POLYNOMIALS ON THE FINITE PLANE

Alexander Polishchuk

1 Introduction

Let $\mathbf{F}_q$ be the finite field consisting of q elements. We are interesting in the functions on the finite plane $\mathbf{FP} = \mathbf{F}_q^2$ with value in $\mathbf{F}_q$. Any such a function is of course polynomial one, more precisely we identify the space of all these functions with the space of polynomials in x, y of degree $< q$ in each variable. In particular we associate to each function on $\mathbf{FP}$ its bidegree $=$ $(\deg_x, \deg_y)$. The problem we are concerned with is the following one: we have two functions ϕ, ψ on $\mathbf{FP}$ such that $\phi \equiv \psi$ outside some set $S \subset \mathbf{FP}$(we write $\equiv$ for pointwise equality of functions). We would like to assert that if $\deg_x\phi$, $\deg_y\psi$ and card$S$ are sufficiently small (to be more precise are of order resp. εq, εq and εq^2) then there exists some function f such that bideg$f$ is small and f equals to ϕ and ψ outside S. Unfortunately we cannot assert something like this in general - we should impose some conditions on S as the following simple example shows.

Example. Put $S = \{(x,y) \neq (0,0)$ such that either $x = 0$ or $y = 0\}$. Define our functions as follows: $\phi(x,y) = \theta(y), \psi(x,y) = \theta(x)$ where $\theta(0) = 1$ and $\theta(t) = 0$ for $t \neq 0$. Then $\deg_x\phi = 0$, $\deg_y\psi = 0$ and $\phi \equiv \psi$ outside S. Assume that $f \equiv \phi$ outside S for some function f such that $\deg_x f < q-1$, $\deg_y f < q-1$. Then for any $y \neq 0$ $f(.,y) = 0$ therefore $f(0,.) = 0$ which is contradiction.

In the previous example we had rather special subset $S \subset \mathbf{FP}$. To avoid such pathologies we should assume that S contains any coordinate line (horizontal or vertical) if S contains sufficiently large part of it. We fix more precise notion in the following definition.

Definition. Subset $S \subset \mathbf{FP}$ is called *ε-stable* if for any coordinate line $L \subset FP$ if card$(L \cap S) > (1-\varepsilon)q$ then $L \subset S$.

Definition. S is called *(n,m)-regular* if for any functions ϕ and ψ on $\mathbf{FP}$ such that $\deg_x\phi < n$, $\deg_y\psi < m$, $\phi \equiv \psi$ outside S there exists f such that

$\mathrm{deg}_x f \leq \mathrm{deg}_x \phi$, $\mathrm{deg}_y f \leq \mathrm{deg}_y \psi$ and $f \equiv \phi$ outside S.

Our main result is the following theorem.

Theorem 1 *Assume that S is ε-stable where $0 < \varepsilon < 1/2$ and $\mathrm{card} S < [\delta q]^2$ where $\delta = (1 - 2\varepsilon)/3$ and $[x]$ denotes the largest integer $\leq x$. Then S is $(\varepsilon q, \varepsilon q)$-regular.*

This theorem has the following corollary which is important for complexity theory as D. Spielman informed me. For any subset $S \in FP$ define the probability of S: $\mathrm{P}(S) = \mathrm{card} S/q^2$.

Theorem 2 *There exists a constant $c > 0$ (independent on q) such that for any $\varepsilon < c$, for any functions ϕ and ψ on* $\mathbf{FP}$ *such that $\mathrm{deg}_x \phi < \varepsilon q$, $\mathrm{deg}_y \psi < \varepsilon q$, $\mathrm{P}\{(x,y) | \phi(x,y) \neq \psi(x,y)\} = p < c$ there exists f such that $\mathrm{deg}_x f \leq \mathrm{deg}_x \phi$, $\mathrm{deg}_y f \leq \mathrm{deg}_y \psi$ and $\mathrm{P}\{(x,y) | \phi(x,y) \neq f(x,y)$ or $\psi(x,y) \neq f(x,y)\} < \frac{1+\mu}{1-\mu} p$ where $\mu = \varepsilon + 2\frac{p}{1-\varepsilon}$.*

Proof. Let $S \subset \mathbf{FP}$ be the set of points where ϕ and ψ take different values. Take some $\nu > 0$ and consider the set S_ν which is obtained from S by deleting all the coordinate lines L for which $\mathrm{card}(L \cap S) > (1-\nu)q$. Then S_ν is ν-stable by definition. Consider also the functions ϕ_1 and ψ_1 obtained from initial functions by multiplying with the equations of deleted lines so that these new functions coincide outside S_ν. It is easy to see that the number of deleted horizontal (or vertical) lines doesn't exceed $\frac{p}{1-\nu} q$. It follows that the $(S_\nu, \phi_1, \psi_1, \varepsilon_1)$ satisfies the conditions of Theorem 1 if only $\max(\nu, \varepsilon + \frac{p}{1-\nu}) \leq \varepsilon_1$ and $p < (\delta_1 - q^{-1})^2$ where $\delta_1 = (1 - 2\varepsilon_1)/3$. Choose ν so that

$$\nu = \varepsilon + \frac{p}{1-\nu}$$

namely put $\nu = \frac{1}{2}(1 + \varepsilon - \sqrt{(D)})$ where $D = (1-\varepsilon)^2 - 4p$ is assumed to be positive (this is indeed the case provided that ε and p are sufficiently small). It is easy to see that $0 < \nu < \mu = \varepsilon + 2\frac{p}{1-\varepsilon}$. Hence if we put $\varepsilon_1 = \nu$ all the conditions above are satisfied if only ε and p are small enough. Applying Theorem 1 we obtain that ϕ_1 and ψ_1 coincide outside S_ν. Therefore ϕ and ψ coinside outside the union of S and deleted coordinate lines which we denote by S_1. It is easy to see that $\mathrm{P}(S_1) \leq p + 2\nu\frac{p}{1-\nu} = \frac{1+\nu}{1-\nu} p$ so we are done ▮.

Acknowledgements. I am grateful to Alexander Shen for formulating this problem to me and encouragement and to Dan Spielman for his interest to this work.

2 Connection with interpolation

Let us denote by k^S the space of functions on some set S with value in some field k. Let $V_{n,m} \subset \mathbf{F}_q[x,y]$ be the subspace of polynomials f such that $\deg_x f < n$, $\deg_y f < m$. Put $V = V_{q,q} \simeq \mathbf{F}_q^{FP}$.

Definition. Subset $S \subset \mathbf{FP}$ is called (n,m)-negligible if for any $\phi, \psi \in V$ such that $\deg_x \phi < n$, $\deg_y \psi < m$ and $\phi \equiv \psi$ outside S it follows that $\phi = \psi$.

Example. Let L be a vertical or horizontal line in $\mathbf{FP}$. Then if $n > 0$, $m > 0$ L is not (n,m)-negligible. It follows that if S contains a coordinate line then it is not (n,m)-negligible.

This example in some sense is the worst one: if S has relatively small intersection with each coordinate line it will be (n,m)-negligible. The next proposition gives very useful criterion for S to be (n,m)-negligible.

Proposition 3 *S is (n,m)-negligible iff restriction map $V_{q-n,q-m} \to \mathbf{F}_q^S$ is surjective.*

Proof. By the definition S is not (n,m)-negligible iff there are some $\phi, \psi \in V$ such that $\deg_x \phi < n$, $\deg_y \psi < m$, $\phi \equiv \psi$ outside S, $\phi \neq \psi$. Put $f = \phi - \psi$. It is easy to see that

$$\sum_{(x,y)\in S} f(x,y)x^i y^j = 0 \text{ for any } i,j \text{ st } 0 \leq i < q-n, 0 \leq j < q-m. \qquad (1)$$

Conversely, easy dimension count shows that if this system of equations holds for some $f \in \mathbf{F}_q^S$ (which we consider as an element of V extending by zero outside S) then it can be presented in the form $f = \phi - \psi$ for some ϕ and ψ as above. So S is (n,m)-negligible iff (1) has only zero solution. But this means that the matrix of this system has maximal rank which is equivalent to the surjectivity of the restriction map $V_{q-n.q-m} \to \mathbf{F}_q^S$ ▮.

Now we are going to deduce Theorem 1 from the following statement which will be proved in the next section.

Theorem 4 *Let $S = Z(F) \subset \mathbf{FP}$ be the set of zeroes of the polynomial F of bidegree (d_x, d_y). Assume that S contains no coordinate line. Then the restriction map $V_{n,m} \to \mathbf{F}_q^S$ is surjective provided that $n \geq \frac{3}{2}d_x + \frac{1}{2}q$, $m \geq \frac{3}{2}d_y + \frac{1}{2}q$.*

In fact we are able to prove the following more powerful result.

Theorem 5 *Let $S \subset Z(F)$ be the subset of the zero set of some polynomial F such that* bideg$F$ *$= (d_x, d_y)$. Let l_x (resp. l_y) be the number of vertical (resp. horizontal) lines contained in $Z(F)$. Assume that S is ε-stable. Then S is (n_x, n_y)-regular where $n_* = \max(\frac{1}{2}q - \frac{3}{2}d_* + \frac{1}{2}l_*, \varepsilon q)$, $*$ denotes x or y.*

Note that Theorem 1 follows immediately because for any $S \subset \mathbf{FP}$ such that card$S < [\delta q]^2$ there exists some polynomial F of bidegree (d_x, d_y) where $d_x, d_y \leq \delta q$ so that $\frac{1}{2}q - \frac{3}{2}d_* \geq \varepsilon q$ and $S \subset Z(F)$.
Proof of Th.5. If $Z(F)$ contains no coordinate line the statement follows from Theorem 4 and the proposition above. Now we proceed by induction on the number of coordinate lines contained in $Z(F)$. Let for example $F = (x-a)F_1$ where F_1 doesn't vanish on the line $L = \{(x = a)\}$ (we can assume so). Put $S_1 = S \setminus L \subset Z(F_1)$. Let ϕ, ψ be some functions such that $\deg_x\phi < n_x$, $\deg_y\psi < n_y$, $\phi \equiv \psi$ outside S. Put $\phi_1 = (x-a)\phi$, $\psi_1 = (x-a)\psi$. Then $\phi_1 \equiv \psi_1$ outside S_1 so by induction hypothesis there exists some $f_1 \in V$ such that $\deg_x f_1 \leq \deg_x\phi + 1$, $\deg_y f_1 \leq \deg_y\psi$ and $f_1 \equiv (x-a)\phi$ outside S_1. In particular f_1 vanishes on L so that $f_1 = (x-a)f$ for some f. It follows that $f \equiv \phi$ outside $S \cup L$ so it remains to verify that f coincides with ϕ at the point $(a, b) \in L \setminus S$. But the restrictions of f and ϕ to the line $(y = b)$ are polynomials of degree $< \varepsilon q$ coinciding at the set $L \setminus S$ of cardinality $\geq \varepsilon q$ so they coincide identically ∎

3 Algebraic geometry

In this section we will prove Theorem 4. The crucial remark is that the statement we need to prove is geometric one in the sense that it is enough to prove an analogous statement after extension of the basic field from $\mathbf{F}_q$ to its algebraic closure $k = \overline{\mathbf{F}_q}$. So let $C \subset \mathbf{A}_k^2$ be the curve defined by $F \in \mathbf{F}_q[x, y]$, $S = C(\mathbf{F}_q)$ is the set of rational points on C. The problem is to interpolate any k-valued function ϕ on S by polynomial of possibly smaller bedegree. We do this in two steps: at first lifting ϕ to the section of some linear bundle on C and then representing this section by polynomial. The reason to do so is that at each step we have the problem of lifting from divisor which is easy to treat.

Remark that embedding $\mathbf{A}_k^2 \subset \mathbf{P}_k^1 \times \mathbf{P}_k^1$ induces by restriction an isomorphism $H^0(\mathbf{P}_k^1 \times \mathbf{P}_k^1, \mathcal{O}(n-1, m-1)) \simeq V_{n,m}$ so it is natural to complete our curve C by its closure $\overline{C}$ in $\mathbf{P}_k^1 \times \mathbf{P}_k^1$ which is the divisor of bidegree (d_x, d_y). Consider first the case of irreducible curve C.

Lemma 6 *Let X be an irreducible divisor of bidegree (d_1, d_2) on $\mathbf{P}_k^1 \times \mathbf{P}_k^1$, $S = \{x_1, \ldots, x_s\}$ be the set of s distinct k-points where $s \leq q(d_1+d_2)/2$. Then if $n_i > \frac{3}{2}d_i + \frac{1}{2}q - 2$ $(i = 1, 2)$ the restriction map $H^0(\mathbf{P}_k^1 \times \mathbf{P}_k^1, \mathcal{O}(n_1, n_2)) \rightarrow k^S$ is surjective.*

Proof. Remark first that the restriction map $H^0(\mathbf{P}_k^1 \times \mathbf{P}_k^1, \mathcal{O}(n_1, n_2)) \rightarrow H^0(\mathcal{O}_X(n_1, n_2))$ is surjective. Indeed this map fits in the exact sequence

$$0 \rightarrow H^0(\mathbf{P}_k^1 \times \mathbf{P}_k^1, \mathcal{O}(n_1 - d_1, n_2 - d_2)) \rightarrow H^0(\mathbf{P}_k^1 \times \mathbf{P}_k^1, \mathcal{O}(n_1, n_2)) \rightarrow$$

$$\rightarrow H^0(\mathcal{O}_X(n_1, n_2)) \rightarrow H^1(\mathbf{P}_k^1 \times \mathbf{P}_k^1, \mathcal{O}(n_1 - d_1, n_2 - d_2) \rightarrow \ldots$$

and the last term is equal to zero because $n_i > d_i - 2$. So it is enough to prove that there exists some Cartier divisor D on X such that $\mathrm{supp} D = S$ and the natural map $H^0(\mathcal{O}_X(n_1, n_2)) \rightarrow H^0(\mathcal{O}_D(n_1, n_2))$ is surjective. For the last condition note that from the cohomology sequence of the exact triple

$$0 \rightarrow \mathcal{O}_X(n_1, n_2)(-D) \rightarrow \mathcal{O}_X(n_1, n_2) \rightarrow \mathcal{O}_D(n_1, n_2) \rightarrow 0$$

it follows as above that it is enough to verify that $H^1(\mathcal{O}_X(n_1, n_2)(-D)) = 0$. By Serre duality on X we have $H^1(\mathcal{O}_X(n_1, n_2)(-D)) \simeq$
$\simeq H^0(\mathcal{O}_X(-n_1, -n_2)(K + D))^*$ where $K \simeq \mathcal{O}_X(d_1 - 2, d_2 - 2)$ is the canonical class on X. As X is irreducible it suffice to require that
$\deg(\mathcal{O}_X(d_1 - n_1 - 2, d_2 - n_2 - 2)(D)) < 0$ that is

$$\deg D < n_1 d_2 + n_2 d_1 - 2d_1 d_2 + 2(d_1 + d_2)$$

Let r_i be the multiplicity of x_i on X (see [1]). Then we can choose for D Cartier divisor of degree

$$\deg D = \sum r_i \leq s + \sum_{x \in \mathrm{Sing} X} (r_x - 1)$$

where for k-point $x \in X$ we denote by r_x its multiplicity, Sing$X$ is the set of singular points of X. It is well known (see [1]) that

$$\sum_{x \in X} (r_x - 1) \leq p_a$$

where $p_a = d_1 d_2 - d_1 - d_2 + 1$ is the arithmetical genus of X. Hence $\deg D \leq s + d_1 d_2 - d_1 - d_2 + 1$. Now by assumption

$$n_1 d_2 + n_2 d_1 > (\frac{3}{2} d_1 + \frac{1}{2} q - 2) d_2 + (\frac{3}{2} d_2 + \frac{1}{2} q - 2) d_1 =$$

$$= 3 d_1 d_2 - 2(d_1 + d_2) + q(d_1 + d_2)/2 \geq 3 d_1 d_2 - 3(d_1 + d_2) + 1 + s$$

Combining this with the previous ineqality we obtain the required estimate for $\deg D$ ▮.

Now we can finish the proof of Theorem 4 as follows. Decompose F into the product of irreducible polynomials (we can assume that each of them has multiplicity 1): $F \Rightarrow \prod F_i$ where $\mathrm{bideg} F_i = (d_x^{(i)}, d_y^{(i)})$, let $C = \cup C_i$ be the corresponding decomposition of C into the union of irreducible components. The proof will be based on applying of lemma to the closures of C_i. Let ϕ be the function on S we want to interpolate. Note that we can apply the previous lemma to the pair $(S_i = S \cap C_i,\ C_i)$ because $\mathrm{card}(S \cap C_i) \leq q \cdot \min(d_x^{(i)}, d_y^{(i)}) \leq q(d_x^{(i)} + d_y^{(i)})/2$. Let $n_*^{(i)}$ be the minimal integer such that $n_*^{(i)} > \frac{3}{2} d_*^{(i)} + \frac{1}{2} q - 2$ where $* = x, y$. Let us begin with interpolation of the restriction of ϕ to S_1 by some polynomial f_1 of bidegree $\leq (n_x^{(1)}, n_y^{(1)})$. Next interpolate $(\phi - f_1)/F_1$ on $S_2 \setminus S_1$ by polynomial f_2 of bidegree $\leq (n_x^{(2)}, n_y^{(2)})$. Note that $f_1 + F_1 f_2$ agrees with ϕ on $S_1 \cup S_2$. Next we interpolate $(\phi - f_1 - F_1 f_2)/(F_1 F_2)$ on $S_3 \setminus (S_1 \cup S_2)$ and so on. In the end we obtain the interpolating polynomial of ϕ on S in the form $f = f_1 + F_1 f_2 + F_1 F_2 f_3 + \ldots$ where $\mathrm{bideg} F_i \leq (n_x^{(i)}, n_y^{(i)})$. Then $\deg_x f \leq \max(n_x^{(i)} + \sum_{j \neq i} d_x^{(j)}) \leq \max(\frac{3}{2} d_x^{(i)} + \frac{1}{2} q - 1 + \sum_{j \neq i} d_x^{(j)}) \leq \frac{3}{2} d_x + \frac{1}{2} q - 1$. The analagous estimate holds for $\deg_y f$ so we are done ▮.

References

[1] R.Hartshorne, *Algebraic geometry* (Springer-Verlag,1977).