We need to show $x!$ and
$f(x,y,t) = \prod_{1\le k\le t}(x+ky)$ are Diophantine
($\approx$ covers $\prod_{j\le y}(y_i - j)$ too ... why?)

$x!$ is special case of latter.

We'll need

<u>Matiyasevich's Lemma</u>: ~~[illegible]~~ x^y is Diophantine.

Let's <u>assume</u> for now and show above functions are Diophantine.

We'll do $x!$ since it's simpler, then say "f is similar."

<u>Lemma</u> $x!$ is Diophantine.

<u>Pf</u>: Observe that
$$x! = \lim_{r\to\infty} r^x / \binom{r}{x}$$

since for $r \ge x$ we have:

$$\frac{r^x}{\binom{r}{x}} = \frac{r^x}{r!/x!(r-x)!} = x!\left(\frac{r\cdot r\cdots r}{r(r-1)\cdots(r-x+1)}\right)$$

$\to 1$ as $r\to\infty$

$\exists r$ (r is large enough $\wedge$

$\mathcal{E}$①

Note that $x! \leq r^x/\binom{r}{x}$ though, so for large enough r we have

$$x! = \left\lfloor r^x/\binom{r}{x} \right\rfloor$$

$y \leq [\ldots]^x/(rx)$

So, for large enough r we have
$y = x!$ iff $y \leq r^x/\binom{r}{x} < y+1$
iff $\binom{r}{x} y \leq r^x < \binom{r}{x}(y+1)$

So: to prove $x!$ is D_{10}, need to show $\binom{r}{x}$ is D_{10} and we can find "large enough r" in D_{10} way

For second part, let's check $r = (2x)^{x+1}$ works

We know:

$$x! \leq r^x/\binom{r}{x} = x!\left(\frac{r}{r}\frac{r}{r-1}\cdots\frac{r}{r-x+1}\right)$$
$$= x!\left(\frac{1}{1-\frac{0}{r}}\,\frac{1}{1-\frac{1}{r}}\cdots\frac{1}{1-\frac{x-1}{r}}\right)$$
$$\leq x!\left(\frac{1}{1-x/r}\right)^x$$

Now, note that for $0<\alpha<\frac{1}{2}$ we have $\frac{1}{1-\alpha} < 1+2\alpha$

(Why ow $\geq$, now multiply out and see..)

So, for $r > 2x$ we have

(✱) $$x!\left(\frac{1}{1-x/r}\right)^x < x!\left(1+\frac{2x}{r}\right)^x$$

Now note, for $0<\beta<1$ we have
$(1+\beta)^x < 1+\beta\cdot 2^x$

(Why: binomial expansion:
$$(1+\beta)^x = \sum_0^x \binom{x}{i}\beta^i = 1+\beta\underbrace{\sum^x \binom{x}{i}\beta^{i-1}}_{\leq 2^x \text{ since } \beta<1}$$)

hence by ✱ we have
$$< x!\left(1+\frac{2x}{r}\cdot 2^x\right)$$

so if r large enough so $x!\left(1+\frac{2x}{r}2^x\right) \leq$
$x!+1$ we're good,
i.e. want $x!\left(\frac{2x}{r}\cdot 2^x\right) < 1$
i.e. $r > 2x\,2^x\cdot x! = 2^{x+1}\cdot x\cdot x!$
but this is certainly true if $r > (2x)^{x+1}$
so claim holds,
i.e. if we knew exponentiation is Δ_0
then asserting $r > (2x)^{x+1}$ is Δ_0 too

($<$ is Δ_0, compositions of Δ_0 is Δ_0 –
didn't need bdd quant to prove)

Now let's check:

<u>Lemma</u> $\binom{r}{x}$ is Diophantine (can define $=0$ if $r<x$)

<u>Pf</u>: By binomial theorem:

$$(u+1)^r = \sum_0^r \binom{r}{x} u^x$$

Thus if $\binom{r}{x} < u$ for all $x \le r$ we have a base u expansion of $(u+1)^r$ in terms of $\binom{r}{x}$'s

E.g. can take $u = 2^{r+1}$ (or even 2^r+1)
Then $\binom{r}{x}$ is coefficient of u^x in base u expansion of $(u+1)^r$

Define $\Phi(m,b,w)$ = coeff. of b^m in b-ary expansion of w (assume $b \ge 2$)

So: $\binom{r}{x} = \Phi(x, 2^{(r+1)}, (2^{(r+1)}+1)^r)$

Since compositions of D10 functions are D10 and we're assuming exp. functions are D10, enough to show Φ is D10.

But <u>notice</u>:

$\Phi(m,b,w) = q$ iff
$$\exists p \exists r (w = p + q \cdot b^m + r \wedge q < b \wedge r < b^m \wedge p \equiv 0 \pmod{b^{m+1}}))$$

which is clearly Dio (assuming exponentiation

✓

So we've shown x^y Dio $\Rightarrow$ $x!$ is too
How to prove more general $\prod_{1\le k \le t} (x+yk)$
Dio too?
Spr'dly similar arg – doesn't seem
entirely straightforward to me.
You try! We'll take for granted.

So: we've reduced showing r.e. $\Leftrightarrow$ Diophantine
to showing x^y is Dio.
This is Matiyasevich's contribution

Lemma below says we can reduce
showing x^y is Dio to showing there
is a Dio function that "grows exponentially"

<u>Lemma</u> Suppose there exists a Diophantine function $y(a,n)$ s.t. for every $a>1$ and every n we have

$$(2a-1)^n \le y(a,n+1) \le (2a)^n$$

<u>Then</u>: a^n is Diophantine.

<u>Pf</u>: Sps we have such a y.
Observe, for any M we have:

$$\frac{y(aM,n+1)}{y(M,n+1)} \le \frac{(2aM)^n}{(2M-1)^n} = a^n\left(\frac{2M}{2M-1}\right)^n$$
$$= a^n\left(1-\frac{1}{2M}\right)^{-n}$$

and

$$\frac{y(aM,n+1)}{y(M,n+1)} \ge \frac{(2aM-1)^n}{(2M)^n} = \left(a-\frac{1}{2M}\right)^n$$
$$= a^n\left(1-\frac{1}{2aM}\right)$$

Altogether:

$$a^n\left(1-\frac{1}{2aM}\right)^n \le \frac{y(aM,n+1)}{y(M,n+1)} \le a^n\left(1-\frac{1}{2M}\right)^{-n}$$

So for M large enough (relative to a fixed n) we have

$$a^n - 1 < \frac{y(aM, n+1)}{y(M, n+1)} < a^n + 1 \qquad (*)$$

We will show $y(a+1, n+2)$ is a good enough lower bound.

Specifically, we claim:

$a^n = m$ iff

$\exists M$ s.t.

1. $M > y(a+1, n+2)$ (Dio, assuming y is)
2. $(m-1)\, y(M, n+1) < y(aM, n+1)$ and $(m+1)\, y(M, n+1) > y(aM, n+1)$ (Dio if y is: $<$, $\cdot$, composition all Dio) (is just $*$ with m as a^n)
3. a divides M (Dio)

(need clause 3 to assure we actually hit a^n: we'll prove for such M, y ratio falls between $a^n - 1$ and $a^n + 1$ (so $m = a^n$), but at same time it could also fall between $a^n - 2$ and a^n ($m = a^n - 1$) or a^n and $a^n + 2$ ($m = a^n + 1$) so we need to rule these out.)

So assume $M > y(a+1, n+2)$

We show we get $(*)$. First consider LHS

$$a^n\left(1-\tfrac{1}{2aM}\right)^n = a^n\left(\sum_0^n (-1)^i \binom{n}{i}\left(\tfrac{1}{2aM}\right)^i\right)$$

$$= a^n - \frac{1}{2M}\sum_1^n (-1)^{i-1}\binom{n}{i}\left(\frac{1}{2M}\right)^{i-1} a^{n-i}$$

$$\geq a^n - \frac{1}{2M}(1+a)^n$$

Since $(1+a)^n = \sum_0^n \binom{n}{i} a^{n-i}$ is $\geq$ sum above

So $M \geq (1+a)^n$ works and we knew $y(a+1, n+2) \geq (2(a+1)-1)^{n+2} = (2a+1)^{n+2}$

For RHS: if $M > a$ we have:

$$a^n\left(1-\tfrac{1}{2M}\right)^{-n} = \left(2aM/2M-1\right)^n \quad \text{(from before simplifying)}$$

$$\leq \left[(2M+1)a+1/2M\right]^n \quad \text{(cross multiply use } M>a\text{)}$$

$$= \left[a + \frac{(a+1)}{2M}\right]^n$$

$$= \sum_0^n \binom{n}{i} a^{n-i}(a+1)^i\left(\frac{1}{2M}\right)^i$$

$$= a^n + \frac{1}{2M}\sum_1^n \binom{n}{i} a^{n-i}(a+1)^i\left(\frac{1}{2M}\right)^{i-1}$$

$$\leq a^n + \frac{1}{2M}\left(a+(a+1)\right)^n = a^n + \frac{1}{2M}(2a+1)^n$$

So $M \geq (2a+1)^n$ works

and $y(a+1, n+2)$ exceeds $(2a+1)^n$ ✓

Next goal is to prove there is such a y, Diophantine - then we're done!

Long way still...

First: some induction.

<u>Pell's Equation</u>:

- Key tool in proving Matiy is Pell's eq'n
- For $d \in \mathbb{N}$ this is the eq'n
$$x^2 - dy^2 = 1$$
- Can factor LHS as
$$(x - \sqrt{d}y)(x + \sqrt{d}y)$$
- suggests we might consider the integral domain $\mathbb{Z}[\sqrt{d}]$
$$= \{a + \sqrt{d}b : a, b \in \mathbb{Z}\}$$
- For $\alpha = a + \sqrt{d}b \in \mathbb{Z}[\sqrt{d}]$, <u>conjugate</u> is $\bar{\alpha} = a - \sqrt{d}b$

- norm of α is $\|\alpha\| = \alpha \cdot \bar{\alpha} = a^2 - db^2$

- to solve Pell's: look for $\alpha \in \mathbb{Z}[\sqrt{d}]$ with $\|\alpha\| = 1$

Some observations:

Fact: the set $S = \{\alpha \in \mathbb{Z}[\sqrt{d}] : \alpha > 0, \|\alpha\| = 1\}$ is a group under the usual multiplication (i.e. a multiplicative subgroup of $\mathbb{R}^+$)

Pf: not hard to check $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$
so if $\alpha, \beta \in S$ then $\overline{\alpha\beta} = 1 \cdot 1 = 1$
$\Rightarrow \alpha\beta \in S$
clear $\bar{\alpha}$ is multiplicative inverse of α also of norm 1. ✓

Following is a general fact about subgroups of $(\mathbb{R}^+, \cdot)$

Fact: Sps $(G, \cdot)$ a subgroup of $(\mathbb{R}^+, \cdot)$
Then either G is dense in $\mathbb{R}^+ = (0, \infty)$ or discrete (i.e. no limit points).
If discrete, there is $\gamma \in G$ s.t.
$G = \{\gamma^n : n \in \mathbb{Z}\}$