# Homework set 14

Hilbert's tenth problem seminar, Fall 2013, due January 14th

By Niels Voorneveld

**Exercise 1:**
We are in the field $\mathbb{F}_q[Z]$. Remember that $\mathcal{M}$ consists of triples $(F, w, s)$ with $s$ a $q$-th power, $w \leq s$ and $F = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} Z^{si+j}$ where $d$ some natural number and all $a_{ij} \epsilon \mathbb{F}_q$.
Remember that $\theta : \mathcal{M} \to \mathbb{F}_q[V, W]$ sends $(\Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} Z^{si+j}, w, s)$ to $\Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} V^i W^j$.

Let $(F_1, w, s), (F_2, w, s) \epsilon \mathcal{M}$.
a) Prove that $\theta(F_1, w, s) + \theta(F_2, w, s) = \theta(F_1 + F_2, w, s)$

**Proof:**
We can write $F_1 = \Sigma_{i=0}^{d_1-1} \Sigma_{j=0}^{w-1} \alpha_{ij} Z^{si+j}$ and $F_2 = \Sigma_{i=0}^{d_2-1} \Sigma_{j=0}^{w-1} \beta_{ij} Z^{si+j}$.
Take $d = max(d_1, d_2)$. Notice that for this new $d$, we can still write:
$F_1 = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} Z^{si+j}$ and $F_2 = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \beta_{ij} Z^{si+j}$, where we can take the $\alpha$'s and $\beta$'s zero if they are out of range. (So $\alpha_{ij} = 0$ if $i >= d_1$ and $\beta_{ij} = 0$ if $j >= d_2$).

So $\theta(F_1, w, s) = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} V^i W^j$ and $\theta(F_2, w, s) = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \beta_{ij} V^i W^j$
Hence $\theta(F_1, w, s) + \theta(F_2, w, s) = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} (\alpha_{ij} + \beta_{ij}) V^i W^j$.
On the other hand: $F_1 + F_2 = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} Z^{si+j} + \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \beta_{ij} Z^{si+j} = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} (\alpha_{ij} + \beta) Z^{si+j}$. Since the summation range has not changed, we see that $F_1 + F_2$ is still a stride polynomial of degree $w$-$s$, or in other words, $(F_1 + F_2, w, s)$ is an element of $\mathcal{M}$. For this element: $\theta(F_1 + F_2, w, s) = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} (\alpha_{ij} + \beta_{ij}) V^i W^j$ hence the equation is satisfied.

b) Prove that if $2w \leq s$, $\theta(F_1, w, s) \cdot \theta(F_2, w, s) = \theta(F_1 F_2, 2w, s)$
**Proof:**
$F_1 F_2 = (\Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} Z^{si+j}) \cdot (\Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \beta_{ij} Z^{si+j}) = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \Sigma_{h=0}^{d-1} \Sigma_{k=0}^{w-1} \alpha_{ij} \beta_{hk} Z^{s(i+h)+j+k} = \Sigma_{a=0}^{2d-2} \Sigma_{b=0}^{2w-2} (\Sigma_{i=0}^{a} \Sigma_{j=0}^{b} \alpha_{ij} \beta_{(a-i)(b-j)}) Z^{sa+b}$. So this is a stride polynomial of degree $2w - 1, s$, so also of degree $2w, s$. Since by assumption $2w \leq s$ and $s$ of course is still a power of $q$, $(F_1 F_2, 2w, s)$ is an element of $\mathcal{M}$. So can calculate:
$\theta(F_1 F_2, w, s) = (\Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} Z^{si+j}) \cdot (\Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \beta_{ij} Z^{si+j}) = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \Sigma_{h=0}^{d-1} \Sigma_{k=0}^{w-1} \alpha_{ij} \beta_{hk} Z^{si+j} = \Sigma_{a=0}^{2d-2} \Sigma_{b=0}^{2w-2} (\Sigma_{i=0}^{a} \Sigma_{j=0}^{b} \alpha_{ij} \beta_{(a-i)(b-j)}) V^a W^b$.
On the other hand: $\theta(F_1, w, s) \cdot \theta(F_2, w, s) = (\Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \alpha_{ij} V^i W^j) \cdot (\Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \beta_{ij} V^i W^j) = \Sigma_{i=0}^{d-1} \Sigma_{j=0}^{w-1} \Sigma_{h=0}^{d-1} \Sigma_{k=0}^{w-1} \alpha_{ij} \beta_{hk} V^{i+h} W^{j+k} = \Sigma_{a=0}^{2d-2} \Sigma_{b=0}^{2w-2} (\Sigma_{i=0}^{a} \Sigma_{j=0}^{b} \alpha_{ij} \beta_{(a-i)(b-j)}) V^a W^b$, so the equation is satisfied.

**Exercise 2:**
a) Prove that the following function:
$\delta : \mathbb{F}_q[Z] \times \mathbb{F}_q[Z] \to \mathbb{F}_q[Z]$, $(A, B) \mapsto A^p Z + B^p$ is injective.

**Proof:**
Take an arbitrary element of $F_1, F_2 \epsilon \mathbb{F}_q[Z]$ which we can write the following way: $F_1 = \Sigma_{i=0}^{d} \alpha_i Z^i$ and $F_2 = \Sigma_{i=0}^{d} \beta_i Z^i$, where $d \epsilon \mathbb{N}$ and all $\alpha_i, \beta_i \epsilon \mathbb{F}$ (again, $d$ can be taken large enough: $d = max(deg(F_1), deg(F_2))$, or even arbitrarily larger).

-Since $p$ is the characteristic of the field, a sum to the power $p$ is the same as the sum of the elements individually to the power $p$.
-Also the map: $(.)^p : \mathbb{F}_q \to \mathbb{F}_q$ is a bijection.
So: $\delta(F_1, F_2) = (\Sigma_{i=0}^d \alpha_i Z^i)^p Z + (\Sigma_{i=0}^d \beta_i Z^i)^p = \Sigma_{i=0}^d \alpha_i^p Z^{ip} Z + \Sigma_{i=0}^d \beta_i^p Z^{ip} = \Sigma_{i=0}^d (\alpha_i^p Z^{ip+1} + \beta_i^p Z^{ip})$. Since $p > 1$, none of the $Z$ powers $Z^{ip}$ coincide with $Z^{iP+1}$. So the image is fully determined by the coeficients $\alpha_i^p$ and $\beta_i^p$. So if we have two other elements $F_3, F_4$ of $\mathbb{F}_q[Z]$, such that $(F_1, F_2) \neq (F_3, F_4)$, at least one of the $\alpha$'s or one of the $\beta$'s must be different, so at least one of the $\alpha_i^p$ or $\beta_i^p$ must be different. Hence, they will give an other image under $\delta$. So $\delta$ is injective. Also note that this function is diophantine.

b) Knowing that any r.e. subset of $\mathbb{F}_q[Z]$ is diophantine in $\mathbb{F}_q[Z]$, prove that any r.e. subset of $\mathbb{F}_q[Z]^k$ for some $k > 1$ is diophantine in $\mathbb{F}_q[Z]$.

**Proof:**
With induction on $n$, we are going to prove that any r.e. subset of $\mathbb{F}_q[Z]^n$ is diophantine over $\mathbb{F}_q[Z]$.
The induction basis, $n = 1$ is already given.
Induction step: Assume for $n > 0$ that any r.e. subset of $\mathbb{F}_q[Z]^n$ is diophantine. Take arbitrary r.e. subset of $A \subset \mathbb{F}_q[Z]^{n+1}$. So $A$ consists of elements of the form $(a_0, a_1, ..., a_n)$. Now define $\delta_n : \mathbb{F}_q[Z]^{n+1} \to \mathbb{F}_q[Z]^n$ by taking $\delta$ of the first two elements, so $\delta_n(a_0, a_1, ..., a_n) = (\delta(a_0, a_1), a_2, ..., a_n)$. Since $\delta$ is injective and diophantine, $\delta_n$ is also injective and diophantine. So $B := \delta_n(A)$ is r.e. in $\mathbb{F}_q[Z]^n$. So by the hypothesis, $B$ is diophantine. Hence the following statement gives a diophantine expression of $A$:
$x \epsilon A \Leftrightarrow \delta_n(x) \epsilon B$. So $A$ is diophantine.
Hence any r.e. subset of $\mathbb{F}_q[Z]^{n+1}$ is diophantine over $\mathbb{F}_q[Z]$. So the induction proof has been completed.

**Exercise 3:**
Take $\mathbb{F}$ to be a recursive infinite algebraic extension of the field $\mathbb{F}_p$, with $p$ some prime. Take $q$ a power of $p$. Take $X \epsilon \mathbb{F}[Z]$ and assume the following:

$(\exists a, b, u) : X \epsilon \mathcal{A}_u$
$\wedge q^a > u \wedge q^b > u \wedge gcd(a, b) = 1$
$\wedge X^{q^a} \equiv X \pmod{Z^{q^a} - Z}$
$\wedge X^{q^b} \equiv X \pmod{Z^{q^b} - Z}$

Remember from the lecture that if $X \epsilon \mathcal{A}_u$ than $deg(X) \leq u$.

Prove that $X \epsilon \mathbb{F}_q[Z]$
(Hint, remember last week's hand-in exercise).

**Proof:**
Take $X, a, b, u$ as in the assumption. Since $X \epsilon \mathcal{A}_u$ we have that $deg(X) \leq u$, so we can write $X = \Sigma_{i=0}^u \alpha_i Z^i$ with all $\alpha_i \epsilon \mathbb{F}$. Since $q$ is a power of $p$ prime, and $p$ is the characteristic of the field $\mathbb{F}$, we have that for powers of $q$ the same rule applies as before: the Power of sum is the sum of powers.
Hence in particular for $q^a$:
$X^{q^a} = (\Sigma_{i=0}^u \alpha_i Z^i)^{q^a} = \Sigma_{i=0}^u \alpha_i^{q^a} Z^{q^a i}$. Looking at this for modulo $Z^{q^a} - Z$, we know that because $Z^{q^a} \equiv Z \pmod{Z^{q^a} - Z}$, $X^{q^a} \equiv \Sigma_{i=0}^u \alpha_i^{q^a} Z^i$. By our assumption, this is equivalent to $X$ itself

(mod $Z^{q^a} - Z$).
But notice that $deg(X) \leq u < q^a = deg(Z^{q^a} - Z)$, hence the $X^{q^a} = X$ (Equivalence is equality).
So $\Sigma_{i=0}^{u} \alpha_i^{q^a} Z^i = \Sigma_{i=0}^{u} \alpha_i Z^i$, so for all $i$, $\alpha_i^{q^a} = \alpha_i$. But that means all $\alpha_i \epsilon \mathbb{F}_{q^a}$.
By the same reasoning, all $\alpha_i \epsilon \mathbb{F}_{q^b}$. So by last week's exercise: all $\alpha_i \epsilon \mathbb{F}_{q^a} \cap \mathbb{F}_{q^b} = \mathbb{F}_{q^{gcd(a,b)}} = \mathbb{F}_q$.
Hence $X \epsilon \mathbb{F}_q[Z]$.

Points: Exercise 1:
0.5 points: Noting that two elements can have the same $d$.
1 point: Calculation in 1a.
1.5 points: Calculation in 1b.
0.5 points: Checking if $(F_1F_2, 2w, s)$ is a proper element of $\mathcal{M}$.

Exercise 2:
1 point: Calculation of the image of an element under $\delta$
1 point: Finishing argument of injectivity.
1.5 points: answer question 2b.

Exercise 3:
1 point: Writing down $X$ and calculating $X^{q^a}$ and $X^{q^b}$.
1 point: Arguing that equivalence is identity.
1 point: Finishing the proof.