

Linear recurrence relations are Δ_0 definable

Alessandro Berarducci

Dipartimento di Matematica, Università di Pisa
Via Buonarroti 2, 56127 Pisa, Italy
berardu@dm.unipi.it

Benedetto Intrigila

Dipartimento di Matematica, Università di L'Aquila
Via Vetoio, 67010 Coppito, L'Aquila, Italy
intrigila@axscaq.aquila.infn.it

Abstract

We prove that the map $A, n \mapsto A^n$, where A is a $k \times k$ matrix with non-negative integer coefficients is Δ_0 definable. As a consequence functions obtained by linear recurrence relations with non-negative integer coefficients are Δ_0 definable. These include the Fibonacci sequence as well as functions of polynomial growth rate. It turns out that it is impossible to mimic the well known Δ_0 definition of the exponential map $n \mapsto 2^n$. A combinatorial approach based on counting the number of solutions of linear diophantine equations is instead used.

1 Introduction

Among the fragments of Peano Arithmetic (see [K,HP] for an overview) we can distinguish among:

1. strong fragments: $PA \supset I\Sigma_n \supset I\Sigma_1 \supset PRA \supset I\Delta_0 + exp$,
2. medium fragments: $I\Delta_0 + \Omega_1 \supset I\Delta_0 \supset IE_1$,
3. weak fragments: $IO+$ normality $\supset IO \supset$ Robinson's Q .

Strong fragments interpret a reasonable amount of the theory of hereditarily finite sets and a large part of elementary number theory can be carried

out over these fragments. Weak fragments possess an elegant algebraic characterization which links them to the theory of real closed fields [S]. Medium fragments are the most elusive ones, due their deep connection with central issues in computational complexity (see [Bu]). On the other hand, some medium fragments are also of special interest in that they are the natural framework to determine which finite combinatorial principles, formulated as schemes for bounded formulas, are needed to prove classical theorems of number theory (see [WI, W, PWW, BI2]). In this note we are interested in the most typical medium fragment, $\text{I}\Delta_0$ or “bounded arithmetic”, obtained by restricting the induction scheme to Δ_0 formulas.

We recall that a subset $P \subset \mathbf{N}^k$ is Δ_0 (definable by a Δ_0 formula) iff it can be defined using only the arithmetical operations $+$, \cdot , the order relation \leq , boolean connectives, and bounded quantifiers $\forall x \leq p(\vec{y})$ and $\exists x \leq p(\vec{y})$, where p is a polynomial. A function $F: \mathbf{N}^k \rightarrow \mathbf{N}$ is Δ_0 iff its graph $G(F) = \{(x, y) \mid F(x) = y\}$ is a Δ_0 subset of \mathbf{N}^{k+1} .

One is interested both in the Δ_0 definability of functions, and in the proof of the “relevant properties” of the functions inside the theory $\text{I}\Delta_0$. When this can be done, then the function can be extended in a meaningful way from \mathbf{N} to an arbitrary model of $\text{I}\Delta_0$.

In general it can be a difficult task to prove that a given function is Δ_0 , not to speak of the $\text{I}\Delta_0$ provability of its properties. For instance let:

$$F(x) = \begin{cases} 0 & \text{if } x \text{ is prime} \\ 1 & \text{if } x \text{ is composite} \end{cases}$$

F is Δ_0 because “ n is prime” can be expressed using only bounded quantifiers: $\forall x, y \leq n(x > 1 \wedge y > 1 \rightarrow n \neq xy)$. So testing for primes is Δ_0 . It is however an open problem [W] whether “counting the primes $\leq n$ ” is Δ_0 , namely whether the function

$$G(n) := \sum_{i \leq n} F(i) \tag{1}$$

is Δ_0 . On the other hand, by the prime number theorem $G(n)$ is approximately equal to the Δ_0 function given by the integer part of $\frac{n}{\log(n)}$. So, by some number theoretic fact $G(n)$ could turn out to be Δ_0 representable, and nevertheless it might happen that one cannot prove in $\text{I}\Delta_0$ its relation with primes. In general Δ_0 functions are not closed under composition. If however we restrict to those Δ_0 functions which are polynomially bounded, then we obtain a class of functions Δ_0^{poly} which is closed under composition

and is contained in the second class \mathcal{E}_2 of the Grzegorzczyc hierarchy. It is not known whether $\Delta_0^{\text{poly}} = \mathcal{E}_2$. The problem is that \mathcal{E}_2 is closed under bounded recursion (i.e. those primitive recursive definitions which do not lead outside the polynomially bounded functions), while the example of equation (1) shows that Δ_0^{poly} is not even known to be closed under summations (which is a special case of bounded recursion). In view of these remarks a crucial problem is:

Which kinds of recursive definitions do not lead outside Δ_0 ?

A satisfactory answer is still very remote. A basic result is that the graph of exponentiation $x^y = z$ is Δ_0 [B,GD,P,D,BI]. Woods, Paris and Wilkie have partial results on the summation problem. If G is defined recursively in terms of F as in equation (1) and $k \in \mathbf{N}$, then:

1. $n \mapsto G(\log^k(n))$ is Δ_0 [W, PWW].
2. $n \mapsto \min\{G(n), \log^k(n)\}$ is Δ_0 provided F is 0, 1 valued [PW] (we can interpret this by saying that we can count sparse Δ_0 sets).

Using these results one can solve the corresponding problem for products: $G(n) := \prod_{i \leq n} F(i)$ is always Δ_0 whenever F is Δ_0 [BD].

In this note we show that for fixed k , linear recurrence relations

$$F(n+k) = a_1 F(n+k-1) + a_2 F(n+k-2) + \dots + a_k F(n)$$

with non-negative coefficients $a_1, \dots, a_k \in \mathbf{N}$ and given initial conditions, are Δ_0 (i.e. the function $n \mapsto F(n)$ has Δ_0 graph, and moreover the dependency on the coefficients a_i and the initial conditions is also Δ_0).

We also show that if A is a $k \times k$ matrix with non-negative integer coefficients then the function $A, n \mapsto A^n$ (which we call **matrix iteration**) has Δ_0 graph as a function from $\mathbf{N}^{k^2} \times \mathbf{N}$ to \mathbf{N}^{k^2} . Actually matrix iteration and linear recurrence relations are essentially the same thing.

To keep all the definitions Δ_0 , we follow a direct combinatorial approach which, in the difficult case, reduces the problem of computing A^n to that of counting the number of solutions of certain linear diophantine equations. Since complex exponentiation $n \rightarrow \alpha^n$ ($n \in \mathbf{N}, \alpha \in \mathbf{C}$) is not directly available as a Δ_0 function, it is not clear whether an approach based on Jourdan normal forms can be used. On the other hand our approach might be a tool to deal with complex numbers through matrix encodings.

In the last section we consider the problem of proving the relevant properties of matrix iteration inside $\text{I}\Delta_0$.

2 The Turing predicate

Often one can prove that a function is Δ_0 with the help of its “Turing predicate” as follows. Given a function f defined by a set of recursive equations, we say that a natural number C **codes a computation** of $f(x) = y$ if C codes an equational proof of $f(x) = y$.

In some cases instead of the equational proof one can use a shorter but essentially equivalent code. For instance suppose that we define exponentiation via the equations $2^0 = 1, 2^{x+1} = 2^x \cdot 2$ (plus appropriate equations for addition and multiplication). We say that C codes a computation of $2^4 = 16$ iff C codes the sequence of numbers $(1, 2, 4, 8, 16)$ (as all the needed information of the equational proof is already contained here).

It is a well known fact of basic recursion theory that if f is defined by a general recursive system of equations, then the predicate $\{(C, x, y) \mid C \text{ codes a computation of } f(x) = y\}$ is primitive recursive, and even Δ_0 if the coding is done with some care (one can also do it in a uniform way in f , obtaining the so called “Turing predicate”).

We obviously have:

$$f(x) = y \text{ iff } \exists C : \text{“}C \text{ codes a computation of } f(x) = y\text{”}.$$

Since the expression between quotes is Δ_0 , the whole expression is Σ_1 (i.e. Δ_0 preceded by unbounded existential quantifiers).

If one manages to obtain a polynomial bound on C in terms of $\max\{x, y\}$, then one obtains a Δ_0 definition of (the graph of) f . This is somehow easier if f is rapidly growing, since then y is very big, and there are more chances of giving a polynomial bound on C in terms of y . This remark is exploited in the proof that (the graph of) $x \mapsto 2^x$ is Δ_0 definable. Indeed the main ideas are:

1. Exploit the fact that 2^x is rapidly growing;
2. Instead of $2^0 = 1, 2^{x+1} = 2^x \cdot 2$, use the functional equations $2^0 = 1, 2^{2x} = (2^x)^2, 2^{2x+1} = (2^x)^2 \cdot 2$ in order to shorten computations.

Suppose now that A is a $k \times k$ matrix with entries in \mathbf{N} . We want to generalize integer exponentiation by giving a Δ_0 definition of the graph of $A, n \mapsto A^n$ (as a function $F: \mathbf{N}^{k^2} \times \mathbf{N} \rightarrow \mathbf{N}^{k^2}$). We can still exploit the functional equations $A^{2x} = (A^x)^2, A^{2x+1} = (A^x)^2 \cdot A$, but in general the entries of A^n are not rapidly growing, so one of the two ingredients of the Δ_0 definition of integer exponentiation cannot be used for matrix

iteration. For instance if $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, then $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, and all the entries of A^n grow only linearly. Now let $\max A$ be the maximum of the entries of the matrix A . Using essentially the same ideas as those for integer exponentiation one can (only) show that:

Theorem 2.1 *The function $A, n \mapsto A^n$ (as a function from $\mathbf{N}^{k^2} \times \mathbf{N}$ to \mathbf{N}^{k^2}) is Δ_0 provided A^n grows exponentially, i.e. $p(\max(A^n)) \geq m^n$, where $p(y)$ is a polynomial depending only on the dimension k of the matrix, and m is the maximum between $\max A$ and 2.*

Proof. It suffices to observe that, as in the case of integer exponentiation, there is an integer polynomial $p(y)$ such that $A^n = B$ iff $\exists C \leq p(m^n) : "C$ codes a computation of $A^n = B"$. Now if $\geq m^n$ is polynomially bounded in terms of $\max(A^n)$, one obtains that C is polynomially bounded by $\max B$ and therefore $A^n = B$ is Δ_0 definable. More details can be found in the unpublished note [BI]. QED

Now, we would like to eliminate the "proviso" from Theorem 2.1. However let us first notice that Theorem 2.1 is already sufficient to obtain a Δ_0 definition of the Fibonacci function $n \mapsto F(n)$ as follows (see [BI]). The function F is defined by the linear recurrence relation $F(n+2) = F(n+1) + F(n)$ with initial conditions $F(0) = 0, F(1) = 1$. Introducing an auxiliary function $G(n)$ we obtain a 2×2 system of linear equations

$$\begin{cases} F(n+1) = F(n) + G(n) \\ G(n+1) = F(n) \end{cases} \quad \text{with the initial conditions } F(0) = 0, G(0) = 1.$$

Next put the system in matrix form: $\begin{pmatrix} F(n+1) \\ G(n+1) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} F(n) \\ G(n) \end{pmatrix}$.

Deduce that $\begin{pmatrix} F(n) \\ G(n) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Using such arguments one can easily show:

Proposition 2.2 *The problem of giving a Δ_0 definition of matrix iteration is equivalent to the problem of giving a Δ_0 definition of functions defined by linear recurrence relations.*

The main ideas to extend Theorem 2.1 are combinatorial. We first consider the case of a 0,1-matrix G , which turns out to be the crucial case. These matrices correspond in a natural way to graphs, and G^n has a well

known combinatorial interpretation in terms of counting the number of paths of length n in the graph. We define an “exponential vertex of a graph” as a vertex which belongs to a non-cyclic strongly connected component of the graph. We show that if G is a $0, 1$ matrix, then all the entries of $n \mapsto G^n$ are polynomially bounded iff the corresponding graph has no exponential vertices. In this case computing G^n amounts to counting the number of solutions of certain linear diophantine equations, and using generating functions we can give an explicit coding-free Δ_0 definition of G^n . This will settle iteration of $0, 1$ -matrices in the case of polynomial growth case. The cases of exponential growth are handled by coding computations as in Theorem 2.1. In the general case some entries of G^n grow polynomially and others exponentially depending also on the congruence properties of n . Here a more detailed analysis is needed of the behaviour of G^n , leading anyway to a combination of the above two techniques. The case of an arbitrary matrix, not necessarily $0, 1$, is handled similarly.

3 Graphs and multigraphs

Definition 3.1 A **multigraph** G is given by a set $V = V(G)$ of vertices, a set $E = E(G)$ of edges, and two maps **source**: $E \rightarrow V$ and **target**: $E \rightarrow V$ giving the initial and end-vertices of every edge. A **path** in a multigraph is a finite sequence $\sigma = (x_1, e_1, x_2, e_2, \dots, e_{n-1}, x_n)$ where each e_i is an edge with source x_i and target x_{i+1} . The number n of edges is the **length** of the path σ . We write $\sigma: a \rightarrow b$ if a is the initial vertex of σ and b is its final vertex. If $a = b$ we say that σ is a **circuit**. A circuit of length 1 is called a **loop**. A path $\sigma = (x_1, e_1, x_2, e_2, \dots, e_{n-1}, x_n)$ is **simple** if **target**(e_i) \neq **target**(e_j) whenever $i \neq j$. Note that a loop is always simple. A **simple circuit** is a simple path which is also a circuit. Two paths α and β can be concatenated if there are $a, b, c \in V(G)$ with $\alpha: a \rightarrow b$ and $\beta: b \rightarrow c$. Their **concatenation** is the path $\alpha\beta: a \rightarrow c$.

Definition 3.2 A **graph** is a multigraph G such that given two vertices $a, b \in V(G)$ there is at most one edge e with **source**(e) = a and **target**(e) = b . So the edge e is uniquely determined by the ordered pair (a, b) and we can identify the set E of edges with a subset of V^2 . A path $\sigma = (x_1, e_1, x_2, e_2, \dots, e_{n-1}, x_n)$ in a graph G can be identified with its sequence of vertices (x_1, x_2, \dots, x_n) since the information about the edges is redundant.

Given a path $\sigma = (x_0, \dots, x_n)$ in a graph G , we denote by $|\sigma|$ its **underlying graph**, namely the graph with set of vertices $\{x_0, \dots, x_n\}$ and set of edges (x_i, x_{i+1}) , $i = 0, \dots, n - 1$. A graph is a **(simple) cycle** if it is the underlying graph of a (simple) circuit.

Definition 3.3 Given a graph G and $a, b \in V(G)$ we say that a and b are **connected**, written $a \sim b$, iff there is a path from a to b and a path from b to a . The connected component a/\sim of a is the set of all vertices connected to a . The graph G is connected if it has only one connected component. The edges $(a, b) \in E(G)$ with $a \sim b$ will be called **permanent** edges. The edges $(a, b) \in E(G)$ with $a \not\sim b$ will be called **transitory** edges.

Remark 3.4 Any path σ in a graph G can traverse a transitory edge at most once.

Definition 3.5 Given a graph G the **quotient multi-graph** G/\sim is defined by taking as set of vertices $V(G/\sim)$ the connected components of G , and taking $E(G/\sim) = E(G)$. Given $(a, b) \in E(G/\sim)$ we set **source** $(a, b) = a/\sim$ and **target** $(a, b) = b/\sim$.

Remark 3.6 A path of G/\sim is simple if and only if it *is* a loop or it *has no* loops.

Definition 3.7 Given a graph G and a simple path θ in G/\sim we define G_θ as the subgraph of G with the same set of vertices $V(G_\theta) = V(G)$, and with set of edges $E(G_\theta) \subseteq E(G) \subseteq V(G)^2$ defined as follows. Given $(x, y) \in V(G)^2$, we put (x, y) in $E(G_\theta)$ iff one of the following holds:

1. (x, y) is a transitory edge of G and (x, y) is one of the edges of θ .
2. (x, y) is a permanent edge of G and the connected component C of x (which coincides with the one of y) is one of the vertices of θ .

The subgraphs of G of the form G_θ will be called **segments** of G .

Remark 3.8 There is a natural bijection between simple paths in G/\sim and segments of G .

Definition 3.9 Given a graph G and $a, b \in V(G)$, let $S(G, a, b)$ be the set of all simple paths $\theta: a/\sim \rightarrow b/\sim$ in the multigraph G/\sim .

Remark 3.10 Given $\theta \in S(G, a, b)$ and a path $\sigma: a \rightarrow b$ in G_θ , σ crosses each transitory edges of G_θ exactly once.

The following easy result will be important.

Theorem 3.11 *Let $a, b \in V(G)$. For every path $\sigma: a \rightarrow b$ in G , there exists one and only one $\theta \in S(G, a, b)$ such that σ is a path in the segment G_θ .*

So paths from a to b can be partitioned into the various segments from a to b .

Definition 3.12 G has three kinds of connected components: the trivial ones consisting of only one vertex and no edges; those consisting of a simple cycle; and those containing at least two cycles. We call the last ones **exponential components**, and its vertices **exponential vertices**. A path in G is exponential if it contains an exponential vertex.

The reason for this name is that inside an exponential component we can find exponentially many circuits of length n , provided n is a multiple of the greatest common divisor of the sizes of all the circuits of G (see later).

It is easy to see that if c belongs to a segment G_θ , then c is exponential as a vertex of G_θ iff it is exponential as a vertex of G .

4 Number of non-negative solution of a linear diophantine equation

Given a diophantine equation:

$$c_1x_1 + \dots + c_kx_k = n \tag{2}$$

where c_1, \dots, c_k, n are non-negative integers and each c_i is non-zero, we want to find a Δ_0 formula giving the number of non-negative solutions (x_1, \dots, x_k) of the equation. We need the following well known result (see [G], p. 321) which can be proved using generating functions.

Lemma 4.1 *The number of non-negative solutions of (2) is the coefficient of y^n in the power series expansion of $1/(1 - y^{c_1})(1 - y^{c_2}) \dots (1 - y^{c_k})$.*

Corollary 4.2 *Let c be the least common multiple of c_1, \dots, c_k . Then for every $0 \leq r < c$ there is a rational polynomial $P_r(y) \in \mathbf{Q}[y]$ such that for every $n \equiv r \pmod{c}$ the number of solutions of (2) is $P_r(n)$.*

Proof. Since each c_i divides c , we have that each polynomial $(1 - y^{c_i})$ divides $(1 - y^c)$ in $\mathbf{Z}[y]$. So $1/(1 - y^{c_1})(1 - y^{c_2}) \dots (1 - y^{c_k}) = G(y)/(1 - y^c)^k$ for some $G(y) = b_0 + b_1y + \dots + b_sy^s \in \mathbf{Z}[y]$.

Now the power series development of $1/(1 - y^c)^k$ is given by $\sum_{q=0}^{\infty} \binom{q+k}{k} y^{cq}$. Then when $n = cq + r$ with $0 \leq r < c$, the coefficient of y^n in $G(y)/(1 - y^c)^k$ is $b_r \binom{q+k}{k} + b_{r+c} \binom{q-1+k}{k} + b_{r+2c} \binom{q-2+k}{k} + \dots + b_{r+tc} \binom{q-t+k}{k}$ where t is maximal such that $r+tc$ is less or equal to the degree of $G(y)$. The statement of the proposition now follows at once noticing that for fixed k , the binomial coefficient $\binom{q}{k}$ is a rational polynomial in q , hence in n . QED

A similar computation is carried over in a specific case in ([GKP], p. 324).

Corollary 4.3 *For fixed c_1, \dots, c_k , the function $f(n) =$ the number of solutions of (2) is Δ_0 -definable.*

Question 4.4 Is the number of solution of (2) a Δ_0 function also of the coefficients c_1, \dots, c_k ?

We also need the following easy facts:

Lemma 4.5 *There is a number $d = d(c_1, \dots, c_k)$ such that if (2) has a solution (x_1, \dots, x_k) in \mathbf{Z}^k (or in particular in \mathbf{N}^k), then it has a solution in \mathbf{Z}^k within distance d from any given real solution $(r_1, \dots, r_k) \in \mathbf{R}^k$ (in the sense that $|x_i - r_i| \leq d$).*

Proof. The integral points on the hyperplane $c_1x_1 + \dots + c_kx_k = n$ constitute a module over \mathbf{Z} generated by $k - 1$ independent vectors (if it is non-empty). Take d to be the diameter of the polyedron generated by these vectors. QED

It follows in particular that there are “balanced solutions” in the sense of the following result:

Corollary 4.6 *There is a number $q = q(c_1, \dots, c_k)$ such that if (1) has a non-negative integer solution, then it has a non-negative integer solution $(x_1, \dots, x_k) \in \mathbf{N}^k$ with $x_i \geq \lceil n/q \rceil$ for all i .*

Proof. Consider a real solution (r_1, \dots, r_k) with $r_1 = \dots = r_k = \frac{n}{c_1 + \dots + c_k}$. QED

5 A decomposition theorem to compute the matrix G^n

We identify a graph G with set of vertices $V(G)$ with its adjacency matrix $(G_{a,b})$ defined by: for any $a, b \in V(G)$, $G_{a,b} = 1$ if (a, b) is an edge of G and $G_{a,b} = 0$ otherwise. We write $(G^n)_{a,b}$ for the (a, b) -entry of the matrix G^n . It is well known that $(G^n)_{a,b}$ has the following combinatorial interpretation:

Proposition 5.1 (see [AHU], p. 202) *$(G^n)_{a,b}$ is equal to the number of paths of length n from a to b in the graph G .*

By the previous proposition and Theorem 3.11 we immediately obtain the following decomposition theorem.

Theorem 5.2 $(G^n)_{a,b} = \sum_{\theta \in S(G,a,b)} (G_\theta^n)_{a,b}$

Let $\theta \in S(G, a, b)$. By the above theorem in order to give a Δ_0 definition of $(G^n)_{a,b}$ it is enough to give a Δ_0 definition of $(G_\theta^n)_{a,b}$ as function of n . The definition differs according to:

- G_θ has an exponential vertex. In this case it is convenient to compute the whole matrix $(G_\theta)^n$ using a Turing predicate, and then extract its (a, b) -entry.
- G_θ has no exponential vertices. In this case it is better to compute the entry $(G_\theta^n)_{a,b}$ directly without computing first the whole matrix $(G_\theta)^n$.

In the following sections we consider the two cases.

6 The non-exponential case

Remark 6.1 Let $\theta \in S(G, a, b)$. If G_θ has no exponential vertices then every path $\sigma: a \rightarrow b$ in G_θ has the form $\sigma = \alpha_1 \Delta_1^{x_1} \beta_1 \dots \alpha_k \Delta_k^{x_k} \beta_k$ where Δ_i is a simple circuit of length c_i and $\rho = \alpha_1 \beta_1 \dots \alpha_k \beta_k$ is a simple path from a to b . Moreover ρ is the only simple path from a to b in G_θ .

Definition 6.2 Given $\theta \in S(G, a, b)$ with G_θ without exponential vertices, let $L(\theta, a, b)$ be the length of the unique simple path $\rho: a \rightarrow b$ in G_θ .

It follows from the previous remark:

Lemma 6.3 Let $\theta \in S(G, a, b)$. If G_θ has no exponential vertices, then $(G_\theta^n)_{a,b}$ is equal to the number of non-negative solutions $(x_1, \dots, x_k) \in \mathbf{N}^k$ of the diophantine equation $c_1 x_1 + \dots + c_k x_k + L(\theta, a, b) = n$, where c_1, \dots, c_k are the sizes of the non-trivial connected components of G_θ (necessarily simple cycles).

Using Corollary 4.2 we conclude:

Corollary 6.4 If the segment G_θ has no exponential vertices, then $n \mapsto (G_\theta^n)_{a,b}$ is a Δ_0 function of n .

7 The exponential case for a connected graph

If G is connected and exponential (i.e. it has an exponential vertex) we will find an exponential lower bound on $(G^n)_{a,b}$ for n belonging to some arithmetical progressions.

Definition 7.1 For an arbitrary graph G , let $\gcd(G)$ be the greatest common divisor of the lengths of all (not necessarily simple) circuits of G .

$\gcd(G)$ is well defined because the greatest common divisor of an infinite set of integers coincide with the greatest common divisor of a big enough finite subset. In particular, it is easy to prove that:

Proposition 7.2 $\gcd(G)$ is equal to the greatest common divisor of the size of all simple circuits of G

So $\gcd(G)$ can be easily computed by inspecting the finitely many simple cycles of G .

Remark 7.3 If $G_{a,a}^n \neq 0$, then $\gcd(G)$ divides n .

Conversely we will prove that if n is a big enough multiple of $\gcd(G)$, then $(G^n)_{a,a}$ is exponential in n . We need a representative finite family of “independent” circuits.

Proposition 7.4 *Let G be an exponential connected graph. There is a finite family \mathcal{F} of (not necessarily simple) circuits of G passing through a given vertex a , such that:*

1. $\gcd(G)$ coincides with the gcd of the lengths of the circuits in \mathcal{F} ;
2. each circuit in \mathcal{F} cannot be decomposed as the concatenation of two circuits through a ;
3. every vertex of G is in some circuit in \mathcal{F} ;
4. \mathcal{F} has at least two elements.

Proof. Every circuit Δ in G , not necessarily through a , can be obtained as the “difference” of two circuits passing through a , namely there is a circuit σ through a such that $\sigma\Delta$ is also a circuit through a . Indeed it is enough to take a circuit σ consisting of a path from a to the initial vertex b of Δ , followed by a path from b to a . Such paths exist since G is connected.

It follows that, for the sake of computing $d = \gcd(G)$, it is enough to consider only the circuits passing through a . Then clearly there is a *finite* set \mathcal{F} of circuits through a , such that d is the gcd of the lengths of the circuits in \mathcal{F} . Moreover, we may freely assume that every vertex of G is in some circuit in \mathcal{F} .

We can further arrange so that \mathcal{F} consists entirely of circuits that cannot be written as the concatenation of smaller circuits through a . Indeed if \mathcal{F} contains an element σ which can be written as $\sigma = \sigma_1\sigma_2$ where σ_1 and σ_2 are circuit passing through a , then we can modify \mathcal{F} by removing σ and adding the two circuits σ_1 and σ_2 . Observe that no vertex is lost in this transformation. It only remains to ensure that \mathcal{F} has at least two elements. This is easily done using the fact that G has an exponential vertex. QED

The following lemma explains the name “exponential vertex”.

Lemma 7.5 *Let G be a connected exponential graph. Let $d = \gcd(G)$. There is an integer $q = q(G)$, such that for every $a \in V(G)$ and every sufficiently big n (with respect to the number of vertices of G), $(G^{dn})_{a,a} \geq 2^{\frac{n}{q}}$.*

Proof. Let $\mathcal{F} = \{\tau_1, \dots, \tau_k\}$ be the family of Proposition 7.4. We associate to \mathcal{F} and to n the diophantine equation

$$c_1x_1 + \dots + c_kx_k = dn \tag{3}$$

where $c_i = lh(\tau_i)$.

Since $d = \gcd(G) = \gcd\{c_1, \dots, c_k\}$, it follows from Corollary 4.6 that there is a number $q = q(c_1, \dots, c_k)$ such that the equation (2) has a solution with $x_i \geq \lceil \frac{n}{q} \rceil$ for every i .

To any given solution (x_1, \dots, x_k) we associate a circuit $\sigma: a \rightarrow a$ of length dn by taking $\sigma = \tau_1^{x_1} \tau_2^{x_2} \dots \tau_k^{x_k}$. Since all the τ_i 's are circuits through the same vertex a they can be traversed in any order. Moreover since the circuits τ_i cannot be decomposed as the concatenation of smaller circuits through a , any order of traversing them yields different circuits as a result. So each solution of (2) actually yields as many solutions as the number of ways of ordering x_1 copies of τ_1 , x_2 copies of τ_2 , \dots , x_k copies of τ_k . Since $k \geq 2$, if we fix a solution with $x_i \geq \frac{n}{q}$ for all i (it actually suffices $i = 1, 2$), then this particular solution yields more than $2^{\frac{n}{q}}$ circuits. QED

In particular we have proved that for n big enough $(G^{dn})_{a,a} \neq 0$. For small n 's there can be exceptions. Note that since there are finitely many graphs G with k vertices, the integer $q = q(G)$ can actually be chosen so that it depends only on k .

Lemma 7.6 *Let G be a connected exponential graph and let $d = \gcd(G)$. Given $a, b \in V(G)$, there is a number $r = r(G, a, b) < d$, such that every path from a to b has length congruent to r modulo d .*

Proof. Suppose $\alpha: a \rightarrow b$ and $\beta: a \rightarrow b$ are two paths from a to b . Since G is connected there is a path $\gamma: b \rightarrow a$. Then $\alpha\gamma$ and $\beta\gamma$ are two circuits from a to a , so they have length congruent to zero modulo d . By subtracting γ it follows that the length of α is congruent to the length of β modulo d . QED

Corollary 7.7 *Let G be a connected exponential graph and let $a, b \in V(G)$. There is an arithmetical progression $P = \{dm + r \mid m \in \mathbf{N}\}$ such that:*

1. if $n \notin P$, $(G^n)_{a,b} = 0$,

2. if $n \in P$ is sufficiently big (with respect to G), $(G^n)_{a,b} \geq 2^{\frac{n}{q}}$ for some positive integer $q = q(G)$.

Proof. Let $d = \gcd(G)$ and $r = r(G, a, b)$. It is enough to concatenate the exponentially many paths from a to a given by Lemma 7.5 with a fixed path from a to b . QED

Corollary 7.8 *Let G be a connected exponential graph. There is a some positive integer $q = q(G)$ such that for every big enough n , $\max(G^n) \geq 2^{n/q}$.*

Proof. Let $d = \gcd(G)$ and let $r < d$ be such that $n \equiv r \pmod{d}$. Take $a, b \in V(G)$ so that $r(G, a, b) = r$. (For every a there exists such a b : it suffices to consider any path of length r starting from a and to define b as its final vertex.) Then $(G^n)_{a,b} \geq 2^{n/q}$. QED

Corollary 7.9 *Let G be a connected exponential graph. Then $n \mapsto G^n$ is Δ_0 definable.*

Proof. By Theorem 2.1. QED

8 The general exponential case

Definition 8.1 Given $\theta \in S(G, a, b)$,

- let $\gcd(\theta)$ be the greatest common divisor of the lengths of all the cycles of the graph G_θ ;
- let $T(\theta, a, b)$ be defined as the unique number $q < \gcd(\theta)$ such that for every path $\sigma: a \rightarrow b$ in G_θ we have $lh(\sigma) \equiv q \pmod{\gcd(\theta)}$.

Observe that $T(\theta, a, b)$ is well defined by arguing as in Lemma 7.6.

Theorem 8.2 *Let $\theta \in S(G, a, b)$ and suppose G_θ has an exponential vertex. If n is sufficiently big (with respect to G_θ) we have:*

1. if n is of the form $n = \gcd(\theta)m + T(\theta, a, b)$, then $(G_\theta^n)_{a,b} > 2^{\frac{n}{q}}$ for some $q = q(G_\theta)$;

2. $(G_\theta^n)_{a,b} = 0$, otherwise.

Proof. Part 2. is easy. We prove 1. Let C_1, \dots, C_k be the non-trivial connected components appearing as vertices of the path θ . At least one of them is exponential. Without loss of generality suppose C_1 is exponential. Let $d = \gcd(\theta)$. Then d is also equal to $\gcd\{c_1, \dots, c_k\}$ where $c_i = \gcd(C_i)$ is the gcd of all the lengths of the circuits in C_i . By Corollary 4.6, if m is big enough the diophantine equation

$$c_1x_1 + \dots + c_kx_k = dm \tag{4}$$

has a solution (x_1, \dots, x_n) with all $x_i > \frac{m}{q}$ for some $q = q(c_1, \dots, c_k)$. Thus each x_i is “big”. It then follows that each C_i has at least one circuit of length c_ix_i starting from an arbitrarily given vertex. This is clear if C_i is a simple cycle, otherwise we use Lemma 7.5. Again by Lemma 7.5 C_1 has exponentially many circuits of length c_1x_1 . Concatenating these circuits along θ we obtain exponentially many paths from a to b of length $dm + T(\theta, a, b)$. QED

Reasoning as in Corollary 7.8 and Corollary 7.9 we obtain.

Corollary 8.3 • *If G_θ has an exponential vertex, then $\max(G_\theta^n) \geq 2^{n/q}$ for some $q = q(G_\theta)$.*

• $n \mapsto (G_\theta^n)$ is Δ_0 -definable.

For later purposes we need:

Proposition 8.4 *Let $(a, b) \in E(G)$ be a permanent edge of G . There is a number $q = q(G)$ such that for all sufficiently large n there is a path of length n which crosses the edge (a, b) at least n/q times.*

Proof. Reason as in Theorem 8.2. QED

9 Δ_0 -definition of A^n in the general case

Let k be a positive integer. If G is a 0,1 matrix of dimension k , then by Theorem 5.2, Corollary 6.4 and Corollary 8.3, we have:

Theorem 9.1 $n \mapsto G^n$ is Δ_0 definable.

Since there are only finitely many $0, 1$ matrices G of dimension k , also the map $G, n \mapsto G^n$ is Δ_0 definable. Now let us consider a $k \times k$ matrix A with non-negative integer entries.

Definition 9.2 Let $G = G(A)$ be the $0, 1$ -matrix defined by $G_{a,b} = 1$ if $A_{a,b} \neq 0$ and $G_{a,b} = 0$ if $A_{a,b} = 0$. We identify G with a graph as usual.

In the sequel G is the graph $G(A)$. We can think of A as the graph G plus a weight assigned to its edges. The edge (a, b) has weight $A_{a,b}$. Each path σ of length n in G can be written as a concatenation of n edges $\sigma = e_1 e_2 \dots e_n$ (not necessarily distinct), and its weight $w(\sigma)$ is then defined as the product of the weights $w(e_i)$ of its edges. We have the following combinatorial interpretation of A^n .

Remark 9.3 $(A^n)_{a,b}$ is the sum of the weights of the paths $\sigma: a \rightarrow b$ of length n .

Remark 9.4 $(A^n)_{a,b} = 0$ iff $(G^n)_{a,b} = 0$.

We will generalize to A^n the results about G^n .

Definition 9.5 Given $\theta \in S(G, a, b)$ we define A_θ as the matrix whose (a, b) -entry is $(A_\theta)_{a,b} = A_{a,b}(G_\theta)_{a,b}$. (This is the product of two numbers, not two matrices.)

So $(A_\theta)_{a,b}$ is either $A_{a,b}$ or zero. Theorem 5.2 can be easily generalized as follows.

Theorem 9.6 $(A^n)_{a,b} = \sum_{\theta \in S(G, a, b)} (A_\theta^n)_{a,b}$

Definition 9.7 Let $G = G(A)$ and $\theta \in S(G, a, b)$. The matrix A is called a (θ, a, b) -**matrix** if $A = A_\theta$.

Definition 9.8 A **reduced (θ, a, b) -matrix** is a (θ, a, b) -matrix A such that $A_{i,j} = 1$ for every transitory edge (i, j) of G_θ .

Lemma 9.9 For every (θ, a, b) -matrix A there is a reduced (θ, a, b) -matrix R and a number $T_{a,b}$ such that for every $n \in \mathbf{N}$ we have $(A^n)_{a,b} = (R^n)_{a,b} T_{a,b}$.

Proof. Define R as the matrix obtained from A by replacing $A_{i,j}$ with 1 whenever (i, j) is a transitory edge of G_θ . Define $T_{a,b}$ as the product of the weights of the transitory edges crossed by θ . To see that this works it suffices to recall the combinatorial interpretation of A^n together with the observation that each path $\sigma: a \rightarrow b$ in G_θ crosses the transitory edges of G_θ exactly once. QED

Note that the array of numbers $T_{a,b}$ form a nilpotent matrix T .

Lemma 9.10 *Let A be a reduced (θ, a, b) -matrix and suppose $m = \max A > 1$. There is a number q depending only on G , such that for all sufficiently large n , $\max A^n \geq m^{n/q}$.*

Proof. Let $A_{a,b} = m$. Since $m > 1$ and A is reduced, (a, b) is a permanent edge of θ . Now apply Proposition 8.4. QED

Theorem 9.11 *$A, n \mapsto A^n$ is Δ_0 -definable.*

Proof. By Theorem 9.6 and Lemma 9.9 we can assume that A is reduced. If A is a 0, 1-matrix we apply Theorem 9.1. Otherwise we apply Lemma 9.10 and Theorem 2.1. QED

Question 9.12 Does the Theorem extend to the case of matrices with entries in \mathbf{Z} ? The difficulty with negative numbers is that a sum of functions with Δ_0 graph does not necessarily have the same property.

10 Formalization in $\mathbf{I}\Delta_0$

We have proved that there is a Δ_0 formula $\phi(A, n, B)$ in $k^2 + 1 + k^2$ variables such that $A^n = B$ iff $\mathbf{N} \models \phi(A, n, B)$. In fact, we have not explicitly written down this formula. The reader who has followed the previous sections, is in position to do this in details. A careful formalization should give us a proof of the following conditions inside $\mathbf{I}\Delta_0$ (we have verified most of the details, they are available upon request to the authors). Matrix variables such as A, B etc. denote the corresponding array of k^2 variables. We write $A \leq B$ for $\max A \leq \max B$.

(1) **Functionality:** for every A and n there is at most one B s.t. $\phi(A, n, B)$;

- (2) **Base:** $\phi(A, 0, I)$, where I is the identity matrix;
- (3) **Recursive equation:** $\phi(A, n, B) \rightarrow \phi(A, n + 1, BA)$;
- (4) **invertibility conditions:** there exists a fixed number k_1 which depends only on k such that:
 $\forall n > k_1 (\phi(A, n, B) \rightarrow \bigvee_{1 \leq j \leq k_1} ((\exists B' \leq B) \phi(A, n - j, B')))$;

These conditions ensure the unicity. If $\phi_1(A, n, B)$ is another Δ_0 formula satisfying them, then it is provably equivalent to $\phi(A, n, B)$ inside $\text{I}\Delta_0$ (reason by Δ_0 -induction on a code of the pair $(n, \max B)$). It is not entirely clear whether unicity will hold if we replace the invertibility conditions with the condition $\phi(A, n + 1, B) \rightarrow \exists B' \leq p(B) \phi(A, n, B')$, where p is a fixed polynomial depending only on the dimension k of the matrices. In the case of exponentiation of natural numbers $x, y \mapsto x^y$ this alternative form of the invertibility condition ensures the unicity (see [D]) because exponentiation, unlike matrix iteration, is always increasing.

The difficulty in the proof of the conditions is that we are using a combinations of two methods, namely the Turing predicate and counting the number of solution of diophantine equations. To formalize the latter part we use the fact that the formulas involved in Lemma 4.2 are very simple, namely polynomials with rational coefficients and congruences modulo some standard integers (ultimately depending only on the structure of the graph associated to the matrix). Now a simple conservativity argument works: if an identity between two polynomial expressions is true in the standard model, then it is true in all models of $\text{I}\Delta_0$.

References

- [AHU] A. V. Aho, J. E. Hopcroft and J. D. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, Reading, Massachusetts, 1974.
- [B] J. H. Bennett, *On Spectra*, Ph.D. dissertation, Princeton University, 1962.
- [BD] A. Berarducci and P. D'Aquino, " Δ_0 -complexity of the relation $y = \prod_{i \leq n} F(i)$ ", *Annals of Pure and Applied Logic*, vol. 75, 1995, pp. 49–56.
- [BI] A. Berarducci and B. Intrigila, "A note on coding techniques in Δ_0 ", *Rapporto Matematico n. 231*, Dipartimento di matematica, Siena, 1991.
- [BI2] A. Berarducci and B. Intrigila, "Combinatorial principles in elementary number theory", *Annals of Pure and Applied Logic*, vol.55, 1991,

pp. 35–50.

[Bu] S. R. Buss, *Bounded Arithmetic*, Bibliopolis, Napoli, 1986.

[D] P. D’Aquino, “Local behaviour of Chebyshev’s Theorem in models of $I\Delta_0$ ”, *Journal of Symbolic Logic*, vol. 57, n. 1, 1992, pp. 12–27.

[G] H. Gupta, *Selected topics in number theory*, Abacus Press, 1980.

[GD] H. Gaifman and C. Dimitracopoulos, “Fragments of Peano’s Arithmetic and the MRDP theorem”, in: *Logic and Algorithmic*, Geneve, 1982, pp. 187–296.

[GKP] R. L. Graham, D. Knuth and O. Patashnik, *Concrete mathematics*, Addison-Wesley, Reading, 1989.

[K] R. Kaye, *Models of Peano Arithmetic*, Oxford University Press, Oxford, 1991.

[P] P. Pudlák, “A definition of exponentiation by a bounded Arithmetical formula”, *Commentationes Mathematicae Universitatis Carolinae*, Vol. 24, n. 4, 1983, pp. 667–671.

[PW] A. J. Wilkie and J. B. Paris, “On the scheme of induction for bounded arithmetical formulas”, *Annals of Pure and Applied Logic*, vol. 35, 1987, pp. 261–302.

[PWW] J. B. Paris, A. J. Wilkie and A. R. Woods, “Provability of the pigeonhole principle and the existence of infinitely many primes”, *Journal of Symbolic Logic*, vol. 53, n. 4, 1988, pp. 1235–1244.

[S] J. C. Shepherdson, “A non-standard model for a free variable fragments of number theory”, *Bullettin de l’Academie Polonaise des Sciences, Séries des sciences math., astr. et phys.*, vol. XII, n. 2, 1964, pp. 79–86.

[W] A. R. Woods, *Some problems in logic and number theory and their connections*, Ph.D. Thesis, University of Manchester, Manchester, 1981.

[WI] A. J. Wilkie, Review of “S. Buss, Bounded arithmetic”, *Journal of Symbolic Logic*, vol. 56, n. 2, 1991, pp. 759–760.