A nice condition for linearity

Sophex – University of Texas at Austin

January 31st, 2003

Matilde N. Lalín

1 A condition for linearity

We are going to prove the following:

Theorem 1 *Let p be an odd prime. Then the map*

$$\phi : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p$$

is linear if and only if it satisfies the following two conditions:

1. $\phi(\alpha\, v) = \alpha\, \phi(v)$ *for all* $v \in \mathbb{F}_p^2$ *and* $\alpha \in \mathbb{F}_p$
2. $\sum_{v\in l} \phi(v) = 0$ *for all affine lines* $l \subset \mathbb{F}_p^2$

PROOF. The set of all functions $\phi : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p$ is a $\mathbb{F}_p$-vector space of dimension p^2, while the set of linear functions is a subspace of dimension 2. It is clear that linear functions satisty conditions 1 and 2. Hence, the set of functions satisfying these conditions is a subspace whose dimension is greater or equal than 2. We are going to prove that the dimension is at most 2, and that will prove the statement.

Consider a point $P \in \mathbb{F}_p^2$. There are exactly $p+1$ lines passing through P, one for each possible direction:

$$D := \{(0,1), (1,0), (1,1), \dots (1, p-1)\} \tag{1}$$

Suppose ϕ satisfies the conditions of the statement. Because of condition 1, ϕ is completely determined by its values in the set D (think of the lines through the origin). Then the subspace of functions satisfying condition 1 has dimension $p+1$.

Now we add condition 2. If $(0,0) \in l$, we get $\sum_{v\in l} \phi(v) = 0$ from condition 1. Hence it is enough to consider lines that do not pass through the origin.

Let l be any line through the origin, and $P, Q \in \mathbb{F}_p^2 \setminus l$. Claim:

$$\sum_{v\in l+P} \phi(v) = 0 \Leftrightarrow \sum_{v\in l+Q} \phi(v) = 0 \tag{2}$$

If $l + P = l + Q$, the claim is trivial. Otherwise, there must be some $\alpha \in \mathbb{F}_p$, $\alpha \neq 1$, such that $\alpha P \in l + Q$ (otherwise we would have that l is the line through the origin and P, which contradicts the fact that $P \notin l$). Now $\alpha \neq 0$ (because $(0,0) \notin l + Q$). We have

$$\sum_{v\in l+Q} \phi(v) = \sum_{v\in l+\alpha P} \phi(v) = \sum_{\alpha w\in \alpha l+\alpha P} \phi(\alpha w) = \alpha \sum_{w\in l+P} \phi(w)$$

and that proves the claim.

Hence, we are able to reduce condition 2 to the following:

$$\sum_{v \in l+(1,0)} \phi(v) = 0 \qquad \text{for all} \quad l \quad \text{through} \quad (0,0), \quad l \neq \{(t,0)\} \tag{3}$$

$$\sum_{v \in \{(t,0)\}+(0,1)} \phi(v) = 0 \tag{4}$$

Using the fact that the directions are given by the elements of D,

$$\sum_{t=0}^{p-1} \phi((at+1,t)) = 0 \qquad \text{for} \quad a = 0, 1, \ldots, p-1 \tag{5}$$

When $a = 0$, the condition is

$$\sum_{t=0}^{p-1} \phi((1,t)) = 0 \tag{6}$$

When $a \neq 0$,

$$\begin{aligned} \sum_{t=0}^{p-1} \phi((at+1,t)) &= \sum_{t=0,\ t \neq -a^{-1}}^{p-1} (at+1)\, \phi\left(\left(1, \frac{t}{at+1}\right)\right) - \frac{1}{a}\phi((0,1)) \\ &= \sum_{s=0,\ s \neq a^{-1}}^{p-1} \frac{1}{1-as}\, \phi\left((1,s)\right) - \frac{1}{a}\phi((0,1)) \end{aligned}$$

Observe that

$$\frac{1}{1-as} = \frac{a^{-1}}{a^{-1}-s}$$

and write $b = a^{-1}$. Then, because of

$$\frac{1}{b-s} = (b-s)^{p-2}$$

the family of equations (5) becomes

$$\sum_{s=0}^{p-1} (b-s)^{p-2}\, \phi\left((1,s)\right) - \phi((0,1)) = 0 \qquad \text{for} \quad b = 1, \ldots, p-1 \tag{7}$$

We also get the additional equation

$$\sum_{t=0}^{p-1} \phi((t,1)) = 0 \tag{8}$$

which is equivalent to

$$\phi((0,1)) + \sum_{s=1}^{p-1} \frac{1}{s}\phi((1,s)) \tag{9}$$

So we have $p+1$ equations on the $p+1$ variables

$$\phi((0,1)),\ \phi((1,0)),\ \phi((1,1)), \ldots, \phi((1,p-1)) \tag{10}$$

The corresponding matrix is

$$M = \left(\begin{array}{cccc} 1 & 0 & s^{-1} & \\ 0 & 1 & \dots & 1 \\ -1 & & & \\ \vdots & & (b-s)^{p-2} & \\ -1 & & & \end{array} \right) \tag{11}$$

This matrix has size $(p+1) \times (p+1)$. We will be done if we prove that its rank is greater or equal than $p-1$. In order to do that, we will prove that the minor

$$H = \left\{ (b-s)^{p-2} \right\}_{1 \leq b,\, s \leq p-1} \tag{12}$$

has determinant $\det(H) = 1 \neq 0$. We need the following:

Lemma 2

$$\det \left(\left\{ (a_i - b_j)^{n-1} \right\}_{1 \leq i,\, j \leq n} \right) = \prod_{k=1}^{n-1} (n-k)^{n-2k} \cdot \prod_{j>i} (a_j - a_i)(b_j - b_i) \tag{13}$$

PROOF. Observe that

$$\left\{ (a_i - b_j)^{n-1} \right\}_{i,\, j} = \begin{pmatrix} a_i^{n-1} & -\binom{n-1}{1} a_i^{n-2} & \dots & (-1)^{n-2} \binom{n-1}{n-2} a_i & (-1)^{n-1} \end{pmatrix}_i \begin{pmatrix} 1 \\ b_j \\ \vdots \\ b_j^{n-2} \\ b_j^{n-1} \end{pmatrix}_j$$

Now we compute determinants by using Vandermonde:

$$\det \left(\left\{ (a_i - b_j)^{n-1} \right\}_{i,\, j} \right) = (-1)^{\left[\frac{n}{2}\right]} \prod_{k=0}^{n-1} (-1)^k \binom{n-1}{k} \cdot \prod_{j>i} (a_j - a_i) \cdot \prod_{j>i} (b_j - b_i)$$

Computing

$$(-1)^{\left[\frac{n}{2}\right]} \prod_{k=0}^{n-1} (-1)^k \binom{n-1}{k} = \prod_{k=0}^{n-1} \frac{(n-1)!}{k!\,(n-k-1)!} = \frac{1^n \cdot 2^n \cdots (n-1)^n}{1^{2(n-1)} \cdot 2^{2(n-2)} \cdots (n-1)^{2 \cdot 1}}$$

and we are done. □

Back to the Proof of Theorem 1, we apply the Lemma above,

$$\det(H) \quad = \quad \det \left(\left\{ (b-s)^{p-2} \right\}_{b,\, s} \right) = \prod_{k=1}^{p-2} (p-1-k)^{p-1-2k} \prod_{j>i} (j-i)^2$$

$$\begin{aligned} &= \prod_{k=1}^{p-2}(k+1)^{-2k}\prod_{j=1}^{p-1}((j-1)!)^2 = \frac{1^{2(p-1)}\cdot 2^{2(p-2)}\cdots(p-2)^{2\cdot 2}}{2^{2\cdot 1}\cdot 3^{2\cdot 2}\cdots(p-1)^{2\cdot(p-2)}} \\ &= \frac{1^{2(p-1)}\cdot 2^{2(p-2)}\cdots(p-2)^{2\cdot 2}}{(p-2)^{2\cdot 1}\cdot(p-3)^{2\cdot 2}\cdots 1^{2\cdot(p-2)}} = ((p-2)!)^2 = 1 \end{aligned}$$

by Wilson's Theorem. □

A second Proof can be found in Lemma 7.7 of [3]. The advantage of this proof is that it can be generalized to the following

Theorem 3 *Let p be an odd prime. Then the space of functions $\phi : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p$ such that*

1. *$\phi(\alpha\, v) = \alpha\, \phi(v)$ for all $v \in \mathbb{F}_p^n$ and $\alpha \in \mathbb{F}_p$*
2. *$\sum_{v\in\mathcal{H}} \phi(v) = 0$ for all affine hyperplanes $\mathcal{H} \subset \mathbb{F}_p^n$*

has dimension

$$\frac{p^n-1}{p-1} - \binom{n+p-3}{n-1} \tag{14}$$

Remark 4 *Observe that the space of linear functions has dimension n.*

For $n = 2$, the dimension of the set of functions satistying the statement is

$$\frac{p^2-1}{p-1} - \binom{p-1}{1} = p+1-(p-1) = 2$$

and we recover Theorem 1.

In fact, the only case where linear functions are exactly the ones that satisfy the statement of Theorem 3 (for fixed n and every p) is when $n = 2$.

PROOF. (Sketch) ϕ can be written in a unique way as a polynomial in n variables, of degree at most $p-1$ in each of the variables:

$$\phi(\mathbf{x}) = \sum_{0\,\leq\,\mathbf{I}\,\leq\,p-1} a_{\mathbf{I}}\, \mathbf{x}^{\mathbf{I}} \tag{15}$$

Consider condition 1,

$$\phi(\alpha\, \mathbf{x}) = \sum_{0\,\leq\,\mathbf{I}\,\leq\,p-1} a_{\mathbf{I}}\, \alpha^{|\mathbf{I}|}\, \mathbf{x}^{\mathbf{I}} \overset{?}{=} \sum_{0\,\leq\,\mathbf{I}\,\leq\,p-1} a_{\mathbf{I}}\, \alpha\, \mathbf{x}^{\mathbf{I}} = \alpha\, \phi(\mathbf{x})$$

We conclude that we must have $\alpha = \alpha^{|\mathbf{I}|}$ for every α when $a_{\mathbf{I}} \neq 0$, hence, ϕ satisfies condition 1 if and only if

$$a_{\mathbf{I}} = 0 \qquad \text{for all} \quad \mathbf{I} \quad \text{with} \quad |\mathbf{I}| \not\equiv 1 \bmod (p-1) \tag{16}$$

Now consider condition 2. We claim that

$$a_{\mathbf{I}} = 0 \qquad \text{for all} \quad \mathbf{I} \quad \text{with} \quad |\mathbf{I}| \geq (n-1)(p-1) \tag{17}$$

Take any plane $\mathcal{H}$ that does not pass throught the origin (if it passes through the origin, condition 1 implies condition 2 is trivial for $\mathcal{H}$). It can defined by a formula of the form

$$b_1\,x_1 + \ldots + b_n\,x_n = 1 \qquad \text{for} \quad (b_1, \ldots, b_n) \in \mathbb{F}_p^n \setminus \{0\}$$

the map

$$\phi \longrightarrow s_\phi(\mathbf{b}) = \begin{cases} \sum_{v\in\mathcal{H}} \phi(v) & \text{if} \quad \mathbf{b} \in \mathbb{F}_p^n \setminus \{0\} \\ \\ \qquad 0 & \text{if} \quad \mathbf{b} = 0 \end{cases}$$

is an endomorphism of the spaces of maps $\mathbb{F}_p^n \longrightarrow \mathbb{F}_p$.

We want to see the action of this endomorphism on the monomials. Assume $b_n \neq 0$. Then

$$\begin{aligned} s_{\mathbf{x}^\mathbf{I}}(\mathbf{b}) &= \sum_{\mathbf{x}\in\mathcal{H}} \mathbf{x}^\mathbf{I} = \sum_{\mathbf{x_{(n-1)}}\in\mathbb{F}_p^{n-1}} \mathbf{x_{(n-1)}}^{\mathbf{I_{(n-1)}}} (b_n^{-1}(1 - b_1x_1 - \ldots - b_{n-1}x_{n-1}))^{i_n} \\ &= b_n^{-i_n} \sum_{\mathbf{J_{(n-1)}}\in\mathbb{F}_p^{n-1}} \binom{i_n}{\mathbf{J_{(n-1)}}} (-\mathbf{b_{(n-1)}})^{\mathbf{J_{(n-1)}}} \sum_{\mathbf{x_{(n-1)}}\in\mathbb{F}_p^{n-1}} \mathbf{x_{(n-1)}}^{\mathbf{I_{(n-1)}}+\mathbf{J_{(n-1)}}} \end{aligned}$$

Now use that

$$\sum_{x\in\mathbb{F}_p} x^k = \begin{cases} -1 & \text{if } p-1\,|\,m \quad \text{and} \quad m > 0 \\ \ \ 0 & \text{otherwise} \end{cases}$$

Hence, every term is zero unless

$$p - 1\,|\,i_l + j_l \qquad \text{for} \quad l = 1, \ldots, n \tag{18}$$

If $i_l \neq p-1$, we take $j_l = p - 1 - i_l$, but if $i_l = p-1$ we may take $j_l = 0$ or $p-1$.

Suppose some $i_l = p-1$, let us say $i_1, \ldots, i_k \neq p-1$ and $i_{k+1} = \ldots = i_{n-1} = p-1$ (k may be equal to $n-1$). Choose a plane with $b_{k+1}, \ldots, b_n \neq 0$. We get

$$s_{\mathbf{x}^\mathbf{I}}(\mathbf{b}) = b_n^{-i_n} \sum_{\alpha_l} \binom{i_n}{\mathbf{p-1-I_{(k)}}, \alpha_{k+1}, \ldots, \alpha_{n-1}} (-\mathbf{b_{(k)}})^{\mathbf{p-1-I_{(k)}}} (-1)^{n-1}$$

Here each α_l is either 0 or $p-1$. Note that we have not asked any condition to i_n.

First suppose $k = 0$, so all $i_l = p-1$ except, maybe i_n. Take the hyperplane defined by the equation $x_n = 1$, then

$$s_{\mathbf{x}^\mathbf{I}}(\mathbf{b}) = \sum_{\mathbf{x_{(n-1)}}\in\mathbb{F}_\mathbf{p}^{\mathbf{n-1}}} \mathbf{x_{(n-1)}}^{\mathbf{p-1}} = (-1)^{n-1} \neq 0$$

so $a_\mathbf{I} = 0$ in this case.

Now when $k > 0$ and some $\alpha_l = p-1$ the multinomial is zero, so the only term that survives is the one with every $\alpha_l = 0$, provided that

$$(p-1-i_1) + \ldots + (p-1-i_k) \leq i_n$$

In other words, $k(p-1) \leq i_1 + \ldots + i_k + i_n$ implies the term is nonzero, so $a_\mathbf{I} = 0$. Now recall that $i_{k+1} = \ldots = i_{n-1} = p-1$.

So, whenever

$$(n-1)(p-1) \leq |\mathbf{I}| \quad \text{we must have } a_{\mathbf{I}} = 0$$

We have proved the claim, let us summarize, the only $a_{\mathbf{I}}$ that can be choosen freely are the ones such that

$$\begin{aligned}\sum_{l=1}^{n} i_l &\equiv 1 \mod (p-1) && (19)\\ \sum_{l=1}^{n} i_l &< (n-1)(p-1) && (20)\\ & && (21)\end{aligned}$$

The possible solutions for $0 \leq \mathbf{I} < p$ are all the solutions to the equation (19) except for the ones with

$$\sum_{l=1}^{n} i_l = (n-1)(p-1) + 1 \tag{22}$$

This equation has

$$\binom{p-2+n-1}{n-1}$$

solutions (set all the n places to be equal to $p-1$ and the distribute $p-2$ numbers "-1").

Equation (19) has

$$\frac{p^n-1}{p-1}$$

solutions (by induction).

So, the dimension of the kernel of s_ϕ is

$$\frac{p^n-1}{p-1} - \binom{n+p-3}{n-1} \tag{23}$$

□

Considering the problem without asking the homogenity condition,

Theorem 5 *Let p be an odd prime. Then the space of functions $\phi : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p$ such that*

$$\sum_{v \in \mathcal{H}} \phi(v) = 0$$

for all affine hyperplanes $\mathcal{H} \subset \mathbb{F}_p^n$ has dimension

$$p^n - \binom{n+p-1}{n} \tag{24}$$

PROOF. The problem here is that we need to considerate also the hyperplanes that contain the origin (we did not consider them before because the were ruled out by condition 1).

Let $\mathcal{H}$ be such a hyperplane, which we can suppose it is given by $x_n = b_1x_1 + \ldots + b_{n-1}x_{n-1}$. Then s_ϕ acts also on the functions $\mathbb{F}_p^{n-1} \longrightarrow \mathbb{F}_p$.

$$s_{\mathbf{x}^{\mathbf{I}}}(\mathbf{b_{(n-1)}}) = \sum_{\mathbf{x_{(n-1)}} \in \mathbb{F}_p^{n-1}} \mathbf{x_{(n-1)}}^{\mathbf{I_{(n-1)}}} (b_1 x_1 + \ldots + b_{n-1} x_{n-1}))^{i_n}$$

$$= \sum_{\mathbf{J_{(n-2)}} \in \mathbb{F}_p^{n-2}} \binom{i_n}{\mathbf{J_{(n-2)}}} \mathbf{b_{(n-2)}}^{\mathbf{J_{(n-2)}}} b_{n-1}^{i_n - |\mathbf{J_{(n-2)}}|} \sum_{\mathbf{x_{(n-1)}} \in \mathbb{F}_p^{n-1}} \mathbf{x_{(n-2)}}^{\mathbf{I_{(n-2)}} + \mathbf{J_{(n-2)}}} x_{n-1}^{i_{n-1} + i_n - |\mathbf{J_{(n-2)}}|}$$

As before we want to see for what cases $s_{\mathbf{x}^{\mathbf{I}}}(\mathbf{b_{(n-1)}}) \neq 0$. We need that each component of the vector $\mathbf{I_{(n-2)}} + \mathbf{J_{(n-2)}}$ is a positive multiple of $p-1$, but on the other hand, $i_{n-1} + i_n - |\mathbf{J_{(n-2)}}|$ is also a positive multiple of $p-1$. Adding both terms,

$$|\mathbf{I_n}| \geq (n-1)(p-1)$$

Hence, the hyperplanes through the origin do not add any restrictions to the functions. Therefore, we can restrict ourselves to the condition given by equation (20).

The total dimension is p^n and the number of solutions to $|\mathbf{I}| \geq (n-1)(p-1)$ is

$$\binom{n-1}{n-1} + \binom{n-1+1}{n-1} + \ldots + \binom{n-1+p-1}{n-1} = \binom{n+p-1}{n}$$

(set $p-1$ in each place and distribute: 0, $1, \ldots, p-1$ numbers "-1"). The equality comes from the identity

$$\binom{k}{k} + \binom{k+1}{k} + \ldots + \binom{k+j}{k} = \binom{k+j+1}{k+1}$$

Hence, the dimension of the kernel of s_ϕ is

$$p^n - \binom{n+p-1}{n} \tag{25}$$

□

2 Radon Transform

Let us make some comments about the above statements. The first condition is a quite natural one. What does the second condition mean?

Definition 6 *Let X be a finite set and $\mathcal{S}$ a class of subsets of X. Let K be a field and $\phi : X \longrightarrow K$ a function. The (finite) Radon transform of ϕ is the function $\hat{\phi} : \mathcal{S} \longrightarrow K$ such that*

$$\hat{\phi}(S) := \sum_{x \in S} \phi(x)$$

In Theorem 1, we are taking $\mathbb{F}_p^2$ as the finite set X and $\mathcal{S}$ is the class of lines. Condition 2 means that ϕ is in the kernel of the Radon transform.

Discrete Radon trasforms are used in applied statistics. They are defined in analogy with the ordinary Radon transform:

Definition 7 *Let $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ a function satisfying certain integrality properties. The Radon transform $\hat{f}$ is a real-valued function defined on the affine hyperplanes of $\mathbb{R}^n$:*

$$\hat{f}(\mathcal{H}) = \int_{\mathcal{H}} f \tag{26}$$

The central problem of this theory is the *reconstruction problem*: Is the Radon transform invertible? Can we reconstruct f from $\hat{f}$?

Following Bolker in [1], we write

$$G_x := \{S \in \mathcal{S} | x \in S\}$$

Bolker proves the following:

Theorem 8 *Suppose that the cardinality of G_x is independent of x,*

$$\#(G_x) = \alpha \textit{ for all } x \in X$$

and that

$$\#(G_x \cap G_{x'}) = \beta \neq \alpha$$

independent of x and x'. Then the Radon transform is injective and its inverse is

$$\phi(x) = \frac{1}{\alpha - \beta} \sum_{S \in G_x} \hat{\phi}(S) - \frac{\beta}{\alpha(\alpha - \beta)} \sum_{S \in \mathcal{S}} \hat{\phi}(S)$$

In our case, G_x is the set of lines through a fixed point, then $\alpha = p + 1 = 1$. Given two points there is exactly one line that passes through both of them, so $\beta = 1$, then Theorem 8 can not be applied, which is consistent with the fact that we have a nontrivial kernel.

References

[1] E. D. Bolker, The Finite Radon Transform, *Integral Geometry* (Brunswick, Maine, 1984), 27–50 *Contemp. Math.* **63** Amer. Math. Soc. Providence, RI, 1987.

[2] J. P. S. Kung, Radon Transforms in Combinatorics and Lattice Theory, *Combinatorics and ordered sets* (Arcata, Calif., 1985), 33–74, *Contemp. Math.***57** Amer. Math. Soc. Providence, RI, 1986.

[3] E. F. Schaefer and M. Stoll, How to do a p-Descent on an Elliptic Curve (preprint).

[4] A. V. Zelevinski, Generalized Radon Transforms in Spaces of Functions on Grassmann Manifolds over a Finite Field, *Uspekhi Mat. Nauk.* **28** (1973), no. 5(173), 243–244.