Commentationes Mathematicae Universitatis Carolinae

Pavel Pudlák

A definition of exponentiation by a bounded arithmetical formula

Commentationes Mathematicae Universitatis Carolinae, Vol. 24 (1983), No. 4, 667--671

Persistent URL: http://dml.cz/dmlcz/106264

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE
24,4 (1983)

A DEFINITION OF EXPONENTIATION BY A BOUNDED ARITHMETICAL FORMULA

Pavel PUDLÁK

Abstract: A new definition of exponentiation by a bounded arithmetical formula is presented.

Key words: Exponentiation, bounded arithmetical formula.

Classification: 03F30

It was shown by Gödel that the relation $z = x^y$ can be defined using only + and • . In complexity theory and also for investigations of weak fragments of arithmetic it is very useful to have definitions by <u>bounded arithmetical formulae</u>, i.e. arithmetical formulae in which every quantification is of the form $\exists x \leq y$ or $\forall x \leq y$, where y is some free variable of the formula. Once we have a definition of exponentiation by a bounded formula, we can easily construct such definitions for a variety of other concepts. The first definition of $z = x^y$ by a bounded formula was found by Bennet [1], another formula was constructed by Paris, see [2]. Since so far there is no known simple definition of exponentiation, by a bounded formula, it seems reasonable to look for alternative definitions. Another such definition is presented here.

Let $P(x)$, $x|y$ be the obvious bounded formulae defining "x is a prime", "x divides y" resp. We shall also use the abbreviation

$$\mu x\, \varphi(x)$$

for a bounded formula

$$\varphi(x) \,\&\, \forall y < x \neg \varphi(y).$$

It is enough to define $z = x^y$ only for x prime since then we obtain a general definition by

$$\mu z\, \forall p,k(P(x) \,\&\, p^k | x \longrightarrow p^{ky} | z).$$

Also we can restrict ourselves to sufficiently large exponents, since for a fixed exponent the definition is trivial. The formula is constructed in three steps.

1. $PP(p,a) \longleftrightarrow_{df} \forall q \leq a \; (q | a \longrightarrow q = 1 \vee p | q)$

2. $E(p,k,a,b) \longleftrightarrow_{df}$

   $\mu b(PP(p,a) \,\&\, PP(p,b) \,\&\, (\exists u \leq b)(b = (a-1) \cdot [(a-1) \cdot u + k] + 1))$

3. $\mathrm{Exp}\ (p,k,e) \longleftrightarrow_{df} (\exists m,n,a,b,c,d, \leq e^2)(e = b \cdot c \,\&$

   $\& \, k = n + m^2 \,\&\, n \leq 2 \cdot m < a - 1 \;\&$

   $E(p,m,a,c) \,\&\, E(p,m,p \cdot a,\ a \cdot c) \;\&$

   $E(p,n,a,d) \,\&\, E(p,n,p \cdot a, b \cdot d)).$

<u>Theorem</u>. For p prime, $k \geq 9$ and e arbitrary, Exp(p,k,e) iff $p^k = e$.

Proof: Let p be a prime number.

1. Clearly PP(p,a) iff a is a power of p.

2. If a and b are some powers of p then b is a power of a iff $a-1 | b-1$, just imagine the p-adic representations of a, b, a-1, b-1. Therefore if E(p,k,a,b) then b is a power of a. We shall show that for $k < a-1$, E(p,k,a,b) iff $a^k = b$.

By the remark above it is enough to consider only b's which are powers of a. Let $b = a^m$. Using binomial expansion of $((a-1)+1)^m$ we can represent b uniquely as

$$b = (a-1)\ [(a-1)\ u + n] + 1,$$

with $n < a-1$. Moreover we have $n \equiv m \bmod (a-1)$. Hence a^k is the smallest power of a such that

$$a^k = (a-1)\ [(a-1)\ u+k] + 1.$$

3. Suppose $Exp(p,k,e)$ holds true. Then using 2 we can replace the last four clauses by

$$a^m = c,\ (p.a)^m = a.c,\ a^n = d,\ (p.a)^n = b.d.$$

The first two of them imply $a = p^m$, hence $c = p^{m^2}$; the last two imply $b = p^n$, Hence

$$e = b.c = p^n\ .\ p^{m^2} = p^{n+m^2} = p^k.$$

Now suppose $p^k = e$. Then, clearly, $e = p^n\ .\ p^{m^2}$ for some m, n such that $k = n + m^2$ and $n \leq 2m$. To obtain $Exp(p,k,e)$ one needs only to check that $2m < a - 1$, where $a = p^m$, which is true if $m \geq 3$, hence if $k \geq 9$. The largest of the quantified numbers is $d = a^n = p^{mn} \leq p^{2m^2} \leq e^2$, Q.E.D.

The proof above was done in the standard model of arithmetic. If we use such a formula in a weak fragment of arithmetic, we would like to be able to prove that it defines exponentiation there. But what does it mean? A natural formalization of this requirement is that the theory proves the inductive conditions:

$$1 = x^0,\ z = x^y \longrightarrow x\ .\ z = x^{y+1}.$$

It has been conjectured that for some of the definitions of exponentiation by a bounded formula the conditions are provable using only bounded induction. The formula presented here may seem not to have this property, since in the critical part of the proof we referred to p-adic representation and binomial expansion. However, this was done only for the sake of simplicity of the proof, and we conjecture that our formula is a right one.

It would be a really tedious work to check it formally, therefore we consider the inductive conditions only for the formula $E(p,k,a,b)$. First we need the following lemma.

<u>Lemma</u>. $c>1 \,\&\, c|a.b \longrightarrow \exists s[s>1 \,\&\, s|c \,\&\, (s|a \vee s|b)]$ is provable using only bounded induction.

Proof: Let $A(a,b,c)$ denote the formula above. Using induction we prove $\forall n\, B(n)$ where $B(n)$ denotes the following bounded formula

$$\forall a,b,c\, [a.b+c \leq n \longrightarrow A(a,b,c)].$$

$B(0)$ is trivial. Assume $B(n)$ and let $a.b+c \leq n+1$, $c>1$, $c|a.b$.

1. If $c \leq a$ then $c|(a-c).b < a.b$, hence by the induction assumption there exists $s>1$, $s|c$ such that $s|(a-c)$ or $s|b$. Thus also $s|a$ or $s|b$.

2. The case of $c \leq b$ is symmetrical.

3. Suppose $c>a$ and $c>b$. Let d be such that $c.d = a.b$, then $d<c$. By the induction assumption there exists $s'>1$, $s'|d$ such that $s'|a$ or $s'|b$. Because of symmetry we can investigate only the case of $s'|a$. Let a', d' be such that $a'.s' = a$, $d'.s' = d$. Then $c.d' = a'.b < a.b$, and we can use the induction assumption again to obtain $s>1$, $s|c$ such that $s|s'$ or $s|b$, whence $s|a$ or $s|b$. Q.E.D.

<u>Proposition</u>. $P(p) \,\&\, E(p,k,a,b) \longrightarrow E(p,k+1,a,a.b)$ is provable using only bounded induction.

Proof: Assume the antecedent of the implication, i.e. $PP(p,a)$, $PP(p,b)$ and b is minimal such that

$$b = (a-1).\,[(a-1).u+k] + 1,$$

for some u. Then

$$a.b = (a-1).\,[(a-1).(a.u+k)+k+1] +1,$$

hence $a.b$ has the required form. If $c>1$ and $c|a.b$ then, by

Lemma, for some $s > 1$,

$$s|c \,\&\, (s|a \vee s|b).$$

Since $PP(p,a)$ and $PP(p,b)$, we have $p|s$, hence $p|c$.

Thus we have proved $PP(p,a.b)$. It remains to prove the minimality of $a.b$. Suppose $c < a.b$ has these properties. Then $c \geq a$ and since $PP(p,c)$ we have $a|c$, (consider g.c.d. of a and c). Let $c = a.d$, thus

$(*)$ $a.d = (a-1).\,[(a-1).v+k+1] +1 = a^2.v+a.(k+1-2v)+v-k,$

for some v. Hence $v-k = t.a$ for some t. If we substitute $v = t.a+k$ in $(*)$ and divide it by a, we get, after some computation,

$$d = (a-1).\,[(a-1).t+k] +1.$$

Also $PP(p,d)$ can be shown easily. But $a.d = c < a.b$, so $d < b$. Thus b is not minimal - contradiction. This proves that $a.b$ is minimal. Q.E.D.

References

[1] BENNETT, J.H.: On Spectra, Ph.D. dissertation, Princeton University 1962.

[2] GAIFMAN, H. and DIMITRACOPOLOUS C.: Fragments of Peano´s arithmetic and the MRDP Theorem, in Logic and Algorithmic, Genève 1982, 187-206.

Matematický ústav ČSAV, Žitná 25, Praha 1, Czechoslovakia.

(Oblatum 20.9. 1983)