

A NEW REPRESENTATION FOR THE SYMMETRIC
BINOMIAL COEFFICIENT AND ITS APPLICATIONS
J.P. Jones and Ju.V. Matijasevič

Résumé

En 1961, M. Davis, H. Putnam et J. Robinson ont démontré que tout ensemble récursivement énumérable est défini par une équation diophantienne pouvant comporter la fonction exponentielle. De façon plus précise, tout ensemble récursivement énumérable a peut se définir par $n \in A$ si et seulement si

$\exists x_1, x_2, \dots, x_v (P(n, x_1, \dots, x_v) = Q(n, x_1, \dots, x_v))$, dans laquelle P et Q sont des fonctions d'entiers naturels obtenues à partir des opérations d'addition de multiplication et d'exponentiation. En 1979, ce résultat fut amélioré par Ju.V.

Matijasevič qui a prouvé que trois inconnues x_1 , x_2 et x_3 suffisent (i.e. $v = 3$) et que la représentation est univoque (uni-pli): c'est-à-dire, la solution x_1 , x_2 , x_3 est unique pour $n \in A$. En anglais, cette représentation est appelée "singlefold", en russe, "odno-kratno".

Dans le présent travail, ce résultat est encore amélioré. Nous démontrons que tout ensemble énumérable peut être représenté par une inégalité

$\exists z, y [P(n, z, y) \leq Q(n, z, y)]$, dans lequel z et y sont des entiers uniques (représentation uni-pli), P et Q sont des fonctions d'entiers naturels définies à partir des opérations d'addition, de multiplication et de l'exponentielle 2^x (en base 2). Ceci implique une forme forte du théorème initial ci-dessus des trois inconnues car ici l'exponentiation x^y sous sa forme générale n'apparaît que sous la forme 2^x . De plus, on montre que deux itérations de l'exponentielle suffisent, i.e. 2^{2^x} .

Des résultats connexes et variés sont démontrés: un ensemble énumérable a une représentation sous la forme $\exists z, \forall y [R(n, z, y) \leq S(n, z, y)]$, dans laquelle R et S sont obtenus à partir de l'addition, de la multiplication et de l'exponentielle en base 2.

On montre aussi qu'une relation élémentaire de Kalmar a aussi une représentation, avec une variable (que l'on peut supposer bornée), i.e. sous les formes $\exists y [P(n, y) \leq Q(n, y)]$ et $\forall y [R(n, y) \leq S(n, y)]$; et donc sous les formes $\exists y, x [P(n, y, x) = Q(n, y, x)]$ et $\forall y, \exists x [R(n, y, x) = S(n, y, x)]$ (où les quantificateurs sont bornés). Ces énoncés caractérisent les relations élémentaires de Kalmar. Les nombres premiers forment un ensemble élémentaire de Kalmar, il s'en suit que l'ensemble des nombres premiers possède une représentation sous la forme ci-dessus.

In 1961, it was shown that every recursively enumerable set is exponential diophantine. M. Davis, H. Putnam and Julia Robinson [1961] proved that each r.e. predicate, $W(a)$ could be represented in the form

$$\exists x_1, \dots, x_v [P(a, x_1, \dots, x_v) = Q(a, x_2, \dots, x_v)] \quad (1)$$

where P and Q are functions obtained from natural numbers and variables by the operations of addition, multiplication and exponentiation, the unknowns $x_1, x_2, \dots, x_v$ range over natural numbers.

In the paper of Matijasevič [1974] (cf. also Matijasevič [1976]) this result was improved to show that each r.e. set has a singlefold exponential diophantine representation, i.e. one in which $x_1, \dots, x_v$, when they exist, are unique. For each value of the parameter a there is one and only one solution in the unknowns $x_1, \dots, x_v$.

In the paper of Matijasevic [1979] this result was further improved to the effect that there is always a singlefold exponential diophantine representation in only three unknowns, i.e. every r.e. set can be represented in the form (suppress-

ing the parameter)

$$\exists x, y, z [P(x, y, z) = Q(x, y, z)] . \quad (2)$$

Here P and Q are functions obtained from natural numbers and variables, x, y, z by addition, multiplication and exponentiations of type u^v in two variables, and x, y and z , when they exist, are unique natural numbers.

In the present paper this representation will be further improved. The number of unknowns is the same, three, but we will prove that P and Q can always be obtained from natural numbers and variables x, y, z using only the operations of addition, multiplication and exponentiations of type p^v where the base is a fixed prime p . In fact we will show that we can take $p = 2$. We call such exponential diophantine expressions *unary*, since p^v is a one place function of v whereas u^v is a two place function. As in Matijasevič [1979] we permit iteration of exponentiations, p^v, p^{p^v} , etc. We prove

THEOREM 1. Every recursively enumerable set can be represented in the form

$$\exists z \exists y [P(z, y) \leq Q(z, y)]$$

where P and Q are unary exponential diophantine expressions. Furthermore the representation is singlefold and the second quantifier, $\exists y$ may be bounded.

From Theorem 1 it follows that every r.e. set can be singlefold represented in the form $\exists z \exists y \exists x [P(z, y, x) = Q(z, y, x)]$. Here P and Q are unary iterated exponential functions of z, y and x . The variables z, y and x range over natural numbers and they are unique whenever they exist. We may also suppose further that y and x are less than some bound where the bound takes the form of a unary iterated exponential function of the first unknown z . We will also prove

THEOREM 2. Every r.e. set can be represented in the form $\exists z \forall y [R(z, y) \leq S(z, y)]$ where R and S are unary exponential expressions. Here the

universal quantifier, $\forall y$ may be bounded if we wish.

The representations of Theorems 1 and 2 are best possible both in terms of the number of quantifiers and the bounds. One cannot delete any quantifiers or bound the first quantifier, $\exists z$. (However we do not know if the representation $\exists z, y, x [P(z, y, x) = Q(z, y, x)]$ is best possible in terms of the number of quantifiers.)

Suppose we replace "r.e." by "recursive" in Theorems 1 and 2. Then one might expect to be able to bound all the quantifiers. However a simple diagonal argument shows that this is not the case. (See Davis, Matijasevič, Robinson [1976].) The same argument also shows that also in this case one cannot delete any quantifiers.

In the case of certain particular recursive sets we may be able to delete a quantifier. We will show that this is in fact the case for primes, Mersenne primes, perfect numbers and certain other recursive sets occurring in classical number theory. These sets are all particular examples of Kalmar Elementary Sets. For this type of set we will prove we can delete the quantifier $\exists z$ from Theorems 1 and 2.

THEOREM 3. Every Kalmar elementary relation is representable in both of the forms

$$\exists y [P(y) \leq Q(y)] \quad \text{and} \quad \forall y [R(y) \leq S(y)] .$$

Here P , Q , R and S are unary exponential diophantine expressions. Furthermore y can be bounded in both cases.

Theorem 3 implies immediately the following.

THEOREM 4. Every Kalmar elementary relation is representable in both the forms

$$\exists y \exists x [P(y, x) = Q(y, x)] \quad \text{and} \quad \forall y \exists x [R(y, x) = S(y, x)]$$

where P , Q , R and S are unary exponential diophantine expressions. Here all the quantifiers may be bounded if we wish.

As a corollary of Theorem 4 we see that the sets of prime numbers, Mersenne primes and perfect numbers can be represented in each of the above forms.

We do not know if these forms are best possible. Certainly in at least one interesting case it is possible to do better. The set of Fermat primes can be exponentially defined in only one unknown, i.e. it is possible to construct exponential expressions $P(n,x)$ and $Q(n,x)$ such that for all natural numbers

$$n \text{ is a Fermat prime} \iff \exists x [P(n,x) = Q(n,x)] . \quad (3)$$

For details of how to construct P and Q , cf. Jones [1979], Lemma 4.3.

With the understanding that the quantifiers are bounded, the converses of Theorems 3 and 4 are also trivially true. Hence these theorems provide four new characterizations of the Kalmar elementary sets. These bounds take the form of unary iterated exponential functions of the parameters. In the terminology of Davis, Matijasevič, Robinson [1976] such $\exists$ quantifier bounds are referred to as "iterated exponential test functions". Further information about Kalmar elementary sets and functions is given in §2. There we give several new examples of bases for these sets and an improvement of a theorem of C.C. Marchenkov [1980].

§1. Theorem 1 will be proved from the following lemma. In the course of the proof of this lemma, it will be shown how to modify P and Q to obtain Theorem 2. It will then be clear how to prove Theorems 3 and 4, from the results in §2.

LEMMA 1. For any polynomial equation

$$D(w_1, w_2, \dots, w_v) = 0 , \quad (4)$$

there exist unary exponential diophantine functions $P(z,y)$ and $Q(z,y)$ such that (4) has a solution if and only if there exist (unique) natural z and y

such that

$$P(z,y) \leq Q(z,y) . \quad (5)$$

The proof of Lemma 1 (and hence Theorem 1) will use methods developed by Matijasevič [1979] together with the following generating function for the symmetric binomial coefficient $\binom{2n}{n}$.

$$\text{LEMMA 2. } \frac{1}{\sqrt{1-4x}} = \sum_{n=0}^{\infty} \binom{2n}{n} x^n, \quad |x| < \frac{1}{4} .$$

PROOF of Lemma 2. By the binomial series

$$(1-4x)^{-\frac{1}{2}} = \sum_{n=0}^{\infty} \binom{-1/2}{n} (1-4x)^n$$

together with the identity

$$\begin{aligned} \binom{-1/2}{n} (-4)^n &= \frac{(-1/2)(-3/2)\dots(-1/2-n+1)}{n!} (-2)^n 2^n = \frac{1 \cdot 3 \cdot 5 \dots (2n-1)}{n!} \\ &= \frac{1 \cdot 2 \cdot 3 \cdot 4 \dots (2n-1) \cdot (2n)}{n! n!} = \binom{2n}{n} . \end{aligned}$$

Of course Lemma 2 may also be proved by considering the ordinary Taylor series expansion of $f(x) = (1-4x)^{-\frac{1}{2}}$ about $x = 0$. One proceeds to show that the n^{th} derivative of $f(x)$, $f^n(x) = 2(2n-1)f^{n-1}(x)$ from which it follows that $f^n(x) = (2n)!/n!$.

Now replace x by $1/u$ in Lemma 2 and multiply by u^n to obtain the series (valid for $|u| > 4$)

$$\frac{u^n}{\sqrt{1-4/u}} = u^n + 2u^{n-1} + 6u^{n-2} + \dots + \binom{2n-2}{n-1}u + \binom{2n}{n} + \sum_{k=1}^{\infty} \binom{2n+2k}{n+k} u^{-k} . \quad (6)$$

We may use a geometric series to estimate the size of the fractional part of (6),

$$\sum_{k=1}^{\infty} \binom{2n+2k}{n+k} u^{-k} < \sum_{k=1}^{\infty} 2^{2n+2k} u^{-k} = \frac{4 \cdot 4^n}{u-4} . \quad (7)$$

The series (6) gives a direct formula for the symmetric binomial coefficient in terms of the remainder function, namely

$$\binom{2n}{n} = \text{rem}\left(\left\lceil \frac{u^n}{\sqrt{1-4/u}} \right\rceil, u\right) \quad (\text{whenever } 4 \cdot 4^n + 4 < u) . \quad (8)$$

In the paper of Matijasevič [1979] certain exponential diophantine functions $M(z)$ and $A(z)$ were constructed so that our original equation (4) has a solution in non-negative integers $z_1, \dots, z_v$ if and only if there exists a unique natural number z such that

$$2^{M(z)} \mid \binom{2A(z)}{A(z)} . \quad (9)$$

If 2^M divides u then condition (9) may be rewritten in the form

$$2^M \mid \left\lceil \frac{u^A}{\sqrt{1-4/u}} \right\rceil . \quad (10)$$

For $8 \cdot 4^A + 4 < u$ this condition (10) may be rewritten in the form that for some (unique) natural number y

$$\left| \frac{u^A}{\sqrt{1-4/u}} - 2^M y \right| \leq \frac{1}{2} . \quad (11)$$

Then the condition (11) may be further rewritten in the form that there exists a (unique) y such that

$$\left| \frac{\frac{u^{2A}}{1-4/u} - 2^{2M} y^2}{2^{M+1} y} \right| \leq \frac{1}{4} . \quad (12)$$

The condition (12) is in turn equivalent to the following condition

$$2 \left| \frac{u^{2A}}{1-4/u} - 2^{2M} y^2 \right| \leq 2^M y , \quad (13)$$

which is in turn equivalent to the condition

$$4 \left(\frac{u^{2A+1}}{u-4} - 2^{2M} y^2 \right)^2 \leq 2^{2M} y^2 , \quad (14)$$

which is in turn equivalent to the condition

$$4(u^{2A+1} - 2^{2M} y^2 (u-4))^2 \leq 2^{2M} y^2 (u-4)^2 . \quad (15)$$

Now (15) can be rewritten in the form

$$4(u^{2A+1} + 4 \cdot 2^{2M} y^2)^2 + 4 \cdot 2^{4M} y^4 u^2 + 4 \cdot 2^{2M} y^2 \leq u 2^{2M} y^2 (32 \cdot 2^{2M} y^2 + 8u^{2A+1} + 1) . \quad (16)$$

Now the functions $M(z)$ and $A(z)$ defined in Matijasevič [1979] are such that $M(z)$ is of unary exponential diophantine form and $A(z)$ is such that

$$2A + 1 = \frac{E_1 - E_2}{E_3 - E_4} \quad (17)$$

where E_1, E_2, E_3 and E_4 are unary exponential diophantine functions, and, for all values of z , $E_3(z) > E_4(z)$.

Put

$$u = 2^{(2E_1+4M)(E_3-E_4)} . \quad (18)$$

Then U has the required and properties, namely

$$2^M \mid u \text{ and } 8 \cdot 4^A + 4 < u . \quad (19)$$

Also u and u^{2A+1} may be written in the form

$$u = 2^{E_5-E_6} \text{ and } u^{2A+1} = 2^{E_7-E_8} \quad (20)$$

where E_5, E_6, E_7 and E_8 are unary exponential functions of z .

Hence inequality (16) may be replaced by

$$\begin{aligned} & 4(2^{E_7-E_8} + 4 \cdot 4^M y^2)^2 + 4 \cdot 16^M y^4 2^{E_5-E_6} + 4 \cdot 4^M y^2 \\ & \leq 2^{E_5-E_6} 4^M y^2 (32 \cdot 4^M y^2 + 8 \cdot 2^{E_7-E_8} + 1) . \end{aligned} \quad (21)$$

Now multiply both sides of (21) by $4^{E_6+E_8}$ to obtain

$$\begin{aligned} & 4(2^{E_7} + 4 \cdot 4^M y^2 2^{E_8})^2 4^{E_6} + 4 \cdot (16)^M y^4 2^{E_5+E_8} + 4 \cdot 4^M y^2 4^{E_6+E_8} \\ & \leq 2^{E_5+E_6+E_8} 4^M y^2 (32 \cdot 4^M y^2 2^{E_8} + 8 \cdot 2^{E_7} + 2^{E_8}) . \end{aligned} \quad (22)$$

This proves Lemma 1. The unary exponential diophantine functions $P(z,y)$ and $Q(z,y)$ are given in (22). For the desired three unknown representation we may use the equation

$$P(z,y) + x = Q(z,y) . \quad (23)$$

Equation (23) has exactly one solution in natural numbers x,y,z when the initial equation (4) has a solution in natural numbers $w_1, \dots, w_v$. In the other case, when (4) has no solution, then equation (23) also has no solution in x, y and z .

Note that in equation (23) the unknowns x and y do not appear in the exponents, only the unknown z appears in the exponents.

By essentially the same method we can derive also the representation of Theorem 2.

LEMMA 3. For any polynomial $D(w_1, \dots, w_v)$ we can construct unary exponential diophantine functions $R(z,y)$ and $S(z,y)$ such that $D = 0$ has a solution in $w_1, \dots, w_v$ if and only if

$$\exists z \forall y (R(z,y) \leq S(z,y)) . \quad (24)$$

PROOF of Lemma 3. If we redefine the functions $A(z)$ and $M(z)$ of Matijasevič [1979] by

$$A'(z) = B^-(z, z) \quad (25)$$

and

$$M'(z) = z^{v-1}(T(z) + 2S(z)) - R(z) + S(z) + 1 \quad (26)$$

then we may replace condition (27) of Matijasevič [1979] by $\sigma(A'(z)) < M'(z)$ so that (9) becomes

$$2^{M'(z)} \nmid \binom{2A'(z)}{A'(z)} . \quad (27)$$

If as before $2^{M'}$ divides u , then (9) may be rewritten in the form

$$2^{M'} \nmid \left[\frac{U^{A'}}{\sqrt{1-4/u}} \right], \quad (28)$$

and if again U is large enough that (19) holds, then (28) may be rewritten in the form that, for all y ,

$$\left| \frac{U^{A'}}{\sqrt{1-4/u}} - 2^{M'} y \right| > \frac{1}{2}. \quad (29)$$

Now inequality (29) is exactly inequality (11) with the sign, $\leq$ reversed to $>$. Since inequality (11) was equivalent to inequality (12), inequality (29) is equivalent to (12) with sign reversed. Continuing in this way through (13), (14), (15), (16), (21), (22) we find that for $R(z,y)$ and $S(z,y)$ in (24) we may take $S = P'(z,y)$ and $R(z,y) = Q'(z,y) + 1$ where $P'(z,y)$ and $Q'(z,y)$ are essentially the same as $P(z,y)$ and $Q(z,y)$ in (22) but with different E_6 's due to the changes in $M(z)$ and $A(z)$. (In this case $M(z)$ is not unary exponential diophantine. However it becomes so after replacing z by $z+1$.) This completes the proof of Lemma 3. Note that the universal y quantifier in (24) may be taken to be bounded. By (6), we may suppose that $y < (1+u)^{2E_1} < a$ unary exponential diophantine function of z .

§2. Applications to the theory of Kalmar elementary functions

A. Grzegorzcyk [1953] asked the following question. Is it possible to give a finite basis for the set K of Kalmar elementary functions? i.e. can one find a finite set of initial functions from which all others may be obtained by composition? Under composition we permit also closely related operations such as substitution of natural numbers for variables as well as permutation and identification of variables.

Grzegorzcyk's question was answered affirmatively by D. Rødding [1964]. Subsequently various other authors made further progress, e.g. Ch. Parsons [1968] and C.C. Marchenkov [1980]. Marchenkov considered also the closely related class

of Kalmar elementary relations, the relations whose characteristic functions belong to the class K . Marchenkov [1980], Theorem 2, proves that the set

$$M = \{x + 1, x \dot{-} y, [x/y], x^y\} \quad (30)$$

is a basis for the Kalmar elementary relations. We give here various other bases for these relations. The first of these is given in

THEOREM 5. Every Kalmar elementary relation belongs to the closure of the following class

$$M_1 = \{x + y, x \dot{-} y, [x/y], [\sqrt{x}], 2^x\}. \quad (31)$$

Here Marchenkov's exponential function x^y of two variables has been replaced by two functions, each of one variable. Unfortunately it was also necessary to replace $x+1$ by $x+y$ since closure M_1 would otherwise contain no function $f(x,y)$ with the property that $x \leq f(x,y)$ and $y \leq f(x,y)$ and hence not even contain the function $x+y$.

First we prove a lemma, then Theorem 5 and then we give further examples of bases for Kalmar elementary relations.

LEMMA 4. Each of the functions x^2 , $x \cdot y$, $[\frac{\sqrt{x}}{\sqrt{y}}]$, $\text{rem}(y,x)$ and $\binom{2x}{x}$ belongs to the compositional closure of the class M_1 .

PROOF.

$$x^2 = \left[\frac{2^{2^{2^x}}}{\left[\frac{2^{2^{2^x}}}{\left[\frac{x}{x} \right]} \right]} \right] . \quad (32)$$

$$y \cdot x = \left[\frac{((y+x)^2 \dot{-} y^2) \dot{-} x^2}{2} \right] . \quad (33)$$

$$\left[\frac{\sqrt{x}}{\sqrt{y}} \right] = \left[\frac{\sqrt{x}\sqrt{y}}{y} \right] = \left[\frac{\sqrt{xy}}{y} \right] = \left[\frac{[\sqrt{xy}]}{y} \right] . \quad (34)$$

$$\text{rem}(y, x) = y \dot{-} (x[y/x]) . \quad (35)$$

$$\binom{2x}{x} = \text{rem}\left(\left[\frac{2^{8x^2+4x}}{\sqrt{2^{8x+4}}}\right], 2^{8x}\right) . \quad (36)$$

Formula (36) is obtained from (8) by taking $u = 2^{8x}$.

This completes the proof of Lemma 4 (which is analogous to Marchenkov's Lemma 1). Now the idea of our proof of Theorem 5 is to replace Marchenkov's use of x^y by use of 2^x and his use of $\binom{x}{y}$ by $\binom{2x}{x}$. This could be done by following Marchenkov's [1980] argument and using Lemma 3.5 of Matijasevič [1977] in place of Matijasevič Lemma 3.1 [1977]. However we shall give here instead a different proof which is much shorter.

PROOF of Theorem 5. Let $R(x_1, \dots, x_n)$ be an arbitrary Kalmar elementary relation. By Putnam, Davis, Robinson [1961] and Matijasevic [1971] (cf. also L. Adelman and K. Manders [1975]) it is possible to find a polynomial $D(w_1, \dots, w_\nu)$ and a Kalmar function $g(x_1, \dots, x_n)$ such that

$$\begin{aligned} R(x_1, \dots, x_n) &\iff (w_1, \dots, w_\nu)[D(x_1, \dots, x_n, w_1, \dots, w_\nu) = 0] \\ &< g(x_1, \dots, x_n) . \end{aligned} \quad (37)$$

We may in fact suppose that $g(x_1, \dots, x_n)$ is an iterated exponential function of the type

$$g(x_1, \dots, x_n) = 2^{2^{\dots^{2^{x_1 + \dots + x_n}}}} \quad (38)$$

and hence that $g(x_1, \dots, x_n)$ belongs to the closure of M_1 .

Now let $T(z)$, $R(z)$, $S(z)$ and $B^+(z, w)$ be as in Matijasevič 1979 but redefine the functions $M(z)$ and $A(z)$ in the following way:

$$A(z) = \sum_{w_1=0}^{z-1} B^+(z, w_1) 2^{(2R(z)+3)z^{\nu-1}(w_1+1)} \quad (39)$$

and

$$M(z) = z^{v-1}T(z) + R(z) - S(z) . \quad (40)$$

Then using formula (21) of Matijasevič [1979] it is not difficult to see that for any value of z

$$(\exists w_1, \dots, w_v)[D(x_1, \dots, x_n, w_1, \dots, w_v) = 0] \quad (41)$$

if and only if

$$M(z) \leq \sigma(A(z)) . \quad (42)$$

Now since the equivalence of (41) and (42) holds for any value of z , we may put $z = g(x_1, \dots, x_n)$. By (37) we see that $R(x_1, \dots, x_n)$ is then equivalent to

$$M(g(x_1, \dots, x_n)) \leq \sigma(A(g(x_1, \dots, x_n))) . \quad (43)$$

Now the function $M(z)$ is unary exponential diophantine. So the function $B = M(g(x_1, \dots, x_n))$ belongs to the closure of M_1 . Also, as we have seen, there are unary exponential functions E_1, E_2, E_3 and E_4 such that $E_3 > E_4$ and $E_1 > E_2$ and $A = [E_1 \div E_2 / E_3 \div E_4]$. Hence every Kalmar elementary relation, $R(x_1, \dots, x_n)$ is represented in the form

$$B(x_1, \dots, x_n) \leq \sigma(A(x_1, \dots, x_n)) \quad (44)$$

where $A(x_1, \dots, x_n)$ and $B(x_1, \dots, x_n)$ belong to the closure of M_1 . As usual (44) can be replaced by

$$2^B \mid \binom{2A}{A} . \quad (45)$$

Then (45) can be replaced by

$$\text{rem}(\binom{2A}{A}, 2^B) = 0 . \quad (46)$$

Hence the characteristic function of the relation $R(x_1, \dots, x_n)$ can be represented in the form

$$1 \stackrel{\cdot}{=} \text{rem}(\binom{2A}{A}, 2^B) \quad (47)$$

where $A = A(x_1, \dots, x_n)$ and $B = B(x_1, \dots, x_n)$ are functions in the closure of M_1 . By Lemma 4, (47) is a function in the closure of M_1 . Hence Theorem 5 is proved.

Since the functions of M_1 belong to the closure of each of the following sets, (48) and (49), these may also be taken as a basis for the Kalmar elementary relations

$$\{x \stackrel{\cdot}{=} y, [x/y], [\sqrt{x}], 2^{x+y}\} \quad (48)$$

$$\{x \stackrel{\cdot}{=} y, [\sqrt{x/y}], x^2, 2^{x+y}\}. \quad (49)$$

Whether or not the following set, (50) is a basis, is an interesting open problem:

$$\{x \stackrel{\cdot}{=} y, [\sqrt{x/y}], 2^{x+y}\}. \quad (50)$$

It may be possible to do better here by considering other functions such as $\sigma(x)$, $\binom{2x}{x}$ or $x!$. For example it is easy to prove that the following sets (51), (52) and (53) are bases:

$$\{x + y, x \stackrel{\cdot}{=} y, [x/y], \sigma(x), 2^x\} \quad (51)$$

$$\{x + y, x \stackrel{\cdot}{=} y, [x/y], \binom{2x}{x}, 2^x\} \quad (52)$$

$$\{x + y, x \stackrel{\cdot}{=} y, [x/y], x!, 2^x\}. \quad (53)$$

REMARK. As regards functions (as opposed to relations), since every finite valued function is a finite sum of characteristic functions, Theorem 5 implies also that finite valued Kalmar elementary functions belong to the compositional closure of each of our bases.

References

- [1975] ADELMAN, L. and MANDERS, K., *Computational complexity of decision procedures for polynomials*, Proc. 16th Annual Symposium on Foundations of Comp. Science, 1975, New York, 169-177.
- [1961] DAVIS, M., PUTNAM, H. and ROBINSON, J., *The decision problem for exponential diophantine equations*, Ann. of Math. 74 (1961), 425-436 —
Matematika 8.5 (1964), 69-79.
- [1976] DAVIS, M., MATIJASEVIČ, Ju.V. and ROBINSON, J., *Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution*, Proc. Symp. on the Hilbert Problems, Dekalb, Illinois, May 1974, Amer. Math. Soc. 28 (1976), 323-378.
- [1953] GRZEGORCZYK, A., *Some classes of recursive functions*, Rozprawy matematyczne, No 4, Instytut Matematyczny Polskiej Akademii Nauk, Warsaw, 1953.
- [1975] KOSSOVSKY, N.K., *A hierarchy of diophantine representations for primitive recursive functions* (Russian), Computation techniques and questions of cybernetics, Leningrad State University, Vol. 12 (1975), 99-107.
- [1979] JONES, J.P., *Diophantine representation of Mersenne and Fermat primes*, Acta Arithmetica 35 (1979), 209-221.
- [1980] MARCHENKOV, S.S., *On a new basis whose closure under composition gives the Kalmar elementary functions* (Russian), Mat. Zam. 27 (1980), no 3, 321-331.
English translation: Math. Notes 27 (1980), 161-166.
- [1971] MATIJASEVIČ, Ju.V., *Diophantine representation of enumerable predicates* (Russian), Izvestija Akademii Nauk SSSR, Serija Matematika, Vol. 35 (1971), 3-30. English translation: Mathematics of the USSR —
Izvestija, Vol. 5 (1971), 1-28.

- [1974] MATIJASEVIČ, Ju.V., *The existence of noneffectizable estimates in the theory of exponential diophantine equations*, Zapiski Naučnyh Seminarov Leningradskogo Otdelenija Matematičeskogo Instituta im. V.A. Staklova, Akad. Nauk. SSSR 40 (1974), 77-93. English translation: Jour. Soviet Math. (Plenum Publishers), 8 (1977).
- [1976] MATIJASEVIČ, Ju.V., *A new proof of the theorem on exponential diophantine representation of enumerable sets* (Russian), Zapiski Naučnyh Seminarov Leningradskogo Otdelenija Matematičeskogo Instituta im. V.A. Steklova, Akad. Nauk. SSSR 60 (1976), 75-89. English translation: Jour. Soviet Math. 14 (1980), 1475-1486.
- [1977] MATIJASEVIČ, Ju.V., *A class of primality criteria formulated in terms of the divisibility of binomial coefficients* (Russian), Zapisky Naučnyh Seminarov Leningradskogo Otdelenija Matematičeskogo Instituta im. V.A. Steklova, Akad. Nauk. SSSR 67 (1977), 167-183. English translation: Jour. Soviet Math. 16 (1981), 874-885.
- [1979] MATIJASEVIČ, Ju.V., *Algorithmic unsolvability of exponential diophantine equations in three unknowns* (Russian), Studies in the Theory of Algorithms and Mathematical Logic, Moscow, Nauka, 1979, 69-78. English translation available from University of Calgary, Dept. of Mathematics and Statistics.
- [1968] PARSONS, Ch., *Hierarchies of primitive recursive functions*, Zeitschrift für Math. Logik und Grundlagen der Mathematik, Vol. 14, No. 4 (1968), 357-376.
- [1964] RÖDDING, D., *Über die Eliminierbarkeit von Definitionsschemata in der Theorie der Rekursiven Funktionen*, Zeit. für Math. Logik und Grundlagen der Mathematik, Vol. 10, No. 4 (1964), 315-330.

Department of Mathematics and Statistics
University of Calgary
Calgary, Alberta
Canada
T2N 1N4

Steklov Mathematical Institute of
Academy of Science
27 Fontanka, L.O.M.I.
Leningrad 191011
U.S.S.R.

Manuscript reçu le 20 octobre 1981.