Will be convenient to show closure under a modified bounded $\forall$ quantification

Prop'n Given a Diophantine relation $\exists \vec{y}\,(F(\vec{x}, k, \vec{y}) = 0)$, the relation

(*) $\forall k,\ 1 \le k \le t\ (\exists \vec{y}\, F(\vec{x}, k, \vec{y}) = 0)$

is also Diophantine

($\vec{x}$ = $x_1, \dots, x_n$; $\vec{y}$ = $y_1, \dots, y_m$)

Notice: since $\forall a < b\ [\exists \vec{y}\, F(\vec{x}, a, \vec{y}) = 0]$ can be written

$$b = 0 \ \vee\ \exists b'\,(b'+1 = b \wedge \exists \vec{y}\, F(\vec{x}, 0, \vec{y}) = 0 \wedge \forall a,\ 1 \le a \le b\ \exists y\, F(\vec{x}, a, y) = 0)$$

prop'n $\Rightarrow$ usual bdd $\forall a<b$ quantification closure under

Naive translation of (*) is:

$$\exists \vec{y}^1\, \exists \vec{y}^2 \dots \exists \vec{y}^t \left[F(\vec{x}, 1, \vec{y}^1) = 0 \wedge \dots \wedge F(\vec{x}, t, \vec{y}^t) = 0 \right]$$

($\vec{y}^1$ = $y_1^1, y_2^1, \dots y_m^1$) which is not a formula: # of $\exists$'s and $\wedge$'s depends on t

↳ so we need to code

↳ will help to use a modified version of β function.

Def'n define $\tilde{\beta}(a,b,i) = \text{rem}(a, 1+bi)$

(recall: $\beta(a,b,i) = \text{rem}(a, 1+(b+1)i)$)

Easy to check: - $\tilde{\beta}$ also Diophantine
- satisfies "+1 index shifted" version of coding lemma: For all sequences $\ell_1, \ldots, \ell_m$ there are a,b s.t. $\tilde{\beta}(a,b,i) = \ell_i \quad 1 \le i \le m$
((call this "$\tilde{\beta}$-coding lemma")

- we note for future: in pf of coding lemma ① $b = N!$ for some large N
② possible to pick a arbitrarily large (if a works - so does $a + b_1 b_2 \cdots b_m$)

↳ in lemma below: use $\tilde{\beta}$ instead of β to code
- Y_i's will code (via $\tilde{\beta}(Y_i, N!, k) = y_i^k$) the witnesses y_i^k, for each $i \le m$

$$\begin{matrix} y_1^1 & y_2^1 & \cdots & y_m^1 \\ y_1^2 & y_2^2 & \cdots & y_m^2 \\ \vdots & & & \\ y_1^t & y_2^t & \cdots & y_m^t \end{matrix}$$

Y_i codes ith column

- we'll be able to get away with $m+3$ $\exists$'s as a result
- magnitude of N, K, Y, c, d will ensure $\equiv$ implies $=$ often

Coding Lemma: Sps $F(x_1, \ldots, x_n, k, y_1, \ldots, y_m)$ is a poly in $\mathbb{Z}$. Let $A \subseteq \mathbb{N}^{n+1}$ be the set of $(\vec{x}, t)$'s satisfying

$$\forall k, 1 \le k \le t \; \exists \vec{y} \; (F(\vec{x}, k, \vec{y}) = 0)$$

Then: $(\vec{x}, t) \in A$ iff there are Y, N, K (capital) and $y_1, \ldots, y_m$ (which can be chosen arb large) solving the following system:

① $N > c(x_1, x_2 \ldots x_n t Y)^d$

② $1 + KN! = \prod_{1 \le k \le t} (1 + kN!)$ (lowercase)

③ $F(\vec{x}, K, y_1, \ldots, y_m) \equiv 0 \pmod{1 + KN!}$

④ $\beta(y_i, N!, k) \le Y \quad \forall i \le m, \; 1 \le k \le t$

where c, d are constants that depend on F.

Pf: - fix $c >$ max of 2^n and all coeffs in F (abs value of)
- fix $d > m \cdot$ (max of all exponents in F)

Observe: For a given N, if $\underset{\sim}{K}$ is the (unique) soln to

$$1+\underset{\sim}{K}N! = \prod_{1\le k\le t} 1+kN!$$

(hence $= (1+N!)(1+2N!)(\cdots$
$(1+tN!)$
$= 1+(\cdots)N!$ ← this is $\le$)

then $\underset{\sim}{K} \equiv k \pmod{1+kN!}$ $\forall k \le t$

Why: $-1+\underset{\sim}{K}N!$ and $1+kN!$ both divis by $1+kN!$
- hence so is their difference $(\underset{\sim}{K}-k)N!$
- but $N!$ and $1+kN!$ coprime
$\Rightarrow 1+kN! \mid (\underset{\sim}{K}-k)$ ✓

Back to proof of coding lemma:

($\Rightarrow$) - Supp $(\vec{x}, t) \in A$ and fix tuples $\vec{y}^k$ witnessing this for $1 \le k \le t$.
- pick Y large enough so $Y > \max y_i^k$
- then pick N large enough so ① is true
- then $\underset{\sim}{K}$ determined by ② as observed.

↳ By $\tilde{\beta}$-coding lemma, for every $1 \le i \le m$, can find Y_i so that $\tilde{\beta}(Y_i, N!, k) = y_i^k$ $\forall 1 \le k \le t$

N is large enough

which implies (4) by choice of Y.

So we need only check (3).

- Since the y_i^k are witnesses and $Y_i \equiv y_i^k \pmod{1+kN!}$ & defn of $\tilde{\beta}$ we have $\forall\, 1 \le k \le t$,

$$F(\vec{x}, k, Y_1, \ldots, Y_m) \equiv F(\vec{x}, k, y_1^k, \ldots y_m^k) \; (=0) \pmod{1+kN!}$$

remember: mod arithmetic is nice! can make $\equiv$ substitutions in polynomial expressions and maintain $\equiv$.

- By choice of N, the integers $1+kN!$ are coprime (if p divides $1+kN!$ and $1+\ell N!$ then $p \mid (k-\ell)N!$ But $|k-\ell| < N$ so $\Rightarrow p \mid N!$ contradicting $p \mid 1+kN!$)

- Since $\underset{\sim}{k} \equiv k \pmod{1+kN!}$ $\forall\, 1 \le k \le t$ we get

$$F(\vec{x}, \underset{\sim}{k}, \vec{y}) \equiv 0 \pmod{1+kN!} \qquad \forall\, 1 \le k \le t$$

which gives

$$F(\vec{x}, \underset{\sim}{k}, \vec{y}) \equiv 0 \pmod{1+\underset{\sim}{k}N!}$$

Since $1+kN!$'s are rel. prime, which gives 3 ✓

($\Leftarrow$) - Now suppose we have $Y, N, \underset{\sim}{k}, Y_1, \ldots, Y_m$ satisfying (1) - (4)

- let $y_i^k = \text{rem}(Y_i, 1+kN!)$
  $= \tilde{\beta}(Y_i, N!, k)$ ($< Y$ by (4))

$Y_i \equiv y_i^k \pmod{1+kN!}$

- By (3), $F(\vec{x}, \underset{\sim}{k}, Y_1, \ldots, Y_m) \equiv 0 \pmod{1+\underset{\sim}{k}N!}$
  and hence $\equiv 0 \pmod{1+kN!}$ $\forall 1 \le k \le t$

- Since $\underset{\sim}{k} \equiv k \pmod{1+kN!}$ $\forall 1 \le k \le t$
  we have
  $$F(\vec{x}, k, y_1^k, \ldots, y_m^k) \equiv 0 \pmod{1+kN!}$$

- then by choice of c, d and by (1) must be that $|F(\vec{x}, k, y_1^k, \ldots, y_m^k)| < N$

- so must be $F(\vec{x}, k, \vec{y}^k) = 0$ $\forall 1 \le k \le t$
  i.e. $(\vec{x}, t) \in A$ ✓

Note that condition (4) is still a conjunction of length t, so if we want to turn (1)-(4) into a Fmla we still have an issue.

We claim that (4) can be replaced by the following:

(4)' $\prod_{j \le Y} (Y_i - j) \equiv 0 \pmod{1+kN!}$ and $Y < Y_i$ for every $i, 1 \le i \le m$

i.e. we claim (1)-(4)' holds iff (1)-(4) holds

($\Rightarrow$) if (4)' holds then for some $j \le Y$ we have $Y_i - j \equiv 0 \pmod{1+kN!}$

hence $\equiv 0 \pmod{1+kN!}$ $\forall 1 \le k \le t$

so $Y_i \equiv j \pmod{1+kN!}$ $\forall 1 \le k \le t$

giving $\tilde{\beta}(Y_i, N!, k) \equiv j$ and hence

$\le j$ and hence $\le Y$

which shows (4)

($\Leftarrow$) Conversely, sps we have (1)-(4) and we've chosen Y_i large enough so $Y_i > Y$ $\forall 1 \le i \le m$.

then by (4) we have $\tilde{\beta}(Y_i, N!, k)$

$= \text{rem}(Y_i, 1+kN!) = j \le Y$

for every $1 \le k \le t$

so for every k there is $j \le Y$ s.t.

$Y_i \equiv j \pmod{1+kN!}$

hence $\prod_{j \le y} (y_i - j) \equiv 0 \pmod{1 + kN!}$ $\forall 1 \le k \le t$

but then since $1+kN!$'s are coprime $\prod_{j \le y} (y_i - j) \equiv 0 \pmod{1 + k_0 N!}$ $\forall i$, giving $(4)'$. ✓

So what have we gained?

Coding lemma w/ $(4)'$ says we can write $(\vec{x}, t) \in A$ (i.e. $\forall k, 1 \le k \le t$ $\exists \vec{y}\ F(\vec{x}, k, \vec{y}) = 0$)

of:

$\exists Y \exists N \exists \cancel{S} \exists y_1 \cdots \exists y_m$ s.t.

(1) (statement w/ "$N >$ (long product)"

$\wedge$ (2) (see below — diophantine)

$\wedge$ (3) (asserting $\equiv$ of two quantities — die but involving $N!$ — see below)

$\wedge$ $(4)'$ (y length product and N. — see below)

So: we've got a fixed # of $\exists$'s and $\wedge$'s

But we need to see factorials $N!$ are diophantine, and also "generalized factorials", i.e. functions of the form

$$(t,x,y) \to \prod_{1 \le k \le t} (x+ky)$$

(note: if $x=0$ and $y=1$ this is just $t!$)

So: if we can show all generalized factorials are diophantine we'll be done.

Crux turns out to be:

Lemma (Matiyasevich's Lemma) The function $(x,y) \to x^y$ is Diophantine.