Linear forms in p-adic roots of unity

John Tate and José Felipe Voloch

1. Introduction

In this note we will prove the following inequality for linear forms in p-adic roots of unity (Theorem 2 below). For fixed $a_1, \ldots, a_n \in \mathbf{C}_p$, the completion of the algebraic closure of $\mathbf{Q}_p$, there exists a constant $c > 0$ such that for any roots of unity $\zeta_1, \ldots, \zeta_n$ in $\mathbf{C}_p$ either $\sum \zeta_i a_i = 0$ or $|\sum \zeta_i a_i| \geq c$. The proof splits into two steps. First we show the result is true if the roots of unity are restricted to have order prime to p and the a_i are in an unramified extension of $\mathbf{Q}_p$, and then we reduce the general case to that case. We will be able to say a lot more in the situation of the first step and develop an analogy with a similar problem in power series fields.

Let $K = k((t))$ be the field of formal power series over a field k. Let $a_1, \ldots, a_n$ be elements of K, not all zero. We can think of $(a_1 : \ldots : a_n)$ as a branch of an analytic curve in $\mathbf{P}^{n-1}$, parametrized by t, in an infinitesimal neighbourhood of the point $P_0 = (a_1(0) : \ldots : a_n(0))$ (assuming that the a_i are scaled so that they do not have a pole and not all vanish at $t = 0$). There is a descending sequence $\mathbf{P}^{n-1} = V_0 \supseteq V_1 \supseteq V_2 \supseteq \cdots$ of linear subspaces of $\mathbf{P}^{n-1}$ such that, for each $m \geq 0$

$$V_m(k) = \{(\zeta_1 : \ldots : \zeta_n) \in \mathbf{P}^{n-1}(k) \mid \sum_{i=1}^{n} \zeta_i a_i \equiv 0 \pmod{t^m}\}.$$

Indeed, the congruence in question amounts to m linear conditions on the indeterminate constants $\zeta_1, \ldots, \zeta_n$. Geometrically, we view $\zeta_1, \ldots, \zeta_n$ as the coordinates of the hyperplane $\sum \zeta_i X_i = 0$ and interpret V_m as the space of hyperplanes in $\mathbf{P}^{n-1}$ which meet our branch with multiplicity at least m at P_0. The fact that the descending sequence $V_0 \supseteq V_1 \supseteq \cdots$ becomes stationary shows that there exists a positive constant c such that for any $\zeta_1, \ldots, \zeta_n \in k$, either $\sum \zeta_i a_i = 0$ or $|\sum \zeta_i a_i| \geq c$. Indeed, if $V_m = V_{m_0}$ for $m \geq m_0$, then $|\sum \zeta_i a_i| \leq |t|^{m_0}$ implies $\sum \zeta_i a_i = 0$, so we can take $c = |t|^{m_0 - 1}$.

We wish to consider a p-adic analogue of this inequality. So we will take an unramified local field K of characteristic zero with perfect residue field k of characteristic $p > 0$, and $a_1, \ldots, a_n \in K$. As K has no constant field, we take as replacement the set of Teichmüller representatives of the elements of of k, which we denote by $T(k)$. Denote the absolute value on K by $|.|$.

Theorem 1. *Let K be as above. Given $a_1, \ldots, a_n \in K$, there exists a positive constant c such that for $\zeta_1, \ldots, \zeta_n \in T(k)$, either $\sum \zeta_i a_i = 0$ or $|\sum \zeta_i a_i| \geq c$.*

Proof: Without loss of generality, we can assume that k is algebraically closed and that $a_1, \ldots, a_n$ are in the ring of integers of k, which we can identify with the ring of Witt vectors of infinite length over k. For $z \in k$ we let $T(z)$ denote its Teichmüller representative $T(z) = (z, 0, 0, \ldots)$, and we will often write $\zeta = T(z)$, using Greek letters for elements of $T(k)$ and the corresponding latin letters for their residue classes in k. Since the Witt vectors of length m form a ring scheme and T is multiplicative, the condition $\sum \zeta_i a_i \equiv 0 \pmod{p^m}$, for $\zeta_i = T(z_i)$, translates into a set of m homogeneous polynomial equations in $z_1, \ldots, z_n$ and therefore defines a closed subscheme V_m of $\mathbf{P}^{n-1}$ over k. Moreover, the V_m form a decreasing sequence, so must become constant. If $V_{m_0} = V_m$, for $m > m_0$, then any $\zeta_1, \ldots, \zeta_n \in T(k)$ whose residues $z_1, \ldots, z_n$ define a point in V_{m_0} satisfies $\sum \zeta_i a_i = 0$ and all others satisfy $|\sum \zeta_i a_i| \geq |p|^{m_0 - 1}$. This completes the proof.

Remark: It was pointed out to us by Buium and Serre that Theorem 1 can be considerably generalized. See §3, remark (iii).

By analogy with the power series case we will call $(a_1 : \ldots : a_n)$ a p-adic curve germ and think of the scheme V_m as parametrizing the hyperplanes $\sum \zeta_i X_i = 0$ with "constant" coefficients $\zeta_i \in T(k)$ which intersect it with multiplicity at least m. The reader who is interested only in the inequalities needs only to know the existence of the schemes V_m for the proof of Theorem 1 and can skip §2, which is devoted to an investigation of some of their properties. In contrast to the power series case, the p-adic V_m are in general not linear, not irreducible, not smooth, not reduced and not equidimensional, although for m

small relative to the number of a_i not divisible by p, some of these properties do hold (Proposition 1).

In §3 we carry out the reduction of Theorem 2 to a special case of Theorem 1, first reducing to the case the a_i are in $\mathbf{Q}_p$ (even to $a_i = \pm 1$), then to the case that, in addition, the roots of unity are of order prime to p.

In §4 we discuss briefly the global sitution, in which the $a_1, \ldots, a_n$ are in a number field K. Thinking of K as the function field of a non-existent curve, we think of $(a_1 : \ldots : a_n)$ as a map of the curve to $\mathbf{P}^{n-1}$. This point of view has been dubbed "geometry over the field of one element". The interested reader may consult [D],[M] or [Sm] for more on this. (See also [B1] and [I], which are perhaps in the same spirit.) This paper is partly motivated by a question in [Sm]. There he treats the case $n = 2$, where the local theory is trivial, and makes some global conjectures. He asks about a possible higher dimensional generalization of his conjecture. Here we give a possible local theory towards such a generalization. Although we stop short of making a higher dimensional conjecture we discuss some global questions.

2. The unramified case

Let K be an unramified local field of characteristic zero and perfect residue field k of characteristic $p > 0$. We identify the ring of integers of K with the ring of Witt vectors $W_\infty(k)$. If $x_i, 1 \leq i \leq n$ are integers in K with representations $x_i = (x_{i0}, x_{i1}, \ldots)$, the Witt vector of their sum is $\sum_{i=1}^n x_i = (f_0(x), f_1(x), \ldots)$, where the sequence of polynomials f_m in the variables x_{ij} is defined inductively by

$$f_0^{p^m} + p f_1^{p^{m-1}} + \ldots + p^m f_m = \sum_{i=1}^n \big(x_{i0}^{p^m} + p x_{i1}^{p^{m-1}} + \ldots + p^m x_{im} \big)$$

for $m = 0, 1, 2, \ldots$ Thus,

$$f_0(x) = \sum_{i=1}^n x_{i0}, \quad f_1(x) = \sum_{i=1}^n x_{i1} + \frac{1}{p} \big(\sum_{i=1}^n x_{i0}^p - (\sum_{i=1}^n x_{i0})^p \big)$$

and, in general, f_m is a polynomial of degree p^m in the variables $x_{ij}, 1 \leq i \leq n, 0 \leq j \leq m$, with rational integer coefficients.

Suppose $a_i, 1 \leq i \leq n$, are integers in K with representations $a_i = (a_{i0}, a_{i1}, \ldots)$. For variable $z_1, \ldots, z_n \in k$ with Teichmüller representatives $\zeta_i = T(z_i) = (z_i, 0, 0, \ldots)$ we have then $\zeta_i a_i = (a_{i0}z_i, a_{i1}z_i^p, a_{i2}z_i^{p^2}, \ldots)$ for each i and hence $\sum_{i=1}^n \zeta_i a_i = (F_0(z), F_1(z), \ldots)$, where the polynomials $F_m(z) \in k[z_1, \ldots, z_n]$ are defined by $F_m(z) = f_m(x)$, where $x_{ij} = a_{ij}z_i^{p^j}$.

Assume now that not all a_i are divisible by p and let R be a local k-algebra. For $(z_1 : \ldots : z_n) \in \mathbf{P}^{n-1}(R)$ and $\zeta_i = T(z_i) \in W_\infty(R)$ we have that $\sum \zeta_i a_i$ is divisible by p^m if and only if $F_j(z_1, \ldots, z_n) = 0$ for $0 \leq j < m$, which is equivalent to $(z_1 : \ldots : z_n) \in V_m(R)$ where V_m is defined to be the scheme of common zeros of $F_0, F_1, \ldots, F_{m-1}$. As explained in the introduction, we view V_m as the scheme parametrizing hyperplanes meeting our p-adic curve germ $(a_1 : \ldots : a_n)$ with multiplicity at least m. Clearly V_m depends only on the point $(a_1 : \ldots : a_n) \in \mathbf{P}^{n-1}(K)$.

In order to study the varieties V_m we will study their singularities.

Lemma 1. *On V_m, the following identity holds: $\partial F_m/\partial z_i = a_{i0}^{p^m} z_i^{p^m - 1}$.*

Proof: Differentiating the recurrence relation defining the f_m, dividing by p^m and substituting $x_{ij} = a_{ij}z_i^{p^j}$ gives $dF_m(z) = \sum_{i=1}^n a_{i0}^{p^m} z_i^{p^m-1} dz_i$ on V_m as claimed, because $dx_{ij} = 0$ for $j > 0$ and $F_j(z) = 0$ on V_m for $j < m$.

Proposition 1. *With $a_1, \ldots, a_n$ as above, let $r = \sharp\{i | a_i \equiv 0 \mod p\}$. Then,*

(i) If $m < (n+2-r)/3$, V_m is irreducible and generically smooth, of dimension $n-1-m$.

(ii) If $m < (n+1-r)/2$, each irreducible component of V_m is generically smooth, of dimension $n-1-m$; in fact, its singular locus is of codimension at least $n+1-r-2m$.

(iii) If $m = (n+1-r)/2$, each irreducible component of V_m is of dimension $n-1-m$ (but may not be reduced).

(iv) If $m = (n+2-r)/2$, each irreducible component W of V_m is of dimension $n-1-m$ unless, after some permutation of the indices there are non-zero Teichmüller

representatives $\zeta_i, 1 \le i \le m-1$, *such that* $a_i + \zeta_i a_{i+m-1} \equiv 0 \pmod{p^m}$ *for* $1 \le i \le m-1$, *and* $a_i \equiv 0 \pmod{p^m}$ *for* $n-r+1 \le i \le n$, *in which case,* W_{red} *is the linear space of all* $z_1, \ldots, z_n$ *such that, after the permutation of indices,* $a_{i0} z_i + a_{i+m-1,0} z_{i+m-1} = 0,\ 1 \le i \le m-1$.

Proof: The Jacobian matrix of V_m, by Lemma 1, is proportional to

$$\begin{pmatrix} a_{10}z_1 & a_{20}z_2 & \cdots & a_{n0}z_n \\ (a_{10}z_1)^p & (a_{20}z_2)^p & \cdots & (a_{n0}z_n)^p \\ \vdots & \vdots & \ddots & \vdots \\ (a_{10}z_1)^{p^{m-1}} & (a_{20}z_2)^{p^{m-1}} & \cdots & (a_{n0}z_n)^{p^{m-1}} \end{pmatrix}$$

Let Z_m be the variety of points in $\mathbf{P}^{n-1}$ where this matrix does not have maximal rank. The $(m \times m)$-minors of this matrix are Moore determinants which factor as a product of all (up to proportionality) non-trivial linear combinations of the elements of their first row with coefficients in $\mathbf{F}_p$ ([Mo]).

The variety Z_m is thus the union of finite set of linear subspaces W of $\mathbf{P}^{n-1}$, one for each assignment $I \mapsto L_I$ which associates to each m-element subset $I \subset \{1, 2, \ldots, n\}$ a non-zero linear form L_I whose coefficients are in $\mathbf{F}_p$ and vanish for $i \notin I$, the corresponding W being the variety of common zeros of the forms $L_I(a_{01}z_1, \ldots, a_{0n}z_n)$. The dimension of W is at most $m-2+r$; otherwise, for some $(m+r)$-element subset $J \subset \{1, 2, \ldots, n\}$ the projection of W onto the corresponding $\mathbf{P}^{m+r-1}$ would be surjective. But this is impossible, because J contains an m-element subset I such that $a_{i0} \neq 0$ for $i \in I$, and the corresponding L_I would not vanish on W. Hence each irreducible component of Z_m has dimension at most $m-2+r$.

Since V_m is cut out by m equations, each irreducible component W of V_m is of dimension at least $n-1-m$, with equality and W generically smooth if $W_{\mathrm{red}} \not\subset Z_m$. However, $W \cap Z_m$ is of codimension at least $n+1-r-2m$ in W, by the above, which proves (ii). If $\dim W > n-1-m$, then $W_{\mathrm{red}} \subset Z_m$, so $n-1-m < m-2-r$, i.e., $2m > n+1-r$. This proves (iii).

To prove (i), note first that V_1 is a hyperplane. Suppose $1 \le m < (n+2-r)/3$.

then, by (iii), the codimension of each component of V_m in V_1 is $m-1$. If V_m has two components, their intersection is of codimension at most $2m-2$ in V_1 and is contained in Z_m, which is impossible if $3m < n+2-r$. This proves (i).

To prove (iv), suppose $2m = n-r+2$. Put $h = m-1$ so that $n = 2h+r$. Permuting indices and dividing those $a_i \not\equiv 0 \pmod p$ by their Teichmüller representatives, we can suppose that $a_i \equiv 1 \pmod p$ for $i \le 2h$ and $a_i \equiv 0 \pmod p$, otherwise. Suppose W is a component of V_m of codimension less than m in $\mathbf{P}^{n-1}$. Reasoning as above shows that W is of codimension $h = m-1$, and that W_{red} is a component of Z_m, so is the set of common zeros of h independent linear forms involving only the variables $z_1, \dots, z_{2h}$, with coefficients in $\mathbf{F}_p$. After another permutation of the first $2h$ indices we can suppose that the linear forms have the shape $L_i = z_i + \sum_{j=1}^{h} c_{ij} z_{j+h}, 1 \le i \le h$, with $c_{ij} \in \mathbf{F}_p$. Thus W_{red} is parametrized by homogeneous variables $t_1, \dots, t_{h+r}$, via $z_i = -\sum_{j=1}^{h} c_{ij} t_j, 1 \le i \le h$ and $z_{i+h} = t_i, 1 \le i \le h+r$. The form F_h vanishes identically on W. Hence, by the lemma, we have, putting $N = p^h - 1$:

$$0 = \frac{\partial F_h}{\partial t_j} = \sum_{i=1}^{n} \frac{\partial F_h}{\partial z_i} \frac{\partial z_i}{\partial t_j} = \sum_{i=1}^{h} z_i^N (-c_{ij}) + z_{j+h}^N, \quad 1 \le j \le h.$$

Consequently, for all $t = (t_1, \dots, t_h) \in \bar{\mathbf{F}}_p^h$, whenever $z_i = -\sum_{j=1}^{h} c_{ij} t_j$ for all i, then

$$t_j^N = \sum_{i=1}^{h} z_i^N (c_{ij}). \qquad (*)$$

Putting $t_j = \delta_{jk}$ (Kronecker δ) yields $z_i = -c_{ik}$; hence, since $(-1)^N = 1$ in $\mathbf{F}_p$, $\delta_{jk} = \sum_{i=1}^{h} c_{ik}^N (c_{ij})$. This shows that (c_{ij}) is an invertible matrix. Let (b_{jk}) be the inverse matrix, so $b_{jk} = c_{kj}^N = 0$ or 1 and $t_j = -\sum_{i=1}^{h} b_{ji} z_i$. Substituting this into (*) yields an identity:

$$\Big(\sum_i b_{ji} z_i\Big)^N = \sum_i c_{ij} z_i^N.$$

We claim that (b_{jk}) is a permutation matrix. Indeed, if for some j, $b_{ji} = b_{ji'} = 1, i \ne i'$, then $h > 1$ and, putting $z_i = x, z_{i'} = y, z_s = 0, s \ne i, i'$ in the above identity, yields an identity $(x+y)^N = x^N + y^N$, which is impossible since N is not a power of p. Therefore (c_{ij})

is also a permutation matrix. After applying this permutation to the indices $h+i, 1 \leq i \leq h$ we obtain $L_i = z_i + z_{i+h}$ for each i. Thus, keeping this permutation of the indices, but going back to the original a_i, the reduced and irreducible component W of V_m of dimension at least $n-m$ is the linear space given by the equations $a_{i0}z_i + a_{i+h,0}z_{i+h} = 0, 1 \leq i \leq h$. By the definition of V_m, this means that $a_i + \zeta_i a_{i+h} \equiv 0 \pmod{p^m}$ for $\zeta_i = T(-a_{i0}/a_{i+h,0})$, $1 \leq i \leq h$, and $a_i \equiv 0 \pmod{p^m}$ for $2h < i \leq n$. This concludes the proof of Proposition 1.

The group $G_n = (T(k^*)^n \rtimes S_n)/T(k^*)$ acts on $\mathbf{P}^{n-1}$ and is the largest linear group keeping our statements invariant. It allows us to assume that $a_{i0} = 1$ for $1 \leq i \leq n-r$ and $a_{i0} = 0$ for $i > n-r$ if that is convenient, as in the proof above. The symmetric group S_n is sometimes said to be PGL_n over the field with one element; we leave to the reader a corresponding interpretation of G_n.

We define a p-adic curve germ to be non-singular, if there is a hyperplane with order of contact exactly 1. That means that $V_1 \neq V_2$. From the proposition, a p-adic curve germ is non-singular unless $r \geq n-2$, i.e., $r = n-2$ or $r = n-1$. For those r's, it is easy to see that a p-adic curve germ is non-singular unless $a_i \equiv 0 \mod p^2$ for each i such that $a_i \equiv 0 \mod p$ and, in the case $r = n-2$, if $a_j, a_k \not\equiv 0 \mod p$, $j \neq k$, then $-a_j/a_k \equiv T(-a_j/a_k) \mod p^2$. Another way to describe non-singularity when $r \geq n-2$ is as follows. If we consider the point $(a_{11}^{1/p} : \ldots : a_{n1}^{1/p})$, then for $r \geq n-2$ the p-adic curve germ is non-singular if and only if this point is well-defined in $\mathbf{P}^{n-1}(k)$ and is distinct from the point $(a_{10} : \ldots : a_{n0})$. Moreover, when this holds, V_2 is the dual linear space to the line joining these two points, with multiplicity p. This can proved using the explicit formulas for F_0, F_1 at the beginning of this section. Note the similarity with the function field case. Regardless of the value of r, if $(a_{11}^{1/p} : \ldots : a_{n1}^{1/p})$ is a well-defined point in $\mathbf{P}^{n-1}(k)$ and is distinct from $(a_{10} : \ldots : a_{n0})$, the line joining these points is invariant under the action of G_n on $(a_1 : \ldots : a_n)$, so is intrinsic to our problem. Surprisingly, this line does not seem to play any role if $r < n-2$.

If we are dealing with a p-adic plane curve germ , i.e., if $n = 3$, then we think of V_2 as the set of tangents. A consequence of the above discussion is that if the curve germ is

non-singular and $r > 0$ it has a unique tangent. The situation for $r = 0$, the generic case, is quite different.

Proposition 2. *A p-adic plane curve germ with $r = 0$ has at most p and, if p is odd, at least $(p+1)/2$ tangents.*

Proof: If $n = 3, r = 0$ then $V_1 \neq V_2$, by Proposition 1. Since V_1 is a line, it follows that V_2 is finite and thus has p elements counted with multiplicities, since $\deg F_1 = p$. As V_2 is the set of tangents, the first assertion follows. Assume now that p is odd. Let C be the plane curve defined by $F_1 = 0$. Then V_2 is the intersection of V_1 and C and we wish to study the intersection multiplicity at the points of V_2. The intersection multiplicity is one unless the Jacobian matrix below has rank less than two,

$$\begin{pmatrix} a_{10} & a_{20} & a_{30} \\ a_{10}^p z_1^{p-1} & a_{20}^p z_2^{p-1} & a_{30}^p z_3^{p-1} \end{pmatrix}$$

If the multiplicity is at least two then V_1 is tangent to C and this tangent is inflexional if and only if the Hessian, $\det(\partial^2 F_1/\partial z_i \partial z_j)$, vanishes. By Lemma 1, the Hessian equals $-(a_{10}a_{20}a_{30})^p (z_1 z_2 z_3)^{p-2}$ and, since $r = 0$, it vanishes only if one of the z_i's vanishes. But if that happens then the above Jacobian matrix has rank two, again since $r = 0$. It follows that V_1 cannot be an inflexional tangent to C and thus the points in V_2 have multiplicity at most two, proving the proposition.

Remark: The lower bound is sharp for small p, but a search for $11 \leq p \leq 100$ failed to produce any p-adic plane curve germs with $a_i \in \mathbf{Q}_p$ with $(p+1)/2$ tangents.

In the power series case, the V_m are a decreasing sequence of linear spaces, and either $V_m = V_{m+1}$ or V_{m+1} is of codimension 1 in V_m. In the p-adic case, however it can happen that V_m is reducible and V_{m+1} is a component of V_m. We will give some examples now. Start with $a_i = 1, i = 1, \ldots, 4$ and assume $p \neq 2$. Then V_∞ consists of three lines $(1 : -1 : z : -z), (1 : z : -z : -1), (1 : z : -1 : -z), z \in k$ and, if $p \neq 3$ and ω is a primitive cube root of unity, the eight points in the S_4-orbit of $(1 : \omega : \omega^2 : 0)$. This follows from Mann's Theorem ([Mn]). Now we perturb our curve a little. Take $a_i = 1, i = 1, 2, a_i = 1 + p^m, i = 3, 4$, where m is large. Then, the first line stays in V_∞ but

the other two are in $V_m \setminus V_{m+1}$. One can perturb further to make V_∞ empty but the first line to be V_n, for some $n > m$.

3. The general case

Theorem 2. *For every integer $n \geq 1$ and every family of n elements $a_1, \ldots, a_n \in \mathbf{C}_p$ there exists a constant $c > 0$ such that for any $\zeta_1, \ldots, \zeta_n$ roots of unity in $\mathbf{C}_p$ either $\sum \zeta_i a_i = 0$ or $|\sum \zeta_i a_i| \geq c$.*

Proof: First we show that by increasing n we can reduce to the case where the coefficients $a_1, \ldots, a_n$ are equal to ± 1. This reduction will be done by induction on the number of non-zero coefficients $a_1, \ldots, a_n$ which are distinct up to sign. If this number is 1 then all coefficients are equal, up to sign, and upon dividing by a_1 we get all coefficients equal to ± 1. For the general case, assume, without loss of generality, that $a_1 = 1$ and write $X = (X_1, \ldots, X_n)$ and

$$A(X) = \sum a_i X_i = \sum_{a_i \neq \pm 1} a_i X_i + \sum_{a_i = \pm 1} a_i X_i = B(X) + C(X),$$

say. Assume, by contradiction, that there is sequence $(\zeta^{(k)})$ of n-tuples of roots of unity in $\mathbf{C}_p$ with $A(\zeta^{(k)}) \neq 0$ but $A(\zeta^{(k)}) \to 0$ as $k \to \infty$. Note that $|B(\zeta^{(k)})| \leq \max\{|a_i|\}$. It follows that

$$B(\zeta^{(k)})C(\zeta^{(k+1)}) - C(\zeta^{(k)})B(\zeta^{(k+1)}) = B(\zeta^{(k)})A(\zeta^{(k+1)}) - B(\zeta^{(k+1)})A(\zeta^{(k)}) \to 0.$$

However, $B(\zeta^{(k)})C(\zeta^{(k+1)}) - C(\zeta^{(k)})B(\zeta^{(k+1)})$ can be written as the value of a linear form in roots of unity, namely,

$$\sum_{\substack{i,j \\ a_i \neq \pm 1 \\ a_j = \pm 1}} \pm a_i \zeta_i^{(k)} \zeta_j^{(k+1)} - \sum_{\substack{i,j \\ a_i \neq \pm 1 \\ a_j = \pm 1}} \pm a_i \zeta_i^{(k+1)} \zeta_j^{(k)},$$

the coefficients of which are equal to those of B, up to sign. Therefore this linear form has fewer non-zero coefficients distinct up to sign than A. From the induction hypothesis,

it follows that the sequence $B(\zeta^{(k)})/C(\zeta^{(k)})$ is eventually constant. Note that $C(\zeta^{(k)}) = A(\zeta^{(k)}) - B(\zeta^{(k)}) \neq 0$ for large k, since the theorem holds for $B(X)$ by the induction hypothesis. Since the theorem also holds for $C(X)$ by the induction hypothesis, it follows that $|C(\zeta^{(k)})| \geq c > 0$, for large k. Combining this with $A(\zeta^{(k)}) \to 0$, we conclude that $B(\zeta^{(k)})/C(\zeta^{(k)}) \to -1$ as $k \to \infty$. Hence $B(\zeta^{(k)})/C(\zeta^{(k)}) = -1$ for k large, which is a contradiction, since $A(\zeta^{(k)}) \neq 0$.

Next we suppose $a_i \in \mathbf{Q}_p, 1 \leq i \leq n$, and will reduce to the case the roots of unity ζ_i are of order prime to p, which is taken care of by Theorem 1. Choose a primitive p-th root of unity ξ and let $\mathcal{N}$ be a set of coset representatives for the p-power order roots of unity modulo the p-th roots of unity. Then each root of unity of p-power order can be written as $\eta\xi^j, \eta \in \mathcal{N},\ 0 \leq j \leq p-1$. Also, it is clear that every root of unity $\zeta \in \bar{\mathbf{Q}}_p$ can be written as $\zeta'\eta$, where the order of ζ' is not divisible by p^2 and $\eta \in \mathcal{N}$. Let F denote the maximal unramified extension of $\mathbf{Q}_p$.

Let $\zeta_1, \ldots, \zeta_n$ be roots of unity. Write each ζ_i as $\zeta_i'\eta_i$, where $\eta_i \in \mathcal{N}$ and the order of ζ_i' is not divisible by p^2, so $\zeta_i' \in F(\xi)$. We write

$$A = \sum a_i\zeta_i = \sum a_i\zeta_i'\eta_i = \sum_{\eta \in N} (\sum_{\eta_i = \eta} a_i\zeta_i')\eta.$$

Here $N \subset \mathcal{N}$ is a set of r elements, for some $r \leq n$. Let $M = \{\sigma_0, \ldots, \sigma_{r-1}\}$, where σ_j is an automorphism of $\bar{\mathbf{Q}}_p$ over F such that $\eta^{\sigma_j} = \eta^{1+pj}$ for p-power order roots of unity η. Note that each σ_j is the identity on $F(\xi)$. The determinant $\Delta := \det(\eta^\sigma)$ with η ranging in N and σ in M is equal to $\prod_{\eta \in N} \eta$ times $\det(\eta^{pj})$. The latter is a Vandermonde determinant in the η^p's, for $\eta \in N$. Since these η's are in distinct cosets modulo the p-th roots of unity, their p-th powers are distinct. It follows from Lemma 2 below that $|\Delta| \geq |p|^{\frac{n(n-1)}{2(p-1)}}$. Conjugating the above equation for A by the $\sigma \in M$ and applying Cramer's rule, we can express each sum $\sum_{\eta_i = \eta} a_i\zeta_i'$ as a combination of the conjugates of A, with coefficients which are integers in $\bar{\mathbf{Q}}_p$ divided by Δ, so have p-adic absolute value bounded above by $|\Delta|^{-1}$. Since $|\Delta|^{-1}$ is bounded above in terms of n alone, making A small will make each $\sum_{\eta_i = \eta} a_i\zeta_i'$ small. If we show these cannot be small without being zero, we are done. Write

$\zeta_i' = \zeta_i'' \rho_i$, where the ρ_i are p-th roots of unity and the ζ_i'' have order prime to p. Again break up each $\sum a_i \zeta_i'$ as

$$B = \sum_{j=0}^{p-1} (\sum_{\rho_i = \xi^j} a_i \zeta_i'') \xi^j = \sum B_j \xi^j,$$

say. Since $\sum_{j=0}^{p-1} \xi^j = 0$ we can write $B = \sum_{j=1}^{p-1} (B_j - B_0) \xi^j$, and since $(\xi^j), 1 \leq j < p$, is a basis for $F(\xi)$ over F, we can conclude that if B is small, then each $B_j - B_0$ is small. However, $B_j - B_0 = \sum_{\rho_i = \xi^j} a_i \zeta_i'' - \sum_{\rho_i = 1} a_i \zeta_i''$ is a linear combination of roots of unity of the kind covered by Theorem 1. Hence if B is sufficiently small we get $B_j - B_0 = 0$ so $B = \sum B_j \xi^j = B_0 \sum \xi^j = 0$. To complete the proof of the theorem, it suffices to prove the following lemma.

Lemma 2. *Let $\Delta = \det(\eta_i^j)_{i,j=0,\ldots,r-1}$ where $\eta_0, \ldots, \eta_{r-1}$ are distinct p-power roots of unity in $\bar{\mathbf{Q}}_p$. Then $|\Delta| \geq |p|^{\frac{r(r-1)}{2(p-1)}}$.*

Proof: Since Δ is an $r \times r$ Vandermonde determinant, the lemma follows from the fact that if η, η' are distinct roots of unity of p-power order then $|\eta - \eta'| \geq |p|^{\frac{1}{(p-1)}}$.

Corollary. *The set $S = \{\sum \zeta_i a_i\}$ with the ζ_i varying through the roots of unity in $\mathbf{C}_p$ is a uniformly discrete subset of $\mathbf{C}_p$, in the sense that there exists a constant $c > 0$ such that for any two distinct elements α and β of S, $|\alpha - \beta| \geq c$.*

Proof: Apply Theorem 2 to $a_1, \ldots, a_n, -a_1, \ldots, -a_n$.

Remarks: (i) If we replace $\mathbf{C}_p$ by $\mathbf{C}$, then Theorem 2 is false, even for $n = 2$, with the group of roots of unity replaced by an arbitrary infinite subgroup, because such a subgroup is dense in the unit circle.

(ii) The argument in the reduction step applies more generally for $a_1, \ldots, a_n$ in any non-archimedian valued field and $\zeta_1, \ldots, \zeta_n$ in a subset of the integers in the field closed under multiplication. In particular we can apply the reduction step and prove the analogue of Theorem 2 with $\mathbf{C}_p$ replaced by the completion of the algebraic closure of $k((x))$, for any field k, and the roots of unity replaced by the elements of k^*.

(iii) The theorem is a special case of the following conjecture: Let A be a semiabelian variety over $\mathbf{C}_p$ and X a closed subvariety. There is a lower bound $c > 0$ for the p-adic distance (in the sense of [Si]) of torsion points on A, not in X, to X. It is easy to see that if c_i is such a lower bound for a closed subvariety X_i of A for $1 \leq i \leq r$, then $c = \min\{c_i\}$ is such a bound for the intersection $X = \bigcap_{i=1}^{r} X_i$. Hence it suffices to consider the case of hypersurface sections X of A, in some given projective or affine embedding. For a linear torus $A = \operatorname{Spec} \mathbf{C}_p[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$, the conjecture follows from our Theorem 2, since a monomial in roots of unity is a root of unity, so any polynomial in roots of unity can be viewed as a linear form in roots of unity with one variable for each monomial. If $A/\bar{\mathbf{Q}}_p$ has good reduction and the Frobenius endomorphism of the reduction lifts to an endomorphism of A, Buium [B2] has proved the weaker version of this conjecture in which one considers only those torsion points fixed by a power of the lift of Frobenius. In particular, he recovers Theorem 1. Serre pointed out to us that, more generally, a similar argument yields the following result: Let K be a non-archimedian local field with residue field k and $Y \subset X$ varieties over K, with Y closed in X. If Z is a finite-dimensional k-subvariety of the Greenberg transform of X, then there is a lower bound $c > 0$ for the p-adic distance of points in $Z(k)$ (considered as a subset of $X(K)$) not in Y, to Y.

Surprisingly, if $\mathbf{Q}_p(a_1, \ldots, a_n)/\mathbf{Q}_p$ is unramified and $p > n(n-1)/2 + 1$, allowing arbitrary roots of unity ζ_i does not make $\min |\sum \zeta_i a_i|$ smaller than allowing only roots of unity of order prime to p. Indeed, if that minimum is not zero, then it is $|p|^m$ for an integer m such that the V_m of §2 is finite, and we have the following result.

Proposition 3. *Let $a_1, \ldots, a_n \in \bar{\mathbf{Q}}_p$ with $\mathbf{Q}_p(a_1, \ldots, a_n)/\mathbf{Q}_p$ unramified and assume that $p > n(n-1)/2 + 1$. If V_m, associated to $(a_1 : \ldots : a_n)$, is finite and $\zeta_1, \ldots, \zeta_n$ are roots of unity of arbitrary order with $|\sum \zeta_i a_i| \leq |p|^m$ then there exists a root of unity η of p-power order and $\zeta_1', \ldots, \zeta_n'$, roots of unity of order prime to p, with $\zeta_i = \zeta_i' \eta, i = 1, \ldots, n$.*

Proof: Since $p > n$, there exist automorphisms $\sigma_j, j = 1, \ldots n$, of $\bar{\mathbf{Q}}_p$ trivial on F, the maximal unramified extension on $\mathbf{Q}_p$, and such that $\sigma_j(\eta) = \eta^j$ if η is a p-power order

root of unity. Suppose $\zeta_1, \ldots, \zeta_n$ are roots of unity of arbitrary order with $|\sum \zeta_i a_i| \leq |p|^m$ and write $\zeta_i = \zeta_i' \eta_i$, with $\zeta_1', \ldots, \zeta_n'$, roots of unity of order prime to p, and $\eta_1, \ldots, \eta_n$ of p-power order. Let r be number of distinct η's. Then we can apply the argument in the proof of Theorem 2. Namely, we conjugate $A = \sum \zeta_i a_i$ by the automorphisms $\sigma_j, 1 \leq j \leq r$ and apply Cramer's rule, to express each sum $\sum_{\eta_i = \eta} a_i \zeta_i'$ as a combination of the conjugates of A, with coefficients which are integers in $\bar{\mathbf{Q}}_p$ divided by $\Delta = \det(\eta^\sigma)$, so have p-adic absolute value bounded above by $|\Delta|^{-1}$. It follows from Lemma 2 that $|\Delta| \geq |p|^{\frac{r(r-1)}{2(p-1)}} \geq |p|^{\frac{n(n-1)}{2(p-1)}}$. Thus,

$$|\sum_{\eta_i = \eta} \zeta_i' a_i| \leq |p|^m |\Delta|^{-1} \leq |p|^{m - \frac{n(n-1)}{2(p-1)}} < |p|^{m-1}.$$

As $|\sum_{\eta_i = \eta} \zeta_i' a_i|$ has to be an integral power of $|p|$, it follows that $|\sum_{\eta_i = \eta} \zeta_i' a_i| \leq |p|^m$. If there are at least two distinct η, η' among $\eta_1, \ldots, \eta_n$ we conclude that, for all $\zeta \in T(k)$,

$$|\sum_{\eta_i = \eta} \zeta_i' a_i + \sum_{\eta_i = \eta'} \zeta \zeta_i' a_i| \leq |p|^m.$$

This contradicts the finiteness of V_m and proves the proposition.

4. Some remarks on the global case

Let K be a number field and $(a_1 : \ldots : a_n) \in \mathbf{P}^{n-1}(K)$. Then for any non-archimedian place w of K we have an embedding of K into $\bar{\mathbf{Q}}_p$ for some p and therefore we can consider the p-adic curve germ given by $(a_1 : \ldots : a_n)$ and study its behaviour as w varies. These p-adic curve germs are the analogues of the local branches of the image of a curve under a map to $\mathbf{P}^{n-1}$. One could ask, following [Sm], for an analogue of the Plücker formulas (and their higher dimensional extensions, also known as the Brill-Segre formula). At this point, it is not clear what shape these would take but we will pose some questions in this direction below. First notice that, due to Proposition 3, which applies to all but finitely many places, it is not unreasonable to restrict our attention to roots of unity of order prime to p at $w|p$ in the following proposition.

Proposition 4. *Let K be a number field and $(a_1 : \ldots : a_n) \in \mathbf{P}^{n-1}(K)$. Assume that $a_1, \ldots, a_n$ are algebraic integers. For an unramified non-archimedian place $w|p$ of K with completion K_w and residue field $\mathbf{F}_w$, consider the corresponding p-adic curve germ, and let (V_m) be the associated sequence of $\mathbf{F}_w$-subvarieties of $\mathbf{P}^{n-1}$. Let q be the norm of w and $N = p^{(n-1)(n-2)/2}$. If V_{n-1} is finite then $\sharp V_{n-1} \leq N$ and either $\sum a_i\zeta_i = 0$ or $|\sum a_i\zeta_i|_w \geq C^{[K:\mathbf{Q}]q^N}$ for roots of unity ζ_i of order prime to p , where $C^{-1} = \prod_{v|\infty}(\sum |a_i|_v)$ and the absolute values are normalized so that they restrict to the usual ones in $\mathbf{Q}$.*

Proof: V_{n-1} is the intersection of the zero sets of the polynomials $F_0, \ldots, F_{n-2}$ and $\deg F_i = p^i$, so the first statement follows from Bézout's Theorem. It follows that each point $(z_1 : \ldots : z_n) \in V_{n-1}$ is defined over a field of degree at most N over the residue field $\mathbf{F}_w$ of w. Hence $\zeta_1, \ldots, \zeta_n$ are $q^k - 1$-th roots of unity for some $k \leq N$ and are therefore defined over a field L of degree at most q^N over K. Applying the product formula to $\alpha = \sum a_i\zeta_i \in L$, if it is non-zero, gives:

$$1 = |\alpha|_w^{d_w/d} \prod_{v \neq w} |\alpha|_v^{d_v/d} \leq |\alpha|_w^{d_w/d} \prod_{v|\infty} |\alpha|_v^{d_v/d} \leq |\alpha|_w^{d_w/d} \prod_{v|\infty} C^{-d_v/d}.$$

As $d_w \geq 1$ and $d \leq [K : \mathbf{Q}]q^N$, the result follows.

The bound given by this proposition is very weak compared with the function field case, where one can bound the valuation by the degree of the embedding of the curve in projective space. In the case $n = 3$, the finiteness of V_2 holds for all but finitely many w by Proposition 2. For $n = 4$, part (iv) of Proposition 1 gives a criterion for the finiteness of V_3, but it does not follow automatically that it is finite for all but finitely many w. This would follow, (assuming $a_i \neq 0$ and a_i/a_j not a root of unity, for $1 \leq i, j \leq 4,\ i \neq j$) if we knew that there are only finitely many primes p with $a^p \equiv a \mod p^3$ for fixed rational $a \neq 0, \pm 1$ and the natural number field analogue, which is implied by the conjecture in [Sm]. For $n \geq 5$ the situation is unclear, but it seems reasonable to expect that V_{n-1} is finite for all but finitely many w in general. Assuming V_∞ is empty, let us define the

weight of w by

$$M_w = \frac{1}{p^{(n-1)(n-2)/2}} \sum_{(z_1:\ldots:z_n)\in V_{n-1}} \big(w(\sum a_i T(z_i)) - (n-1)\big).$$

In the function field case, the Plücker formula gives an expression for the sum of the analogous weights. As a first approximation to it we can ask if the infinite series $\sum_w M_w \log Nw$ converges if $n \geq 3$. There is no good reason to assume it is a finite sum, but the convergence seems reasonable.

Acknowledgements: The authors would like to thank J-P. Serre for some comments on an earlier draft of the paper and to acknowledge the use of the software PARI for some suggestive numerical calculations. The second author would like to thank the NSF (grant DMS-9301157) and the Alfred P. Sloan Foundation for financial support.

References.

[B1] A. Buium, *Geometry of p-jets*, Duke Math. J., to appear.

[B2] A. Buium, *An approximation property for Teichmüller points*, preprint, 1996.

[D] C. Deninger, *Motivic L-functions and regularized determinants*, in *Motives* (U. Jannsen et al., eds.) Proc. Symp. Pure Math. Vol 55, part 1, AMS, 1994, pp. 707-743.

[I] Y. Ihara, *On Fermat quotient and "differentiation of numbers"* RIMS Kokyuroku **810** (1992) 324-341, (In Japanese). English translation by S. Hahn, Univ. of Georgia preprint.

[M] Yu. Manin, *Lectures on zeta functions and motives (according to Denninger and Kurokawa)*, Astérisque **228** (1995) 121-164.

[Mn] H. B. Mann, *On linear relations between roots of unity*, Mathematika **12** (1965) 107-117.

[Mo] E. H. Moore, *A two-fold generalization of Fermat's Theorem*, Bull. Amer. Math. Soc. **2** (1896), 189-199.

[S] J-P. Serre, *Local Fields*, GTM 67, Springer, New York, 1979.

[Si] J. H. Silverman, *Arithmetic distance functions and height functions in Diophantine geometry*, Math. Ann. **279** (1987) 193-216.

[Sm] A. L. Smirnov, *Hurwitz inequalities for number fields*, St. Petersburg Math. J. **4** (1993) 357-375.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: tate,voloch@math.utexas.edu