf{Z}$ are definable in the ring $\mathbf{Z}$, and thus extend naturally to binary operations on ${}^*\mathbf{Z}$; we shall use the same notations gcd, qu and mod for these extended operations.

Let $r > 0$ be an irrational real number, and let $\alpha, \beta \in {}^*\mathbf{Z}$ be such that α and β are positive multiples (in ${}^*\mathbf{Z}$) of each positive integer, and $\alpha/\beta \in {}^*\mathbf{Q}$ realizes the irrational cut in $\mathbf{Q}$ given by r. The latter simply means that for all $m, n > 0$ we have $m/n < r \iff m/n < \alpha/\beta$. (Think of α and β as $N!a_N$ and $N!b_N$ with infinite N.) The proposition will follow if under these assumptions we can always find a set $A \subseteq {}^*\mathbf{Z}$ that contains α and β, is closed under the binary operations $+$, $-$, qu and mod, but does not contain $\gcd(\alpha, \beta)$. Put $A := \mathbf{Z} + \mathbf{Q}\alpha + \mathbf{Q}\beta \subseteq {}^*\mathbf{Z}$; we claim that this set A has the properties listed in the previous sentence.

It is obvious that A contains α and β and is closed under addition and subtraction. Next we show that A is closed under qu. First note that the ordered additive subgroup $\mathbf{Q}\alpha + \mathbf{Q}\beta$ of ${}^*\mathbf{Z}$ embeds into the ordered additive group of real numbers by sending α to r and β to 1, and that each positive

element of $\mathbf{Q}\alpha+\mathbf{Q}\beta$ is $>\mathbf{N}$. Let $x,y\in A$, $x,y>0$; if $y>\mathbf{N}$, then $ny>x$ for some $n>0$, so $\mathrm{qu}(x,y)\in\mathbf{N}\subseteq A$; if $y\in\mathbf{N}$, we write $x=x_0+q_1\alpha+q_2\beta$ with $x_0\in\mathbf{Z}$ and $q_1,q_2\in\mathbf{Q}$, and then $\mathrm{qu}(x,y)=\mathrm{qu}(x_0,y)+(q_1/y)\alpha+(q_2/y)\beta\in A$. Thus A is closed under qu. Using the identity $x=\mathrm{qu}(x,y)y+x \bmod y$, this argument also shows that A is closed under mod.

It remains to show that $\gcd(\alpha,\beta)\notin A$. Since α,β are multiples of each positive integer we have $\gcd(\alpha,\beta)>\mathbf{N}$, and using the archimedean nature of $\mathbf{Q}\alpha+\mathbf{Q}\beta$ it is easy to check that no element $k+s$ with $k\in\mathbf{Z}$ and $0<s\in\mathbf{Q}\alpha+\mathbf{Q}\beta$ can be a common divisor (in ${}^*\mathbf{Z}$) of α and β. (In fact, the usual euclidean algorithm applied to α and β cannot terminate in a finite number of steps since r is irrational; hence $\gcd(\alpha,\beta)<\beta/n$ for all $n>0$.) □

Let us isolate and generalize the key facts about A used in this proof:

Let B be a divisible subgroup of the additive group of ${}^*\mathbf{Z}$, and suppose B is archimedean, that is, whenever $b,c\in B^{>0}$, then $nb>c$ for some n. Then the subgroup $\mathbf{Z}+B$ of ${}^*\mathbf{Z}$ is closed under qu and mod.

Suppose the positive real numbers $1=r_0,r_1,\dots,r_k$ are linearly independent over $\mathbf{Q}$. Let $a_0,a_1,\dots,a_k\in{}^*\mathbf{Z}$ be positive infinite such that $\frac{a_i}{a_0}$ realizes the same cut in $\mathbf{Q}$ as r_i for $i=1,\dots,k$. Let $0<\nu\in{}^*\mathbf{N}$ be a multiple (in ${}^*\mathbf{Z}$) of every positive integer, put $\alpha_i:=\nu a_i$ for $i=0,\dots,k$, and put $B:=\mathbf{Q}\alpha_0+\cdots+\mathbf{Q}\alpha_k$. Then B satisfies the hypothesis of the last lemma: we have an isomorphism of ordered abelian groups $B\cong\mathbf{Q}r_0+\cdots+\mathbf{Q}r_k\subseteq\mathbf{R}$ sending $q_0\alpha_0+\cdots+q_k\alpha_k$ to $q_0r_0+\cdots+q_kr_k$ $(q_0,\dots,q_k\in\mathbf{Q})$.

3. A triple logarithmic lower bound

Our goal in this section is to prove the following *lower bound* on the growth of the function g. We let $\lg x:=\log_2 x$ be the base 2 logarithm of the positive real number x.

Theorem 3.1. *There are sequences (α_n) and (β_n) of positive integers, both strictly increasing, such that $\frac{\alpha_n}{\beta_n}\to\sqrt{2}$ as $n\to\infty$ and*

$$g(\alpha_n,\beta_n)\geq\frac{1}{3}lg\ lg\ lg\ \beta_n$$

for all sufficiently large n.

The constant $\frac{1}{3}$ can be improved, but it would be more interesting to replace the triple logarithmic bound by a double logarithmic bound.

Specific sequences with these properties are obtained as follows. Let (a_n,b_n) for $n\geq 1$ be the nth positive integer solution of the Pell equation $x^2-2y^2=1$, so $(a_1,b_1)=(3,2)$, $(a_2,b_2)=(17,12)$, and so on. Next, put $\kappa_n=\lfloor\sqrt{\lg\ b_n}\rfloor!$ and let $(\alpha_n,\beta_n)=(\kappa_n a_n,\kappa_n b_n)$. Then the theorem holds for this choice of sequences (α_n) and (β_n).

The proof of the theorem is along the lines of that of Proposition 2.1, but with an added twist, as we shall see. The result of this section is not used later in this paper.

We construe $\mathbf{R}$ as the ordered field of real numbers equipped with $\mathbf{Z}$ as a distinguished subset, and with the exponential function exp. We take an $\aleph_1$-saturated elementary extension ${}^*\mathbf{R}$ of $\mathbf{R}$. The ordering $<$ on $\mathbf{R}$ and the various operations definable in the structure $\mathbf{R}$—its ring operations, and the functions $\lfloor x \rfloor$ ($x \in \mathbf{R}$) and $\lg(x)$ ($x > 0$)—have natural extensions to ${}^*\mathbf{R}$, and we use the same symbols to denote these extensions. We let ${}^*\mathbf{Z}$ be the distinguished subring of ${}^*\mathbf{R}$ that corresponds to the distinguished subring $\mathbf{Z}$ of $\mathbf{R}$, so for each $x \in {}^*\mathbf{R}$ we have $\lfloor x \rfloor \in {}^*\mathbf{Z}$ and $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. We take the ordered fraction field ${}^*\mathbf{Q}$ of ${}^*\mathbf{Z}$ inside the ordered field ${}^*\mathbf{R}$. For $x, y \in {}^*\mathbf{R}$ we write $x = o(y)$ to indicate that $|x| \leq \epsilon |y|$ for some positive infinitesimal $\epsilon \in {}^*\mathbf{R}$, and $x = O(y)$ to indicate that $|x| \leq C|y|$ for some positive $C \in \mathbf{R}$.

Let $a, b \in {}^*\mathbf{Z}$ be positive infinite with $a^2 - 2b^2 = 1$. Then $\frac{a}{b} - \sqrt{2} = \frac{1}{ab + b^2\sqrt{2}} < \frac{1}{b^2}$. Actually, the three lemmas that follow hold under the weaker assumptions that $a, b \in {}^*\mathbf{Z}$ are positive infinite, and $\frac{a}{b} - \sqrt{2} = O(\frac{1}{\sqrt{b}})$. The proof of Liouville's theorem on approximating algebraic numbers by rationals shows that there are no (m, n) with $n > 0$ and $|\frac{m}{n} - \sqrt{2}| < \frac{1}{5n^2}$, see for example [5]. This leads to:

Lemma 3.2. *Let $x, y, z \in {}^*\mathbf{Z}$, with $x + ya + zb = 0$, $x = O(b^{1/2})$ and $y = o(b^{1/4})$. Then $x = y = z = 0$.*

Proof. Suppose x, y, z are not all zero. It follows that $y \neq 0$. Dividing by yb gives

$$\frac{x}{yb} + \frac{a}{b} + \frac{z}{y} = \frac{x}{yb} + \big(\frac{a}{b} - \sqrt{2}\big) + \big(\frac{z}{y} + \sqrt{2}\big) = 0.$$

Since $\frac{x}{yb} = O(\frac{1}{\sqrt{b}})$, this gives $\frac{z}{y} + \sqrt{2} = O(\frac{1}{\sqrt{b}})$. In view of $y = o(b^{1/4})$, we obtain $\frac{z}{y} + \sqrt{2} = o(\frac{1}{y^2})$, a contradiction. □

Let $Z := \{x \in {}^*\mathbf{Z} : |x| < b^{1/n} \text{ for all } n > 0\}$, a convex subring of ${}^*\mathbf{Z}$. Let $Q := \mathrm{Frac}(Z)$, an ordered subfield of ${}^*\mathbf{Q}$. The idea is to let Z and Q take over the role of $\mathbf{Z}$ and $\mathbf{Q}$ in the proof of Proposition 2.1. The considerations that follow give substance to this idea.

The lemma above implies that $1, a, b$ are linearly independent over Q. Note that Z is cofinal in Q, so $\frac{1}{b}$ and $\frac{a}{b} - \sqrt{2}$ are Q-infinitesimal. Note also that Q is cofinal in the ordered subfield $Q(\sqrt{2})$ of ${}^*\mathbf{R}$. It follows in particular that $\lfloor f \rfloor \in Z$ for $f \in Q(\sqrt{2})$. These facts are now used to prove the next lemma.

Lemma 3.3. *The set Q is convex in $Q + Qa + Qb$. The map*

$$ya + zb \mapsto y\sqrt{2} + z : Qa + Qb \to Q(\sqrt{2}), \qquad (y, z \in Q)$$

is an isomorphism of ordered abelian groups. If $f_1, f_2 \in Q + Qa + Qb$ and $f_2 \notin Q$, then $\lfloor f_1/f_2 \rfloor \in Z$.

Proof. Let $c = x + ya + zb$ with $x, y, z \in Q$, so

$$\frac{c}{b} = \frac{x}{b} + y\frac{a}{b} + z = \frac{x}{b} + y\big(\frac{a}{b} - \sqrt{2}\big) + y\sqrt{2} + z = \epsilon + y\sqrt{2} + z,$$

where the first term $\epsilon := \frac{x}{b} + y(\frac{a}{b} - \sqrt{2})$ is Q-infinitesimal, and the last part $y\sqrt{2} + z$ is not Q-infinitesimal unless $y = z = 0$. The first two claims of the lemma follow easily.

Consider two elements $f_1 = x_1 + y_1a + z_1b$ and $f_2 = x_2 + y_2a + z_2b$ of $Q + Qa + Qb$ with $x_i, y_i, z_i \in Q$, and $f_2 \notin Q$, that is, y_2 and z_2 are not both 0. Decomposing f_1/b and f_2/b as above into an Q-infinitesimal part and a non-Q-infinitesimal part, we obtain

$$\frac{f_1}{f_2} = \frac{x_1 + y_1a + z_1b}{x_2 + y_2a + z_2b} = \frac{\epsilon_1 + y_1\sqrt{2} + z_1}{\epsilon_2 + y_2\sqrt{2} + z_2} = \epsilon_3 + y_3\sqrt{2} + z_3,$$

where $\epsilon_1, \epsilon_2, \epsilon_3$ are Q-infinitesimal, and $y_3 = \frac{y_2z_1 - y_1z_2}{2y_2^2 - z_2^2}$ and $z_3 = \frac{2y_1y_2 - z_1z_2}{2y_2^2 - z_2^2}$. Hence $\lfloor \frac{f_1}{f_2} \rfloor \in Z$. □

Let $\kappa := \lfloor s \rfloor!$ where $s = \sqrt{\lg b}$. Then $\kappa \in Z$: we have $\kappa < s^s$, so

$$\lg \kappa < s \lg s = (1/2)\sqrt{\lg b} \lg \lg b < (1/n) \lg b = \lg b^{1/n}$$

for all $n > 0$. The reason for taking here the square root of $\lg b$ instead of $\lg b$ itself is that $\lfloor \lg b \rfloor! > Z$.

We put $\alpha := \kappa a$ and $\beta = \kappa b$. Let $d \in {}^*\mathbf{R}$, $d \geq 2$, and put

$$A(d) := \{x + \frac{\eta}{\lambda}\alpha + \frac{\zeta}{\lambda}\beta : x, \eta, \zeta, \lambda \in {}^*\mathbf{Z}, \lambda \neq 0, |x|, |\eta|, |\zeta|, |\lambda| \leq d\}.$$

Note that if $d \leq s$, then $A(d) \subseteq Z + Za + Zb \subseteq {}^*\mathbf{Z}$.

Lemma 3.4. *Let $2 \leq d < d^2 \leq s$, and $f_1, f_2 \in A(d)$. Then $f_1 + f_2$, $f_1 - f_2$, $qu(f_1, f_2)$, and $f_1 \bmod f_2$ lie in $A(d^8)$.*

Proof. Write $f_1 = x_1 + y_1\alpha + z_1\beta$ and $f_2 = x_2 + y_2\alpha + z_2\beta$ where for $i = 1, 2$ we have $x_i \in {}^*\mathbf{Z}$, $y_i = \frac{\eta_i}{\lambda_i}$, $z_i = \frac{\zeta_i}{\lambda_i}$ with $\eta_i, \zeta_i, \lambda_i \in {}^*\mathbf{Z}$, $\lambda_i > 0$, and $|x_i|, |\eta_i|, |\zeta_i|, |\lambda_i| \leq d$.

Suppose first that $f_2 \notin Z$. Then $f_2 \notin Q$, so

$$\frac{f_1}{f_2} = \epsilon + \frac{\lambda_2}{\lambda_1}\big(\frac{(\eta_2\zeta_1 - \eta_1\zeta_2)\sqrt{2} + (2\eta_1\eta_2 - \zeta_1\zeta_2)}{2\eta_2^2 - \zeta_2^2}\big)$$

for some Q-infinitesimal ϵ. Hence

$$\begin{aligned} |\mathrm{qu}(f_1, f_2)| &\leq |\lambda_2|\big(|\eta_2\zeta_1 - \eta_1\zeta_2|\sqrt{2} + |2\eta_1\eta_2 - \zeta_1\zeta_2|\big) + 1 \\ &\leq d(2\sqrt{2} + 3)d^2 + 1 \leq 6d^3. \end{aligned}$$

Therefore

$$f_1 \bmod f_2 = f_1 - \mathrm{qu}(f_1, f_2)f_2 = x_3 + y_3\alpha + z_3\beta, \text{ with}$$
$$x_3 = x_1 - \mathrm{qu}(f_1, f_2)x_2$$
$$y_3 = y_1 - \mathrm{qu}(f_1, f_2)y_2 = \frac{\lambda_2\eta_1 - \mathrm{qu}(f_1, f_2)\lambda_1\eta_2}{\lambda_1\lambda_2}$$
$$z_3 = z_1 - \mathrm{qu}(f_1, f_2)z_2 = \frac{\lambda_2\zeta_1 - \mathrm{qu}(f_1, f_2)\lambda_1\zeta_2}{\lambda_1\lambda_2}.$$

Hence $|x_3| \leq d + 6d^4 \leq d^8$, and the numerators and denominators of y_3 and z_3 in the expressions on the right are in absolute value at most $d^2 + 6d^5 \leq d^8$. Thus $\mathrm{qu}(f_1, f_2)$ and $f_1 \bmod f_2$ belong to $A(d^8)$.

Next, assume $0 \neq f_2 \in Z$, so $y_2 = z_2 = 0$ and $f_2 = x_2$. Then

$$\frac{f_1}{f_2} = \frac{x_1}{x_2} + \frac{\eta_1}{\lambda_1 x_2}\alpha + \frac{\zeta_1}{\lambda_1 x_2}\beta$$

and we note that $|\lambda_1 x_2| \leq d^2 \leq s$, so $\frac{\eta_1}{\lambda_1 x_2}\alpha + \frac{\zeta_1}{\lambda_1 x_2}\beta$ lies in ${}^*\mathbf{Z}$. Hence

$$\mathrm{qu}(f_1, f_2) = \mathrm{qu}(x_1, x_2) + \frac{\eta_1}{\lambda_1 x_2}\alpha + \frac{\zeta_1}{\lambda_1 x_2}\beta.$$

In view of $|\mathrm{qu}(x_1, x_2)| \leq |x_1|$ this yields $\mathrm{qu}(f_1, f_2) \in A(d^2) \subseteq A(d^8)$. Also, $f_1 \bmod f_2 = x_1 - \mathrm{qu}(x_1, x_2)x_2$, hence $f_1 \bmod f_2$ lies in $A(d^8)$. □

For simplicity of notation we stated the lemma with the exponent 8, but its proof shows that this lemma remains valid with $\tau := 7.9$ instead of 8; we shall use this smaller exponent below. Note that $G_0(\alpha, \beta) = \{\alpha, \beta\} \subseteq A(2)$. The last lemma with τ instead of 8 implies by induction on ν that for $\nu \in {}^*\mathbf{N}$ with $2^{\tau^\nu} \leq s$ we have

$$G_\nu(\alpha, \beta) \subseteq A(2^{\tau^\nu}) \subseteq A(s).$$

Recall in this connection that $A(s) \subseteq Z + Za + Zb \subseteq {}^*\mathbf{Z}$.

Proof of 3.1. It suffices to show that

$$g(\alpha, \beta) \geq \frac{1}{3}\lg\lg\lg\beta.$$

From $a^2 - 2b^2 = 1$ we get $\gcd(a, b) = 1$, hence $\gcd(\alpha, \beta) = \kappa$. In combination with the linear independence of $1, a, b$ over Z and the definition and properties of $A(s)$ this gives $\gcd(\alpha, \beta) \notin A(s)$.

Take $\nu \in {}^*\mathbf{N}$ with $\frac{1}{3}\lg\lg\lg\beta \leq \nu \leq 1 + \frac{1}{3}\lg\lg\lg\beta$. ¿From $\beta \leq b^2$ we obtain $\lg\beta \leq 2\lg b = 2s^2$, so $\lg\lg\beta \leq 1 + 2\lg s \leq 3\lg s$, hence $\lg\lg\lg\beta \leq \lg 3 + \lg\lg s$. Using $\lg\tau < 3$ this gives

$$\lg\tau^\nu = \nu\lg\tau \leq (1 + \frac{1}{3}\lg\lg\lg\beta)\lg\tau$$
$$\leq (1 + \frac{1}{3}\lg 3 + \frac{1}{3}\lg\lg s)\lg\tau < \lg\lg s.$$

Therefore $2^{\tau^\nu} \leq s$, hence $G_\nu(\alpha,\beta) \subseteq A(s)$. In view of $\gcd(\alpha,\beta) \notin A(s)$, this yields $g(\alpha,\beta) > \nu \geq \frac{1}{3}\lg\lg\lg\beta$, as desired.

Remarks. One can use other values of s and κ, and variants of the lemmas above, but this doesn't seem to lead to any substantial improvement of the triple logarithmic lower bound. Lemma 3.4 is a bottleneck in this regard.

Theorem 3.1 might be relevant in proving lower bounds on the complexity of algorithms that compute the gcd. I don't mean specific algorithms like the Euclidean algorithm, where good lower bounds are well-known, but all algorithms from some large class, for example, all primitive recursive algorithms using arithmetic operations as givens. Section 6 shows that, compared to the Euclidean algorithm, this particular class contains only highly inefficient algorithms for computing the gcd; see also [6]. A natural question is to obtain non-trivial lower bounds for similarly large classes of algorithms that *do* include the Euclidean algorithm.

4. Allowing multiplication as a generating operation

Define the sequence $(G_n^\times(a,b))$ in the same way as $(G_n(a,b))$, except that $G_{n+1}^\times(a,b)$ contains also all products xy with $x,y \in G_n^\times(a,b)$. Put

$$g^\times(a,b) := \text{least } n \text{ such that } \gcd(a,b) \in G_n^\times(a,b).$$

We have a crude upperbound: $g^\times(a,b) \leq 4 + 2\lg\lg\min(a,b)$ for $a,b > 1$. To see this, note that $0,1,2 \in G_2^\times(a,b)$; next, if $\{0,1,\ldots,k\} \subseteq G_n^\times(a,b)$, then $\{0,1,\ldots,k^2\} \subseteq G_{n+2}^\times(a,b)$. So $\{0,1,2,\ldots,2^{2^n}\} \subseteq G_{2+2n}$, by induction on n. Now use that the least n such that $2^{2^n} \geq \min(a,b)$ is $\leq 1 + \lg\lg\min(a,b)$.

The lexicographically least pair of positive integers $\leq 20,000$ at which $g^\times$ takes the value 4 is $(7786, 13668)$, according to DeLorenzo.

We have the following analogue of Proposition 2.1.

Proposition 4.1. *The function $g^\times$ is unbounded. If (a_n) and (b_n) are sequences of positive integers, and $a_n/b_n \to r$ as $n \to \infty$, with transcendental r, then there are integers $\kappa_n > 0$ such that $g^\times(\kappa_n a_n, \kappa_n b_n) \to \infty$ as $n \to \infty$.*

Unlike the situation of Proposition 2.1 it is not clear that κ_n can be chosen to depend only on n.

Proof. Let $a,b \in {}^*\mathbf{Z}$ be positive infinite such that $t := a/b \in {}^*\mathbf{Q}$ realizes the cut in $\mathbf{Q}$ defined by the transcendental number r. Put $K := \mathbf{Q}(t)$, an ordered subfield of ${}^*\mathbf{Q}$ isomorphic to the ordered subfield $\mathbf{Q}(r)$ of $\mathbf{R}$; in particular, K is archimedean. Take positive infinite $\kappa \in {}^*\mathbf{Z}$ such that $p(a,b)|\kappa$ for all non-zero homogeneous polynomials $p(X,Y) \in \mathbf{Z}[X,Y]$. Put $\alpha := \kappa a$, $\beta := \kappa b$, so $\alpha = t\beta$. In analogy with the proof of proposition 2.1 it suffices to find a subring R of ${}^*\mathbf{Z}$ that contains α and β, is closed under the binary operations qu and mod, and does not contain $\gcd(\alpha,\beta)$. Put

$$R := \{f(\beta) : f(U) \in K[U], f(0) \in \mathbf{Z}\} \subseteq {}^*\mathbf{Q}.$$

We claim that R has the desired properties. It is clear that R is a subring of ${}^*\mathbf{Q}$ containing α and β. We show first that $R \subseteq {}^*\mathbf{Z}$. Let $f(\beta) \in R$, where

$$f(U) = c_0 + c_1 U + \cdots + c_m U^m \in K[U], \quad c_0 \in \mathbf{Z}.$$

For $i = 1, \ldots, m$ we write the coefficient $c_i \in K$ as $c_i = p_i(a,b)/p(a,b)$ with homogeneous $p_i(X,Y), p(X,Y) \in \mathbf{Z}[X,Y]$ and $p(X,Y) \neq 0$. Then $f(\beta) = c_0 + \sum_{i=1}^m c_i \beta^i$, and for $i = 1, \ldots, m$ we have $c_i \beta^i = \kappa^i b^i p_i(a,b)/p(a,b) \in {}^*\mathbf{Z}$ because $p(a,b) | \kappa$. Hence $f(\beta) \in {}^*\mathbf{Z}$.

To show that R is closed under qu, let $x, y \in R$ with $y > 0$. It suffices to show that then $\mathrm{qu}(x,y) \in R$. If $|x| \leq ky$ with $k \in \mathbf{N}$, then $-k \leq \mathrm{qu}(x,y) \leq k$, so $\mathrm{qu}(x,y) \in \mathbf{Z} \subseteq R$. So we can assume that $|x| > ky$ for all $k \in \mathbf{N}$. Write $x = f(\beta)$ with $f(U) \in K[U]$ of degree m, and $y = g(\beta)$ with $g(U) \in K[U]$ of degree n. Note that then $m > n$. Let $f(U)$ have leading coefficient c and $g(U)$ have leading coefficient $d > 0$. Then we have $f(U) = (c/d)U^{m-n} g(U) + h(U)$ where $h(U) \in K[U]$ has degree lower than m, and $h(0) = f(0) \in \mathbf{Z}$. Hence $z := h(\beta) \in R$; because of the lower degree of h we may assume inductively that $\mathrm{qu}(z,y) \in R$. Using $\mathrm{qu}(x,y) = (c/d)\beta^{m-n} + \mathrm{qu}(z,y)$ it follows that $\mathrm{qu}(x,y) \in R$. As the ring R is closed under qu, it is also closed under mod.

It remains to show that $\gcd(\alpha, \beta) \notin R$. Note that each positive infinite element of R is $> \beta/n$ for some $n > 0$. The argument at the end of the proof of proposition 2.1 shows that $n < \gcd(\alpha,\beta) < \beta/n$ for all $n > 0$. It follows that $\gcd(\alpha,\beta) \notin R$. □

The unboundedness of $g^\times$ is equivalent to the following result, which says, roughly, that gcd cannot be expressed explicitly in terms of the usual arithmetic operations, including division with remainder.

Corollary 4.2. *Let $t_1(x,y), \ldots, t_k(x,y)$ be finitely many terms built up from the formal variables x and y, the constant symbols 0 and 1, and the binary function symbols $+$, $-$, $\cdot$, qu and mod. (Such a term defines a function $\mathbf{Z}^2 \to \mathbf{Z}$ in the obvious way.) Then there are positive integers a and b such that $\gcd(a,b) \neq t_i(a,b)$ for $i = 1, \ldots, k$.*

5. A quadruple logarithmic lower bound

This section is more technical; readers primarily interested in the results on primitive recursive algorithms in section 6 can skip it.

Analogous to the triple logarithmic lower bound for g we derive here a quadruple logarithmic lower bound for $g^\times$ on a suitable sequence. To keep notations simple we write l_k for the k-times iterated (natural) logarithm function, where k is a positive integer, so $l_1(x) = \log x$, $l_2(x) = \log\log x$, and so on.

Put $b_n := n!$ and define $a_n \in \mathbf{N}$ by

$$\frac{a_n}{b_n} = \sum_{i=0}^{n} \frac{1}{i!}.$$

Define the multipliers κ_n by

$$\kappa_n := 1 \quad \text{for } n < 4, \quad \kappa_n := \lfloor b_n^{l_2(b_n)l_3(b_n)} \rfloor! \quad \text{for } n \geq 4.$$

Put $\alpha_n := \kappa_n a_n$ and $\beta_n := \kappa_n b_n$, so $\frac{\alpha_n}{\beta_n} = \frac{a_n}{b_n} \to e$ as $n \to \infty$.

Theorem 5.1. *For all sufficiently large n we have*

$$g^\times(\alpha_n, \beta_n) \geq \frac{1}{2}\sqrt[3]{l_4(\beta_n)}.$$

The proof is in the same spirit as that of Theorem 3.1: we elaborate the arguments of section 4 by computing explicit bounds. The key tool in obtaining these bounds is Cijsouw's transcendence measure [2] for e:

$$|p(e)| \geq \exp(-CN^2(N + \log H))$$

for each non-zero polynomial $p(T) \in \mathbf{Z}[T]$ of degree at most N and coefficients of absolute value at most H, where $N \in \mathbf{N}$ and $1 \leq H \in \mathbf{R}$, with a constant $C > 0$ that does not depend on (N, H). In the rest of this section C will have this value, and C_1, C_2, and so on, will denote additional absolute positive real constants, as needed.

We shall also use the following easy estimate:

Lemma 5.2. *$gcd(a_n, b_n) = o(b_n/\log b_n)$ as $n \to \infty$.*

Proof. Let $n > 1$. Then

$$b_n = n(n-1)b_{n-2}, \quad a_n = na_{n-1} + 1 = n(n-1)a_{n-2} + n + 1.$$

Hence $\gcd(a_n, n(n-1)) \leq 2$, and thus $\gcd(a_n, b_n) \leq \frac{2b_n}{n(n-1)}$. Now use that $\log b_n = \log n! < n \log n = o(n(n-1))$ as $n \to \infty$. □

We extend the model-theoretic setting of the previous section, by working inside a so-called non-standard universe; see [1] for details. As part of this universe we have $\aleph_1$-saturated elementary extensions ${}^*\mathbf{R}$, ${}^*\mathbf{Z}$ and ${}^*\mathbf{N}$ of the field $\mathbf{R}$, the ring $\mathbf{Z}$, and the semiring $\mathbf{N}$ (just as in previous sections) but also an $\aleph_1$-saturated elementary extension ${}^*(\mathbf{Z}[T])$ of the ring $\mathbf{Z}[T]$ of polynomials in the indeterminate T over $\mathbf{Z}$. (We use parentheses in ${}^*(\mathbf{Z}[T])$ to avoid confusion with the polynomial ring ${}^*\mathbf{Z}[T]$ over ${}^*\mathbf{Z}$.) The usual notions associated to polynomials such as "degree" and "coefficient" make sense also for $p(T) \in {}^*(\mathbf{Z}[T])$: its degree is an element of ${}^*\mathbf{N} \cup \{-\infty\}$, and its coefficients lie in ${}^*\mathbf{Z}$. Similarly, we can evaluate such a $p(T)$ at any $x \in {}^*\mathbf{R}$ to give a value $p(x) \in {}^*\mathbf{R}$. We also deal with larger non-standard polynomial rings such as ${}^*(\mathbf{Z}[X, Y])$ and ${}^*(\mathbf{Q}(T)[U])$ in a similar way. The usual operations in the standard universe have distinguished extensions in the non-standard universe, and these extensions are denoted by the same symbol (omitting a prefixed star) if the context makes confusion unlikely.

Throughout the rest of this section d, N, N_1, N_2 range over ${}^*\mathbf{N}$, and H, H_1, H_2 over ${}^*\mathbf{R}$, subject to $d, H, H_1, H_2 \geq 1$. We put

$$\mathcal{A}(N,H) := \{p(T) \in {}^*(\mathbf{Z}[T]) : \quad p \text{ has degree at most } N \text{ and its coefficients are all of absolute value } \leq H\}.$$

Lemma 5.3.

(1) $\mathcal{A}(N_1,H_1) + \mathcal{A}(N_2,H_2) \subseteq \mathcal{A}\big(\max(N_1,N_2), H_1+H_2\big)$,
(2) $\mathcal{A}(N_1,H_1) \cdot \mathcal{A}(N_2,H_2) \subseteq \mathcal{A}\big(N_1+N_2, (\min(N_1,N_2)+1)H_1H_2\big)$,
(3) *if* $g \in \mathcal{A}(N,H)$, *then* $g^k \in \mathcal{A}(kN, (N+1)^{k-1}H^k)$ *for positive* $k \in {}^*\mathbf{N}$,
(4) $\mathcal{A}(N,H) + \mathcal{A}(N,H) \subseteq \mathcal{A}(N,2H)$,
(5) $\mathcal{A}(N,H) \cdot \mathcal{A}(N,H) \subseteq \mathcal{A}(2N, (N+1)H^2)$.

Note that (3) follows from (2) by induction on k, and that (4) and (5) are special cases of (1) and (2).

Let $M \in {}^*\mathbf{Z}$, $M > \mathbf{N}$, put $b := b_M = M!$ and let $a := a_M$ be the positive infinite element of ${}^*\mathbf{Z}$ such that

$$t := \frac{a}{b} = \sum_{i=0}^{M} \frac{1}{i!}.$$

Note that then $|t - e| = o(\frac{1}{b})$.

Lemma 5.4. *Let* $p(T) \in \mathcal{A}(N,H)$ *such that* $p(T) \neq 0$, $N = O(l_2(b))$ *and* $\log H = O(l_2(b))$. *Then* $|p(t)| \geq \exp(-C_1N^2(N + \log H))$.

Proof. Write $p(T) = c_0 + c_1T + \cdots + c_NT^N \in {}^*(\mathbf{Z}[T])$ with all $|c_i| \leq H$. For $i = 1, \ldots, N$ we have $|t^i - e^i| = |(t-e)\sum_{j=1}^{i} t^{j-1}e^{i-j}| \leq |t-e|N3^N$. Hence $|p(t) - p(e)| \leq \sum_{i=1}^{N} |c_i(t^i - e^i)| \leq |t-e|HN^2 3^N = o(\frac{HN^2 3^N}{b})$. By the transcendence measure from [2] we have $|p(e)| \geq \exp(-CN^2(N + \log H))$. So it suffices to show that

$$\exp(-CN^2(N + \log H)) > HN^2 3^N / b.$$

This inequality reduces to

$$-CN^2(N + \log H) > \log H + N \log 3 + 2 \log N - \log b,$$

equivalently, $\log b > \log H(CN^2 + 1) + CN^3 + N \log 3 + 2 \log N$. This last inequality is clearly satisfied under the assumptions of the lemma. □

The proof shows that for the absolute real constant C_1 we can take any real number $> C$. *Below we assume* $C_1 \geq 2$.

The role of $\mathbf{Z}$ in the proof of 4.1 will be taken over in this section by

$$Z := \{x \in {}^*\mathbf{Z} : |x| < (\log b)^n \text{ for some } n\}.$$

We also put

$$s := b^{l_2(b)l_3(b)}, \quad \kappa := \lfloor s \rfloor!$$
$$\alpha := \kappa a, \qquad \beta := \kappa b.$$

Thus $\kappa \in {}^*\mathbf{Z}$. For later use we note

$$\kappa \leq s^s = \exp(s \log s) \leq \exp(b^{1+l_2(b)l_3(b)}) \leq \exp(b^{\log b}).$$

The positive infinite $M \in {}^*\mathbf{Z}$ with $b = M!$ is arbitrary, so Theorem 5.1 will follow if we manage to show that $g^\times(\alpha, \beta) \geq \frac{1}{2}\sqrt[3]{l_4(\beta)}$.

Lemma 5.5. *Let $p(X, Y) \in {}^*(\mathbf{Z}[X, Y])$ be non-zero and homogeneous of total degree $O(l_2(b))$ with coefficients in Z. Then $p(a, b)|\kappa$.*

Proof. Take $n > 0$ such that p has total degree $< nl_2(b)$, and all its coefficients have absolute value at most $(\log b)^n$. Using $a \leq 3b$ this gives

$$\begin{aligned} |p(a, b)| &\leq (nl_2(b)) \cdot (3b)^{nl_2(b)} \cdot (\log b)^n \\ &\leq b^{l_2(b)l_3(b)} = s. \end{aligned}$$

In order to conclude that $p(a, b)|\kappa$ it remains to show that $p(a, b) \neq 0$. Let p have total degree N. Then $p(a, b) = b^N q(t)$ where $0 \neq q(T) \in \mathcal{A}(N, H)$ with $H = (\log b)^n$. Now use that $q(t) \neq 0$ by Lemma 5.4. □

We let $\mathcal{B}(d, N, H)$ be the set of all $F = F(U) \in {}^*(\mathbf{Z}[T, U])$ of the form

$$F = f_d U^d + f_{d-1} U^{d-1} + \cdots + f_0$$

where all $f_i \in \mathcal{A}(N, H)$. For F as above we write $\deg F$ for its degree with respect to U, and we refer to $f_0, f_1, \ldots, f_d$ as the coefficients of F.

Let $F, G \in \mathcal{B}(d, N, H) \setminus \{0\}$, with $\deg F = \mu$ and $\deg G = \nu$, and write

$$\begin{aligned} F &= f_\mu U^\mu + f_{\mu-1} U^{\mu-1} + \cdots + f_0 \\ G &= g_\nu U^\nu + g_{\nu-1} U^{\nu-1} + \cdots + g_0 \end{aligned}$$

with all $f_i, g_j \in \mathcal{A}(N, H)$, $f_\mu, g_\nu \neq 0$.

Lemma 5.6. *Suppose $\mu \geq \nu$. Then there are $Q, R \in {}^*(\mathbf{Z}[T, U])$ such that*

$$\begin{aligned} g_\nu^{\mu-\nu} F &= QG + R, \quad \deg Q = \mu - \nu, \quad \deg R \leq \nu, \quad Q(T, 0) = 0, \\ Q &= \sum_{i=1}^{\mu-\nu} g_\nu^{\mu-\nu-i} q_i U^{\mu-\nu-i+1}, \quad R = \sum_{j=0}^{\nu} r_j T^j, \\ q_i &\in \mathcal{A}\big(iN, 2^{i-1}(N+1)^{i-1} H^i\big), \quad i = 1, \ldots, \mu - \nu, \\ r_j &\in \mathcal{A}\big((d+1)N, 2^d (N+1)^d H^{d+1}\big), \quad j = 0, \ldots, \nu. \end{aligned}$$

All coefficients of Q lie in $\mathcal{A}(dN, d2^{d-1}(N+1)^{d-1} H^d)$.

This lemma follows by an incomplete "long division". (The last step in ordinary long division is not carried out, because we want $Q(T, 0) = 0$.) The assertions about the q_is and r_js follow by applying Lemma 5.3. The assertion about the coefficients of Q requires further applications of Lemma 5.3, using also $\mu, \nu \leq d$. The extreme case $\mu = d, \nu = 0$ is best considered separately; in this case we have $Q = F g_0^{d-1} - F(T, 0) g_0^{d-1}$, $G = g_0$ and $R = F(T, 0) g_0^d$.

Next, let $\mathcal{B}'(d,N,H)$ be the set of all $f = f(U) \in {}^*(\mathbf{Q}(T)[U])$ of the form

$$f = \frac{f_d U^d + \cdots + f_1 U}{\phi} + \phi_0$$

where $\phi_0 \in {}^*\mathbf{Z}$ with $|\phi_0| \leq H$, $f_1, \ldots, f_d, \phi \in \mathcal{A}(N,H)$ with $\phi \neq 0$. An easy computation using Lemma 5.3 gives:

Lemma 5.7.

$$\mathcal{B}'(d,N,H) + \mathcal{B}'(d,N,H) \subseteq \mathcal{B}'(d,2N,2(N+1)H^2)$$
$$\mathcal{B}'(d,N,H) \cdot \mathcal{B}'(d,N,H) \subseteq \mathcal{B}'(2d,2N,(d+1)(N+1)H^3).$$

Let $f, g \in \mathcal{B}'(d,N,H) \setminus \{0\}$, with $\deg f = \mu$, $\deg g = \nu$, $\mu \geq \nu$, and write

$$f = \frac{f_\mu U^\mu + \cdots + f_1 U}{\phi} + \phi_0$$
$$g = \frac{g_\nu U^\nu + \cdots + g_1 U}{\chi} + \chi_0$$

with $\phi_0, \chi_0 \in {}^*\mathbf{Z}$, $|\phi_0|, |\chi_0| \leq H$, and $f_1, \ldots, f_\mu, \phi, g_1, \ldots, g_\nu, \chi \in \mathcal{A}(N,H)$, and $\phi, \chi \neq 0$. If $\nu = 0$ we take $\chi = 1$. Put $f_0 := \phi_0\phi$ and $g_0 := \chi_0\chi$, and

$$F := f_\mu U^\mu + \cdots + f_1 U + f_0$$
$$G := g_\nu U^\nu + \cdots + g_1 U + g_0,$$

so $f = F/\phi$ and $g = G/\chi$. The coefficients of F and G lie in $\mathcal{A}(N,H^2)$. We saw above that $g_\nu^{\mu-\nu}F = QG + R$ where $Q \in {}^*(\mathbf{Z}[T,U])$ is of degree $\mu - \nu$ in U, $Q(T,0) = 0$, and $R \in {}^*(\mathbf{Z}[T,U])$ has degree at most ν in U. By the identities above we have

$$\frac{f}{g} = \frac{\chi Q}{\phi g_\nu^{\mu-\nu}} + \frac{\chi R}{\phi g_\nu^{\mu-\nu} G}$$

in the fraction field of ${}^*(\mathbf{Z}[T,U])$. For later use we record some bounds.

Lemma 5.8.

(1) *The coefficients of χQ lie in $\mathcal{A}\big((d+1)N, d2^{d-1}(N+1)^d H^{2d+1}\big)$.*
(2) *The denominator $\phi g_\nu^{\mu-\nu}$ lies in $\mathcal{A}\big((d+1)N, (N+1)^d H^{d+1}\big)$.*
(3) *The coefficient of U^ν in χR lies in $\mathcal{A}\big((d+2)N, 2^d(N+1)^{d+1}H^{2d+3}\big)$.*
(4) *The coefficient of U^ν in $\phi g_\nu^{\mu-\nu}G$ is $\phi g_\nu^{\mu-\nu+1}$, which lies in*

$$\mathcal{A}\big((d+2)N, (N+1)^{d+1}H^{d+2}\big).$$

Proof. By Lemma 5.6 the coefficients of Q lie in $\mathcal{A}\big(dN, d2^{d-1}(N+1)^{d-1}H^{2d}\big)$. In combination with Lemma 5.3 this yields (1), and this lemma also yields (2). The coefficients of R lie in $\mathcal{A}\big((d+1)N, 2^d(N+1)^d H^{2(d+1)}\big)$ by Lemma 5.6, which gives (3). Item (4) follows from (2). □

For the rest of this section we assume:

$$1 \leq d = O(l_2(b)), \quad 1 \leq N = O(l_2(b)), \quad \log H = O(l_2(b)).$$

Then $\phi(t) \neq 0$ for non-zero $\phi \in \mathcal{A}(N,H)$, by Lemma 5.4.

Lemma 5.9. *Let $p(T), \phi(T) \in \mathcal{A}(N,H)$, $\phi(T) \neq 0$. Then $|\frac{p(t)}{\phi(t)}| \leq b$, hence $\frac{p(t)}{\phi(t)} = o(\beta^{1/n})$ for each $n > 0$. In addition, let $F(T,U) \in \mathcal{B}(d,N,H)$ have degree $\mu \geq 0$ in U, with $F = f_\mu U^\mu + \cdots + f_0$, all $f_i \in \mathcal{A}(N,H)$, and put $x := \frac{F(t,\beta)}{\phi(t)}$. Then there is an infinitesimal ϵ in ${}^*\mathbf{Q}$ such that*

$$x = \frac{f_\mu(t)}{\phi(t)}\beta^\mu(1+\epsilon).$$

Proof. We have $|p(t)| \leq H3^{N+1}$. By Lemma 5.4 we have

$$\frac{1}{|\phi(t)|} \leq \exp\big(C_1 N^2(N + \log H)\big).$$

Since $\log H + (N+1)\log 3 + C_1N^2(N+\log H) \leq \log b$, the first inequality of the lemma follows by taking logarithms. We have

$$x = \frac{f_\mu(t)}{\phi(t)}\beta^\mu\big(1 + \sum_{i=0}^{\mu-1}\frac{f_i(t)}{f_\mu(t)}\beta^{i-\mu}\big).$$

Now use the first inequality to obtain

$$|\sum_{i=0}^{\mu-1}\frac{f_i(t)}{f_\mu(t)}\beta^{i-\mu}| \leq \sum_{i=0}^{\mu-1}|\frac{f_i(t)}{f_\mu(t)}|\beta^{-1} \leq \frac{\mu b}{\beta} \leq \frac{d}{\kappa}.$$

This gives the second inequality. □

Put $R(d,N,H) := \{f(t,\beta) \in {}^*\mathbf{Q} : f(T,U) \in \mathcal{B}'(d,N,H)\}$. The set $R(d,N,H)$ is only defined for d, N and H subject to the restrictions above. These sets $R(d,N,H)$ replace the ring R used in the proof of Proposition 4.1.

Lemma 5.10. *The sets $R(d,N,H)$ have the following properties:*

(1) $\alpha, \beta \in R(1,1,1)$;
(2) $R(d,N,H) \subseteq {}^*\mathbf{Z}$;
(3) $C_1N^2(N+\log H) \leq \frac{1}{2}l_2(b) \Longrightarrow gcd(\alpha,\beta) \notin R(d,N,H)$.

Proof. For (1), use that $\alpha = t\beta$. For (2), write $f \in \mathcal{B}'(d,N,H)$ as $f = \frac{F}{\phi}$ with $F \in \mathcal{B}(d,N,H^2)$ and $0 \neq \phi \in \mathcal{A}(N,H)$. Then Lemma 5.5 and an argument as in the proof of Proposition 4.1 show that $f(t,\beta) = \frac{F(t,\beta)}{\phi(t)} \in {}^*\mathbf{Z}$.

For (3), suppose towards a contradiction that $C_1N^2(N+\log H) \leq \frac{1}{2}l_2(b)$ and $\gcd(\alpha,\beta) \in R(d,N,H)$. Write $\gcd(\alpha,\beta) = f(t,\beta)$ where $f = \frac{F}{\phi}$ as in the proof of (2). Let $F = F(T,U)$ have degree μ in U. If $\mu > 1$, then $|f(t,\beta)| > \beta$ by Lemma 5.9, and this contradicts $\gcd(\alpha,\beta) < \beta$. So either $\mu = 0$ or $\mu = 1$.

Suppose $\mu = 0$. Then $|f(t,\beta)| \leq H$, contradicting $H < \kappa \leq \gcd(\alpha,\beta)$.

Suppose $\mu = 1$. Then $\gcd(\alpha, \beta) = \frac{p(t)}{\phi(t)}\beta + \phi_0$ where $0 \neq p \in \mathcal{A}(N, H)$ and $\phi_0 \in {}^*\mathbf{Z}$ with $|\phi_0| \leq H$. Division by κ yields

$$\gcd(a, b) = \frac{p(t)}{\phi(t)}b + \frac{\phi_0}{\kappa}.$$

By Lemma 5.4 we have

$$\begin{aligned} |\frac{\phi(t)}{p(t)}| &\leq 3^{N+1} H \exp[C_1 N^2 (N + \log H)] \\ &= \exp[(N+1)\log 3 + \log H + C_1 N^2 (N + \log H)]. \end{aligned}$$

In view of $C_1 \geq 2$, the assumption $C_1 N^2 (N + \log H) \leq \frac{1}{2} l_2(b)$ yields

$$(N+1)\log 3 + \log H + C_1 N^2 (N + \log H) \leq l_2(b),$$

hence $|\frac{\phi(t)}{p(t)}| \leq \log b$. As $\frac{\phi_0}{\kappa}$ is infinitesimal, we obtain $|\frac{p(t)}{\phi(t)}b + \frac{\phi_0}{\kappa}| \geq \frac{b}{2 \log b}$. By Lemma 5.2 we have $\gcd(a, b) = o(b/\log b)$, a contradiction.

□

Lemma 5.11. *For some absolute positive real constant $c \geq 1$, if*

$$H' := \exp[c(d+2)^3 N^2 (N + \log H)] = O(\log b),$$

then $R(2d, 4(d+1)N, H')$ is defined, and for all $x, y \in R(d, N, H)$ the numbers $x + y$, $x - y$, xy, $qu(x, y)$, and $x \bmod y$ lie in $R(2d, 4(d+1)N, H')$.

Proof. Till further notice we assume about c only that $c \in \mathbf{R}$ and $c \geq 1$. We also assume $H' = O(\log b)$, where H' is defined as in the Lemma. Note that then $R(2d, 4(d+1)N, H')$ is defined.

Let $x, y \in R(d, N, H)$. We shall assume $x, y > 0$. (The other cases are easily reduced to this case.) Lemma 5.7 implies that $x + y$, $x - y$ and xy lie in $R(2d, 4(d+1)N, H')$.

To deal with $\mathrm{qu}(x, y)$ and $x \bmod y$ we write $x = f(t, \beta)$ and $y = g(t, \beta)$ where $f = f(T, U) \in \mathcal{B}'(d, N, H)$ has degree μ in U, and $g = g(T, U) \in \mathcal{B}'(d, N, H)$ has degree ν in U. If $\mu < \nu$, then x/y is infinitesimal by Lemma 5.9, so $x \bmod y = x$, and $\mathrm{qu}(x, y) = 0$, hence $\mathrm{qu}(x, y)$ and $x \bmod y$ lie in $R(2d, 4(d+1)N, H')$.

Suppose $\mu \geq \nu$. With the notations from just before Lemma 5.8, put $Q^* := \frac{\chi Q}{\phi g_\nu^{\mu-\nu}}$ and let $r_\nu(T)$ be the coefficient of U^ν in R. By that lemma we have $Q^* \in \mathcal{B}'\big(d, (d+1)N, d2^{d-1}(N+1)^d H^{2d+1}\big)$. Put $q := Q^*(t, \beta)$, so

$$\frac{x}{y} = q + \frac{\chi(t) R(t, \beta)}{\phi(t) g_\nu(t)^{\mu-\nu} G(t, \beta)}.$$

We assume from now on $c \geq 2$. Then

$$q \in R\big(d, (d+1)N, d2^{d-1}(N+1)^d H^{2d+1}\big) \subseteq R(d, (d+1)N, H').$$

We distinguish two cases.

Case 1. $r_\nu = 0$. Then χR has degree $< \nu$ in U and $\phi g_\nu^{\mu-\nu} G$ has degree ν in U. Applying the second part of Lemma 5.9 to the quantities $\chi(t) R(t, \beta)$

and $\phi(t)g_\nu(t)^{\mu-\nu}G(t,\beta)$ and taking into account Lemma 5.8 and the first part of Lemma 5.9 yields

$$\frac{x}{y} = q + \epsilon$$

for some infinitesimal $\epsilon \in {}^*\mathbf{Q}$. Hence $\mathrm{qu}(x,y) = q$ or $\mathrm{qu}(x,y) = q-1$. Since $d2^d(N+1)^d H^{2d+1} \le H'$, this gives

$$\mathrm{qu}(x,y) \in R\big(d,(d+1)N,d2^d(N+1)^d H^{2d+1}\big) \subseteq R(d,(d+1)N,H').$$

Thus by Lemma 5.7

$$\mathrm{qu}(x,y)y \in R\big(2d,2(d+1)N,(d+1)((d+1)N+1)d^3 2^{3d}(N+1)^{3d}H^{6d+3}\big),$$

where the right hand set is defined because $c \ge 2$. We shall use the weaker estimate

$$\mathrm{qu}(x,y)y \in R\big(2d,2(d+1)N,(d+1)^5 2^{3d}(N+1)^{3d+1}H^{6d+3}\big),$$

where the right hand set is defined because $c \ge 2$. Using again Lemma 5.7, the identity $x \bmod y = x - \mathrm{qu}(x,y)y$ then yields

$$x \bmod y \in R(2d,4(d+1)N,(d+1)^{11}2^{6d+2}(N+1)^{6d+3}H^{12d+6}\big),$$

where the right hand set is defined because $c \ge 2$ and

$$(d+1)^{11}2^{6d+2}(N+1)^{6d+3}H^{12d+6} \le \exp[2(d+2)^3N^2(N+\log H)].$$

Thus $\mathrm{qu}(x,y)$ and $x \bmod y$ lie in $R(2d,4(d+1)N,H')$.

Case 2. $r_\nu \ne 0$. Using Lemma 5.9 as in **Case 1** yields

$$\frac{x}{y} = q + \rho, \quad \rho := \frac{\chi(t)r_\nu(t)}{\phi(t)g_\nu(t)^{\mu-\nu+1}}(1+\epsilon)$$

for some infinitesimal $\epsilon \in {}^*\mathbf{Q}$. By Lemmas 5.4 and 5.8 we have

$$\begin{aligned}\frac{1}{|\phi(t)g_\nu(t)^{\mu-\nu+1}|} &\le \exp[C_1(d+2)^2N^2\{(d+2)N + \log\big((N+1)^{d+1}H^{d+2}\big)\}] \\ &\le \exp[2C_1(d+2)^3N^2(N+\log H)].\end{aligned}$$

By part (3) of Lemma 5.8, and $2 < t < 3$ we have

$$|\chi(t)r_\nu(t)| \le 2^{d+1}(N+1)^{d+1}H^{2d+3}3^{(d+2)N}.$$

Hence $||\lfloor\rho\rfloor|| \le |\rho|+1 \le \exp\big(C_2(d+2)^3N^2(N+\log H)\big)$ with $C_2 := 2C_1+1$. Using $\mathrm{qu}(x,y) = q + \lfloor\rho\rfloor$ this yields

$$\mathrm{qu}(x,y) \in R\big(d,(d+1)N,\exp[C_3(d+2)^3N^2(N+\log H)]\big),$$

with $C_3 := C_2 + 1$, and where we take $c \ge C_3$ to guarantee that the right hand set is defined. Hence by Lemma 5.7

$$\mathrm{qu}(x,y)y \in R\big(2d,2(d+1)N,(d+1)^2(N+1)\exp[3C_3(d+2)^3N^2(N+\log H)]\big),$$

where $c \ge 3C_3$. Using $x \bmod y = x - \mathrm{qu}(x,y)y$, Lemma 5.7 yields

$$x \bmod y \in R\big(2d,4(d+1)N,4(d+1)^5(N+1)^3\exp[C_4(d+2)^3N^2(N+\log H)]\big),$$

where $C_4 := 6C_3$ and $c \geq C_4 + 2$ in order that the right hand set is defined. Thus the lemma holds with $c := C_4 + 2$. □

Proof of Theorem 5.1. Let c be as in the last lemma. For $\nu \in {}^*\mathbf{N}$ we put

$$d_\nu := 2^\nu, \quad N_\nu := 2^{\nu^2+2\nu}, \quad H_\nu := \exp[c^{2\nu} 2^{6\nu^3}].$$

In particular, $d_0 = N_0 = H_0 = 1$. If $H_\nu = O(\log b)$, then clearly $N_\nu = O(l_2(b))$ and $d_\nu = O(l_2(b))$.

Suppose that $H_{\nu+1} = O(\log b)$. Then for all $x, y \in R(d_\nu, N_\nu, H_\nu)$ we have that $x + y$, $x - y$, xy, $\mathrm{qu}(x, y)$ and $x \bmod y$ lie in $R(d_{\nu+1}, N_{\nu+1}, H_{\nu+1})$. (To see this, we need only check by Lemma 5.11 that

$$N_{\nu+1} \geq 4(d_\nu + 1)N_\nu \text{ and } H_{\nu+1} \geq \exp[c(d_\nu + 2)^3 N_\nu^2 (N_\nu + \log H_\nu)],$$

which is straightforward.)

It follows by induction on ν that as long as we have $H_\nu \leq \log b$, then $G_\nu^\times(\alpha, \beta) \subseteq R(d_\nu, N_\nu, H_\nu)$. Hence, by Lemma 5.10:

$$\text{if } H_\nu \leq \log b \text{ and } C_1 N_\nu^2 (N_\nu + \log H_\nu) \leq \frac{1}{2} l_2(b), \text{ then } g^\times(\alpha, \beta) > \nu.$$

By taking logarithms twice, the inequality $H_\nu \leq \log b$ reduces to

$$(2 \log c)\nu + (6 \log 2)\nu^3 \leq l_3(b).$$

This last inequality holds whenever $\nu \leq (\frac{1}{2} + \epsilon)\sqrt[3]{l_3(b)}$, where ϵ is some (small) positive rational number. One also checks easily that the inequality $C_1 N_\nu^2 (N_\nu + \log H_\nu) \leq \frac{1}{2} l_2(b)$ is satisfied whenever $\nu \leq (\frac{1}{2} + \epsilon)\sqrt[3]{l_3(b)}$, where ϵ is a suitable positive rational number.

From the definition of β and the inequality on κ preceding Lemma 5.5 we obtain $l_4(\beta) < (1 + \delta) l_3(b)$ for each positive rational δ. In view of the previous paragraphs, this yields $g^\times(\alpha, \beta) \geq \frac{1}{2}\sqrt[3]{l_4(\beta)}$. This finishes the proof of Theorem 5.1, in view of a remark preceding Lemma 5.5.

6. Limitations of primitive recursive algorithms

We prove here a *linear* lower bound for the complexity of any primitive recursive algorithm that computes the *greatest common divisor function* using the arithmetic operations as givens; see Theorem 6.1. We include here division with remainder among the arithmetic operations. In particular, no such algorithm can match in efficiency the Euclidean algorithm, which takes at most a logarithmic number of steps using only the remainder function as given.

Following [3] we first introduce a formalism that allows efficient definitions of "primitive recursive algorithm", and of the notions that come with it.

In this section recursion is fundamental. Accordingly we take $\mathbf{N}$ as our basic domain of computation instead of $\mathbf{Z}$ in earlier sections. Addition and multiplication will be the usual binary operations on $\mathbf{N}$, and, by an abuse

of language, mod and qu will denote the restrictions of these functions to $\mathbf{N}^2$. An *n-ary function* is by definition a (total) function $\mathbf{N}^n \to \mathbf{N}$.

If g is an m-ary function, and $h_1, \ldots, h_m$ are n-ary functions, then the n-ary function $x \mapsto g(h_1(x), \ldots, h_m(x))$ is denoted by $g(h_1, \ldots, h_m)$.

Given an n-ary function g and an $(n+2)$-ary function h, then the $(n+1)$-ary function f given by

$$f(x, 0) = g(x), \quad x \in \mathbf{N}^n$$
$$f(x, t+1) = h(x, t, f(x, t)), \quad x \in \mathbf{N}^n, t \in \mathbf{N},$$

is said to be obtained by *primitive recursion from g and h*, and we write $R_n(g, h)$ for this function f.

For the rest of this section we let Φ be an arbitrary but fixed collection of n-ary functions, for various n. Specific such collections that play a role below are:

- $\Phi_0 := \{n\text{-ary functions definable in } (\mathbf{N}, +) : n = 0, 1, 2, \ldots\}$;
- $\Phi_1 := \Phi_0 \cup \{\mathrm{mod}\}$;
- $\Phi_2 := \Phi_0 \cup \{\mathrm{mod}, \mathrm{qu}\}$;
- $\Phi_3 := \Phi_0 \cup \{\mathrm{mod}, \mathrm{qu}, \mathrm{multiplication}\}$.

Among the functions in Φ_0 are the unary functions $\lfloor \frac{x}{2} \rfloor$, $\lfloor \frac{x}{3} \rfloor, \ldots$, and the binary functions $x+y$, $x \dot{-} y$, $\min(x, y)$. The functions in Φ_0 can be described alternatively as the "piecewise linear functions" of [6].

We now introduce formal expressions that specify algorithms to compute n-ary functions ($n = 0, 1, 2, \ldots$) using the functions in Φ as givens. The technical term for such an expression will be

n-ary primitive recursive combinator over Φ (or *n-ary* **prc** *over* Φ).

These combinators will be words on the alphabet with the following symbols:

(i) the two symbols O and S;
(ii) for each m and $i = 1, \ldots, m$ a symbol P_i^m;
(iii) for each $\phi \in \Phi$ an associated symbol, also written as ϕ;
(iv) for each m and n a symbol S_m^n, and for each n a symbol R_n.

We assume of course that O and S are distinct symbols, different from the symbols introduced in (ii), (iii) and (iv), that P_i^m and P_j^n are distinct symbols whenever $(i, m) \neq (j, n)$, and that each P_i^m is also different from the symbols in (iii) and (iv), and so on ...

Each n-ary **prc** g over Φ is a word on this alphabet, and has associated to it an n-ary function $\widehat{g}$. The definition is inductive:

(1) the word O of length 1 is a nullary **prc** over Φ, whose associated function takes the value 0;
(2) the word S of length 1 is a unary **prc** over Φ, with associated function $x \mapsto x + 1$;
(3) for $1 \leq i \leq m$ the word P_i^m of length 1 is an m-ary **prc** over Φ, with associated function $(x_1, \ldots, x_m) \mapsto x_i$;

(4) for each n-ary $\phi \in \Phi$ with associated symbol ϕ the word ϕ of length 1 is an n-ary **prc** over Φ, with associated function $\phi \in \Phi$;
(5) if g is an m-ary **prc** over Φ, and $h_1, \ldots, h_m$ are n-ary **prc**'s over Φ, then the word $S_n^m g h_1 \ldots h_m$ is an n-ary **prc** over Φ, with associated function $\widehat{g}(\widehat{h_1}, \ldots, \widehat{h_m})$;
(6) if g is an n-ary **prc** over Φ and h is an $(n+2)$-ary **prc** over Φ, then the word $R_n g h$ is an $(n+1)$-ary **prc** over Φ, with associated function $R_n(\widehat{g}, \widehat{h})$.

To simplify notation we write $f(x)$ instead of $\widehat{f}(x)$ for an n-ary **prc** f over Φ and $x \in \mathbf{N}^n$. We think of such a combinator as specifying an algorithm to compute its associated function.

An m-ary function is said to be a Φ-function if it is associated to an m-ary **prc** over Φ that contains no occurrences of symbols R_n. These Φ-functions will play a special role in what follows.

We now introduce a complexity measure that "assigns no cost to substitution but takes primitive recursion seriously" [6]. The definition here is in terms of the formalism of combinators; it leads to a notion of complexity that is equivalent to that in [6], Section 1.4.

For an n-ary **prc** f over Φ and $x \in \mathbf{N}^n$ the natural number $c(f, x)$ (the cost of computing the output at input x according to program f) is defined inductively as follows:

(1) $c(f, x) := 0$ for $f \in \{O, S\} \cup \{P_i^m : 1 \leq i \leq m\} \cup \{\phi : \phi \in \Phi\}$;
(2) let $f = S_n^m g h_1 \ldots h_m$ as in clause (5) above; then

$$c(f, x) := \max\{c(h_1, x), \ldots, c(h_m, x), c(g, y)\} \text{ with } y := (h_1(x), \ldots, h_m(x));$$

(3) let $f = R_n g h$ as in clause (6) above; then for $x \in \mathbf{N}^n$ we put

$$c(f, (x, 0)) := c(g, x),$$
$$c(f, (x, t+1)) := \max\{c(f, (x, t)) + 1, c(h, y)\} \text{ with } y = (x, t, f(x, t)).$$

If the m-ary **prc** f over Φ contains no symbols R_n, then clearly $c(f, x) = 0$ for all $x \in \mathbf{N}^m$. If $f = R_n g h$ as in (3), then $c(f, (x, t)) \geq t$ for all $(x, t) \in \mathbf{N}^{n+1}$.

The functions associated to **prc**'s over $\emptyset$ are exactly the primitive recursive functions. While this is a large class of functions, the algorithms embodied by such combinators suffer from severe limitations in efficiency, as shown by Colson [3]:

Let f be a binary **prc** *over $\emptyset$ such that $f(x, y) = \min(x, y)$ for all $x, y \in \mathbf{N}$. Then either $c(f, (1, 1000)) \geq 1000$, or $c(f, (1000, 1)) \geq 1000$; more generally, either $c(f, (x, y)) \geq x$ for all (x, y), or $c(f, (x, y)) \geq y$ for all $x, y \in \mathbf{N}$.*

(This particular variant of Colson's result follows from a stronger Theorem 6 in [6], attributed there to Fredholm.)

Moschovakis [6], corollary 19, showed that such inefficiency persists when we allow functions from Φ_0 as givens:

If f is any binary **prc** *over Φ_0 such that $f(x,y) = gcd(x,y)$ for all $x, y \in \mathbf{N}$, then there is a rational constant $C > 0$ such that $c(f,(x,y)) \geq C(x+y)$ for infinitely many $(x,y) \in \mathbf{N}^2$.* (The result in [6] is actually more precise.)

Can we replace here Φ_0 by Φ_1? This question from [6] has a positive answer, even when Φ_0 is replaced by Φ_3:

Theorem 6.1. *Let f be a binary* **prc** *over Φ_3 such that $f(x,y) = gcd(x,y)$ for all $x, y \in \mathbf{N}$. Then there is a rational constant $C > 0$ such that $c(f,(x,y)) > C(x+y)$ for infinitely many $(x,y) \in \mathbf{N}^2$.*

To prove this we first establish a very general fact on primitive recursive algorithms from arbitrary givens, namely Proposition 6.2. This proposition was suggested by the "Basic Lemma" of [6] and by the model-theoretic point of view of earlier sections. We now adopt this model-theoretic setting, and include the (graphs of the) functions in Φ as primitives of our basic model-theoretic structure $\mathbf{Z}$. Thus, given an n-ary **prc** f over Φ and $x \in {}^*\mathbf{N}^n$ we have $f(x) \in {}^*\mathbf{N}$ and $c(f,x) \in {}^*\mathbf{N}$.

Proposition 6.2. *Let f be an n-ary* **prc** *over Φ, and let $a \in {}^*\mathbf{N}^n$. If $c(f,a) \in \mathbf{N}$, then $f(a) = \theta(a)$ for some n-ary Φ-function θ. If $c(f,a) > \mathbf{N}$, then $c(f,a) \geq \theta(a) > \mathbf{N}$ for some n-ary Φ-function θ.*

Proof. We proceed by induction on the construction of the word f. The lemma holds trivially for $f \in \{O, S\} \cup \{P_i^m : 1 \leq i \leq m\} \cup \{\phi : \phi \in \Phi\}$.

Let $f = S_n^m g h_1 \dots h_m$ as in clause (5) of the definition of **prc**. Put $b = (h_1(a), \dots, h_m(a))$.

Suppose first that $c(h_1,a), \dots, c(h_m,a) \in \mathbf{N}$. Then we may assume inductively that $h_1(a) = \theta_1(a), \dots, h_m(a) = \theta_m(a)$ where $\theta_1, \dots, \theta_m$ are n-ary Φ-functions. If also $c(g,b) \in \mathbf{N}$, then, inductively, $g(b) = s(b)$ where s is an m-ary Φ-function, and $c(f,a) \in \mathbf{N}$, and $f(a) = \theta(a)$ for the Φ-function $\theta := s(\theta_1, \dots, \theta_m)$. If on the other hand $c(g,b) > \mathbf{N}$, then we may assume inductively that $c(g,b) \geq s(b) > \mathbf{N}$ where s is an m-ary Φ-function, and then $c(f,a) \geq c(g,b) \geq s(b) = \theta(a) > \mathbf{N}$, where again $\theta := s(\theta_1, \dots, \theta_m)$ is a Φ-function.

Suppose next that $c(h_i,a) > \mathbf{N}$ for a certain i, $1 \leq i \leq m$. Then $c(h_i,a) \geq \theta_i(a) > \mathbf{N}$ for some n-ary Φ-function θ_i (by induction), hence $c(f,a) \geq \theta_i(a) > \mathbf{N}$.

Let $f = R_n g h$ as in clause (6) of the definition of **prc**. So f is $(n+1)$-ary, and we consider a tuple $(a,t) = (a_1, \dots, a_n, t) \in {}^*\mathbf{N}^{n+1}$.

Suppose first that $t \in \mathbf{N}$. For such t we proceed by induction on t (keeping a fixed). We have $f(a,0) = g(a)$ and $c(f,(a,0)) = c(g,a)$, so for $t = 0$ the desired result follows from the inductive assumption on g. Let $t > 0$, and

write $t = k+1$, $k \in \mathbf{N}$, so

$$f(a,t) = h(a,k,f(a,k))$$
$$c(f,(a,t)) = \max\{c(f,(a,k))+1, c(h,(a,k,f(a,k)))\}.$$

Consider first the subcase that $c(f,(a,k)) \in \mathbf{N}$ and $c(h,(a,k,f(a,k)) \in \mathbf{N}$. Then $c(f,(a,t)) \in \mathbf{N}$, and, inductively,

$$f(a,k) = \theta_1(a,k), \quad h(a,k,f(a,k)) = \theta_2(a,k,f(a,k))$$

where θ_1 is an $(n+1)$-ary Φ-function, and θ_2 is an $(n+2)$-ary Φ-function. Hence $f(a,t) = \theta_2(a,k,\theta_1(a,k)) = \theta(a,t)$, where θ is the $(n+1)$-ary Φ-function $(x,y) \mapsto \theta_2(x,k,\theta_1(x,k))$, with $(x,y) = (x_1,\ldots,x_n,y) \in \mathbf{N}^{n+1}$. Second subcase: $c(f,(a,k)) \in \mathbf{N}$ and $c(h,(a,k,f(a,k)) > \mathbf{N}$. Then

$$f(a,k) = \theta_1(a,k)$$
$$c(h,(a,k,f(a,k)) \geq \theta_2(a,k,f(a,k)) = \theta_2(a,k,\theta_1(a,k)) > \mathbf{N}$$

where θ_1 is an $(n+1)$-ary Φ-function, and θ_2 is an $(n+2)$-ary Φ-function. Hence $c(f,(a,t)) \geq \theta(a,t) > \mathbf{N}$ where the $(n+1)$-ary Φ-function θ is defined by the same expression as in the previous subcase.
Third subcase: $c(f,(a,k)) > \mathbf{N}$. Now we use our inductive assumption on t to obtain $c(f,(a,k)) \geq \theta_1(a,k) > \mathbf{N}$, where θ_1 is an $(n+1)$-ary Φ-function. Then $c(f,(a,t)) \geq \theta(a,t) > \mathbf{N}$, where θ is the $(n+1)$-ary function $(x,y) \mapsto \theta_1(x,k)+1$.

Suppose next that $t > \mathbf{N}$. Then $c(f,(a,t)) \geq t = P^{n+1}_{n+1}(a,t) > \mathbf{N}$, so the desired result holds. □

Proof of Theorem 6.1. We take positive infinite $\alpha, \beta \in {}^*\mathbf{Z}$ and R as in the proof of Proposition 4.1. Note that $R^{\geq 0}$ is closed under the natural extensions of the operations of Φ_3 to ${}^*\mathbf{N} \subseteq {}^*\mathbf{Z}$.

Claim. $c(f,(\alpha,\beta)) > \mathbf{N}$.
Suppose otherwise. Then by Proposition 6.2 we have $\gcd(\alpha,\beta) = f(\alpha,\beta) = \theta(\alpha,\beta)$ where θ is a binary Φ_3-function. Hence $\gcd(\alpha,\beta) = \theta(\alpha,\beta) \in R$, contradicting the proof of Proposition 4.1. The claim is established.

Using Proposition 6.2 again, we obtain $c(f,(\alpha,\beta)) \geq \theta(\alpha,\beta)) > \mathbf{N}$, where θ is a binary Φ_3-function. Since $\theta(\alpha,\beta) \in R$, we can use a result stated in the last paragraph of the proof of Proposition 4.1 to conclude that $\theta(\alpha,\beta) \geq C(\alpha+\beta)$ for some rational $C > 0$. Hence $c(f,(\alpha,\beta)) \geq C(\alpha+\beta)$. As $\alpha,\beta \notin \mathbf{N}$, it follows that there are infinitely many $(a,b) \in \mathbf{N}^2$ such that $c(f,(a,b)) \geq C(a+b)$. This finishes the proof of Theorem 6.1.

Applying the argument above to Φ_2 instead of Φ_3, and using Proposition 2.1 we obtain:

Corollary 6.3. *Let f be a binary* **prc** *over Φ_2 such that $f(x,y) = gcd(x,y)$ for all $x,y \in \mathbf{N}$. Let $r > 0$ be irrational, and let (a_n) and (b_n) be sequences of positive integers such that $\frac{a_n}{b_n} \to r$ as $n \to \infty$. Then there is a rational*

$\gamma > 0$ such that $c(f,(\alpha_n,\beta_n)) \geq \gamma(\alpha_n+\beta_n)$ for all sufficiently large n, where $\alpha_n := n!a_n$ and $\beta_n := n!b_n$.

Similarly, the details of Proposition 4.1 lead to:

Corollary 6.4. *Let f be a binary* **prc** *over Φ_3 such that $f(x,y) = gcd(x,y)$ for all $x,y \in \mathbf{N}$. Let $r > 0$ be transcendental, and let (a_n) and (b_n) be sequences of positive integers such that $\frac{a_n}{b_n} \to r$ as $n \to \infty$. Then there is a rational $\gamma > 0$ and there are positive integers κ_n such that $c(f,(\alpha_n,\beta_n)) \geq \gamma(\alpha_n+\beta_n)$ for all sufficiently large n, where $\alpha_n := \kappa_n a_n$ and $\beta_n := \kappa_n b_n$.*

Decomposing a prc over a subset of its domain. Theorem 6.1 and its two corollaries concern only **prc**'s that compute the gcd. The next results about arbitrary **prc**'s are in the spirit of the "Basic Lemma " in [6], and can be viewed as a standard counterpart to the model-theoretic proposition 6.2. We finish this paper with an application to **prc**'s over Φ_1.

Let $S \subseteq \mathbf{N}^n$. A *Φ-set in S* is by definition a level set of the form

$$\{x \in S : \phi_1(x) = a_1, \ldots, \phi_k(x) = a_k\},$$

where $\phi_1, \ldots, \phi_k$ are n-ary Φ-functions. Then the part of Proposition 6.2 that covers the case $c(f,a) \in \mathbf{N}$ is a consequence of the following more precise result.

Proposition 6.5. *Let f be an n-ary* **prc** *over Φ, and $d \in \mathbf{N}$. Then there are disjoint Φ-sets $S_1, \ldots, S_k$ in $\mathbf{N}^n$ and n-ary Φ-functions $\phi_1, \ldots, \phi_k$ such that*

$$\{x \in \mathbf{N}^n : c(f,x) \leq d\} = S_1 \cup \cdots \cup S_k$$

and $f(x) = \phi_\kappa(x)$ for $x \in S_\kappa$, $\kappa = 1, \ldots, k$.

Proof. Call $(S_1, \phi_1, \ldots, S_k, \phi_k)$ *good for* (f,d) if $S_1, \phi_1, \ldots, S_k, \phi_k$ satisfy the conclusion of the proposition. We proceed by induction on f. Suppose $f = S_n^m g h_1 \ldots h_m$ as in clause (5) of the definition of **prc**. If $x \in \mathbf{N}^n$ and $y := h(x) = (h_1(x), \ldots, h_m(x)) \in \mathbf{N}^m$, then

$$c(f,x) \leq d \Longleftrightarrow c(h_1,x), \ldots, c(h_m,x), c(g,y) \leq d.$$

We may assume inductively that we have disjoint Φ-sets $S_1, \ldots, S_k$ in $\mathbf{N}^n$ and n-ary Φ-functions $\phi_{\mu 1}, \ldots, \phi_{\mu k}$ for $\mu = 1, \ldots, m$ such that

$$\{x \in \mathbf{N}^n : c(h_1,x), \ldots, c(h_m,x) \leq d\} = S_1 \cup \cdots \cup S_k$$

and $h_\mu(x) = \phi_{\mu\kappa}(x)$ for $1 \leq \mu \leq m$, $1 \leq \kappa \leq k$ and $x \in S_\kappa$. We may also assume inductively that $(T_1, \chi_1, \ldots, T_l, \chi_l)$ is good for (g,d). Then the kl sets $S_\kappa \cap h^{-1}(T_\lambda)$ are disjoint Φ-sets in $\mathbf{N}^n$, and $f(x) = \phi_{\kappa\lambda}(x)$ for $x \in S_\kappa \cap h^{-1}(T_\lambda)$, where $\phi_{\kappa\lambda} := \chi_\lambda(\phi_{1\kappa}, \ldots, \phi_{m\kappa})$.

Next, let $f = R_n g h$ as in clause (6) of the definition of **prc**. Below we let x range over $\mathbf{N}^n$ and t over $\mathbf{N}$. Then $\{(x,t) : c(f,(x,t)) \leq d\}$ is the disjoint

union of the sets $A_0, \ldots, A_d$ where $A_i := \{(x,t) : c(f,(x,i)) \leq d \text{ and } t = i\}$ for $0 \leq i \leq d$. Thus it suffices to show:

Claim. For each $i \in \{0, \ldots, d\}$ there are disjoint Φ-sets $A_{i1}, \ldots, A_{ik}$ in $\mathbf{N}^n$ (with $k \in \mathbf{N}$ depending on i) and n-ary Φ-functions $\phi_{i1}, \ldots, \phi_{ik}$ such that

$$\{x : c(f,(x,i)) \leq d\} = A_{i1} \cup \cdots \cup A_{ik}$$

and $f(x,i) = \phi_{ij}(x)$ for $j = 1, \ldots, k$ and all $x \in A_{ij}$.

We prove this claim by induction on i. We may assume inductively that $(S_1, \chi_1, \ldots, S_l, \chi_l)$ is good for (g,d). Since $c(f,(x,0)) = c(g,x)$ for all x, the claim holds for $i = 0$ (and any d), with $k = l$, $A_{0j} = S_j$ and $\phi_{0j} = \chi_j$.

Next, assume inductively that the claim above holds for a certain i and all $d > i$, and suppose $i + 1 \leq d$.

We shall prove the claim for i replaced by $i + 1$. Take disjoint Φ-sets $B_1, \ldots, B_k$ in $\mathbf{N}^n$ and n-ary Φ-functions $\psi_1, \ldots, \psi_k$ such that

$$\{x : c(f,(x,i)) \leq d - 1\} = B_1 \cup \cdots \cup B_k$$

and $f(x,i) = \psi_\kappa(x)$ for $\kappa = 1, \ldots, k$ and $x \in A_k$. Let $(T_1, \theta_1, \ldots, T_l, \theta_l)$ be good for (h,d). Put

$$A_{\kappa\lambda} := \{x : x \in B_\kappa, (x, i, \psi_\kappa(x)) \in T_\lambda\},$$

and let $\phi_{\kappa\lambda}$ be the n-ary Φ-function given by $\phi_{\kappa\lambda}(x) = \theta_\lambda(x, i, \psi_\kappa(x))$, for $1 \leq \kappa \leq k$ and $1 \leq \lambda \leq l$. Then the kl sets $A_{\kappa\lambda}$ are disjoint Φ-sets in $\mathbf{N}^n$, and $f(x,i) = \phi_{\kappa\lambda}(x)$ for $x \in A_{\kappa\lambda}$. □

The next result strengthens Proposition 6.2. It also resembles the last proposition, but does not seem to contain it as a special case. A key feature of the theorem is that we allow an arbitrary set $S \subseteq \mathbf{N}^n$ as a parameter.

Theorem 6.6. *Let f be an n-ary* **prc** *over Φ, and let $S \subseteq \mathbf{N}^n$. Then there are disjoint Φ-sets $S_1, \ldots, S_k$ in S and n-ary Φ-functions $\phi_1, \ldots, \phi_k$ such that $S = S_1 \cup \cdots \cup S_k$, and for each $j \in \{1, \ldots, k\}$:*

> **either** *$c(f,x)$ is bounded on S_j and $f(x) = \phi_j(x)$ on S_j,*
> **or** *$c(f,x) \geq \phi_j(x)$ on S_j and ϕ_j is unbounded on S_j.*

Proof. We proceed by induction on f. Suppose $f = S_n^m g h_1 \ldots h_m$ as in clause (5) of the definition of **prc**.

The inductive assumption on $h_1, \ldots, h_m$, together with an induction on m left to the reader, produces disjoint Φ-sets $S_1, \ldots, S_k$ in S with union S such that for each $j = 1, \ldots, k$ one of the following holds:

(a) $c(h_1,x), \ldots, c(h_m,x)$ are bounded on S_j, and we have n-ary Φ-functions $\psi_{1j}, \ldots, \psi_{mj}$ such that $h_1(x) = \psi_{1j}(x), \ldots, h_m(x) = \psi_{mj}(x)$ on S_j;

(b) for some $\mu \in \{1, \ldots, m\}$ there is an n-ary Φ-function $\psi_{\mu j}$ that is unbounded on S_j and satisfies $c(h_\mu, x) \geq \psi_{\mu j}(x)$ on S_j.

Suppose we are in case (a). Then we subdivide each S_j further as follows. Let h denote the map $x \mapsto (h_1(x), \ldots, h_m(x)) : \mathbf{N}^n \to \mathbf{N}^m$. By the inductive

assumption applied to g and the set $h(S_j) \subseteq \mathbf{N}^m$ we can choose disjoint Φ-sets $T_1, \ldots, T_l$ in $h(S_j)$ with union $h(S_j)$ and m-ary Φ-functions $\chi_1, \ldots, \chi_l$ such that for each $\lambda \in \{1, \ldots, l\}$:

either $c(g, y)$ is bounded on T_λ and $g(y) = \chi_\lambda(y)$ on T_λ,
or $c(g, y) \geq \chi_\lambda(y)$ on T_λ and χ_λ is unbounded on T_λ.

For $\lambda = 1, \ldots, l$ we put $S_{j\lambda} := S_j \cap h^{-1}(T_\lambda)$, hence $S_{j\lambda}$ is a Φ-set in S, $h(S_{j\lambda}) = T_\lambda$, and S_j is the disjoint union of $S_{j1}, \ldots, S_{jl}$. Fix some $\lambda \in \{1, \ldots, l\}$. Let $\phi_{j\lambda}$ be the n-ary Φ-function $\chi_\lambda(\psi_{1j}, \ldots, \psi_{mj})$. If $c(g, y)$ is bounded on T_λ, then $c(f, x)$ is bounded on $S_{j\lambda}$, and $f(x) = \phi_{j\lambda}(x)$ on $S_{j\lambda}$. If $c(g, y)$ is unbounded on T_λ, then $c(f, x) \geq c(g, h(x)) \geq \phi_{j\lambda}(x)$ on $S_{j\lambda}$, and $\phi_{j\lambda}$ is unbounded on $S_{j\lambda}$. This takes care of case (a).

Suppose we are in case (b). Then we do not have to subdivide S_j further, since $c(f, x) \geq c(h_\mu, x) \geq \psi_{\mu j}, x)$ on S_j, and $\psi_{\mu j}$ is unbounded on S_j.

Next we assume that $f = R_n g h$ as in clause (6) of the definition of **prc**. Let $S \subseteq \mathbf{N}^{n+1}$. Let x range over $\mathbf{N}^n$, and t over $\mathbf{N}$. If the set of last coordinates t of points $(x, t) \in S$ is unbounded, then we are done, since $c(f, (x, t)) \geq t = P^{n+1}_{n+1}(x, t)$. So we can assume that we have $d \in \mathbf{N}$ such that $t \leq d$ for all $(x, t) \in S$. As in the proof of the last proposition we see that in this situation it suffices to establish the following.

Claim. For each $i \in \{0, \ldots, d\}$ there are disjoint Φ-sets $A_{i1}, \ldots, A_{ik}$ in $S(i) := \{x : (x, i) \in S\}$ whose union is $S(i)$ and there are n-ary Φ-functions $\phi_{i1}, \ldots, \phi_{ik}$ such that for each $j \in \{1, \ldots, k\}$ either $\{c(f, (x, i)) : x \in A_{ij}\}$ is bounded and $f(x, i) = \phi_{ij}(x)$ for all $x \in A_{ij}$, or $c(f, (x, i)) \geq \phi_{ij}(x)$ for all $x \in A_{ij}$ and ϕ_{ij} is unbounded on A_{ij}.

We prove this claim by induction on i. For $i = 0$ the claim follows from the inductive assumption on g. Next, assume inductively that the claim above holds for a certain i and suppose $i + 1 \leq d$. We shall prove the claim for i replaced by $i + 1$. Take disjoint Φ-sets A_{ij} in $S(i)$ and n-ary Φ-functions ϕ_{ij} (for $j = 1, \ldots, k$) that witness the claim above. We now focus on one particular set A_{ij}.

Suppose first that $\{c(f, (x, i)) : x \in A_{ij}\}$ is bounded, so $f(x, i) = \phi_{ij}(x)$ for $x \in A_{ij}$. Then we subdivide A_{ij} as follows. We apply the inductive assumption to h and the set $B_{ij} := \{(x, i, \phi_{ij}(x)) : x \in A_{ij}\} \subseteq \mathbf{N}^{n+2}$. This gives disjoint Φ-sets $T_1, \ldots, T_l$ in B_{ij} with union B_{ij} and $(n+2)$-ary Φ-functions $\theta_1, \ldots, \theta_l$ such that for each $\lambda \in \{1, \ldots, l\}$ either $c(h, y)$ is bounded on T_λ and $h(y) = \theta_\lambda(y)$ on T_λ, or $c(h, y) \geq \theta_\lambda(y)$ on T_λ and θ_λ is unbounded on T_λ. For $\lambda = 1, \ldots, l$ we put

$$A_{ij\lambda} := \{x \in S(i) : (x, i, \phi_{ij}(x)) \in T_\lambda\},$$

so $A_{ij1}, \ldots, A_{ijl}$ are disjoint Φ-sets in $S(i)$ with union A_{ij}. Let $\lambda \in \{1, \ldots, l\}$, and let $\phi_{ij\lambda}$ be the n-ary Φ-function $x \mapsto \theta_\lambda(x, i, \phi_{ij}(x))$. If $\{c(h, y) : y \in T_\lambda\}$ is bounded, so is $\{c(f, (x, i + 1)) : x \in A_{ij\lambda}\}$, and

$$f(x, i + 1) = h(x, i, f(x, i)) = \theta_\lambda(x, i, \phi_{ij}(x)) = \phi_{ij\lambda}(x)$$

for $x \in A_{ij\lambda}$. If $\{c(h,y) : y \in T_\lambda\}$ is unbounded, then we have for $x \in A_{ij\lambda}$:

$$c(f,(x,i+1)) \geq c(h,(x,i,f(x,i)) \geq \theta_\lambda(x,i,\phi_{ij}(x)) = \phi_{ij\lambda}(x),$$

and $\phi_{ij\lambda}$ is unbounded on $A_{ij\lambda}$.

Next, suppose that $\{c(f,(x,i)) : x \in A_{ij}\}$ is unbounded. Then we have $c(f,(x,i+1)) \geq \phi_{ij}(x)$ for all $x \in A_{ij}$, and ϕ_{ij} is unbounded on A_{ij}. So in this case there is no need to subdivide A_{ij} further. □

Our final result solves a version of "Problem 1" of [6]. Its proof is specific to **prc**'s over Φ_1 and does not apply to **prc**'s over Φ_2. The power lower bound in this corollary cannot be replaced by a linear lower bound, as indicated in the example following its proof. We put $|x| := |x_1| + \cdots + |x_n|$ for $x \in \mathbf{N}^n$.

Corollary 6.7. *Let f be an n-ary* **prc** *over Φ_1 such that $\{c(f,x) : x \in \mathbf{N}^n\}$ is unbounded. Then there is rational constant $\gamma > 0$ such that $c(f,x) > |x|^\gamma$ for infinitely many $x \in \mathbf{N}^n$.*

Proof. By the last theorem there is a Φ_1-set S in $\mathbf{N}^n$ and an n-ary Φ_1-function ϕ such that $c(f,x) \geq \phi(x)$ for all $x \in S$ and ϕ is unbounded on S. The set S and the graph of the function ϕ are easily seen to be existentially definable in $(\mathbf{Z},0,1,+,-,<,|)$, the ordered group of integers with order and divisibility. Corollary 1.6 in [4] then implies the existence of a rational constant $\gamma > 0$ such that $\phi(x) > |x|^\gamma$ for infinitely many $x \in S$. □

Example. Let x and y range over $\mathbf{N}$, and let ϕ be the binary function defined by $\phi(x,y) = x$ if $x,y > 0$, $x|y$ and $x+1|y$, and $\phi(x,y) = 0$ otherwise. For any rational γ with $0 < \gamma < 1/2$, we have $\phi(x,y) > (x+y)^\gamma$ for infinitely many (x,y), but $\phi(x,y) > \gamma(x+y)$ for only finitely many (x,y). Using the fact that ϕ is a Φ_1-function, it is easy to obtain a binary **prc** f over Φ_1 such that $c(f,(x,y)) = \phi(x,y)$ for all (x,y).

7. Concluding Remarks

The model theory used in this paper is quite elementary and can probably be avoided with some effort. However, eliminating the model theory would not reflect the way propositions 2.1, 4.1 and 6.2 were *discovered*.

On a minor technical point, the assumption in the proof of Proposition 2.1 that ${}^*\mathbf{Z}$ is $\aleph_1$-saturated is only made to take care of *all* irrational $r > 0$. If ${}^*\mathbf{Z}$ is just a proper elementary extension of the ring $\mathbf{Z}$, then not all irrational cuts in $\mathbf{Q}$ may be realizable by ratios of elements in ${}^*\mathbf{Z}$, but irrationals such as $\sqrt{2}$ and e (which are arithmetically definable) are always realized by such a ratio.

References

[1] C. Chang and J. Keisler, Model Theory, 3rd edition, North-Holland, Amsterdam, 1990.

[2] P. Cijsouw, *Transcendence measures of exponentials and logarithms of algebraic numbers*, Compositio Math. **28** (1974), pp. 163–178.

[3] L. Colson, *About primitive recursive algorithms*, Theoretical Computer Science **83** (1991), pp. 57–69.
[4] L. van den Dries and A.J. Wilkie, *The laws of integer divisibility, and solution sets of linear divisibility conditions*, J. Symbolic Logic (to appear).
[5] W. LeVeque, *Fundamentals of number theory*, Addison-Wesley, Massachusetts, 1977.
[6] Y. Moschovakis, *On primitive recursive algorithms and the greatest common divisor function*, Theoretical Computer Science (to appear).

University of Illinois, Department of Mathematics, 1409 W. Green Street, Urbana, IL 61801
E-mail address: vddries@math.uiuc.edu