A p-adic Analog of Wirtinger's Inequality

C. F. Woodcock

1. Introduction

Let $f: \mathbb{T} \to \mathbb{C}$ be a nonconstant, complex-valued, continuously differentiable function on the unit circle with Fourier coefficients $\{\hat{f}_n\}$ $(n \in \mathbb{Z})$. Then it follows easily from Wirtinger's inequality (see e.g. [1, p. 177] or [2, p. 47]) and Parseval's formula for f and f' that f has no zero on some open arc of $\mathbb{T}$ of length

$$h = \pi\left(\frac{\sum_{n\in\mathbb{Z}}|\hat{f}_n|^2}{\sum_{n\in\mathbb{Z}} n^2|\hat{f}_n|^2}\right)^{1/2},$$

where the arc is to be interpreted as $\mathbb{T}$ if $h > 2\pi$. (If not, divide $\mathbb{T}$ up by suitably closely spaced zeros of f and hence derive the required contradiction.)

It is this implied linking between zero-free regions for f and the relative disposition of its Fourier coefficients $\{\hat{f}_n\}$ for which we intend to derive a p-adic analog. (Note, however, that here it will turn out that the roles of the circle and the integers are interchanged! Also, the link between f' and the Fourier coefficients of f is more complicated than in the complex case.)

Throughout, $\mathbb{Z}_p$ and $\mathbb{Q}_p$ will respectively denote the ring of p-adic integers and the field of p-adic numbers (for p prime). We denote by $\mathbb{C}_p$ the completion of the algebraic closure of $\mathbb{Q}_p$ with respect to the p-adic metric. Let v_p denote the p-adic valuation of $\mathbb{C}_p$ normalized so that $v_p(p) = 1$. For simplicity we shall assume throughout that p is *odd*.

Put $\mathbb{T}_p = \{\omega \in \mathbb{C}_p \mid \omega^{p^n} = 1 \text{ for some } n \geq 0\}$ (the *p-adic circle*) so that $\mathbb{T}_p$ is the union of cyclic (multiplicative) groups C_{p^n} of order p^n (for $n \geq 0$). If $\omega \in \mathbb{T}_p$, $\omega \neq 1$, has order p^r then $v_p(\omega - 1) = 1/(p^{r-1}(p-1))$.

2. Main Theorem

Let K be a tame finite extension of $\mathbb{Q}_p$ with $K \subseteq \mathbb{C}_p$. Suppose that $f: \mathbb{Z}_p \to K$ is a uniformly differentiable function. For each $\omega \in \mathbb{T}_p$, we put

$$\hat{f}_\omega = \lim_{N\to\infty} \sum_{i=0}^{p^N-1} \frac{f(i)\omega^i}{p^N}.$$

Received September 20, 1995.
Michigan Math. J. 43 (1996).

Then the *Fourier coefficients* $\{\hat{f}_\omega\}$ of f enjoy the following properties (P).

(P1) Each $\hat{f}_\omega \in K(\omega)$ and $(\hat{f}_\omega)^g = \hat{f}_{\omega^g}$ for all $g \in \mathrm{Gal}(K(\omega)/K)$ (the Galois group of $K(\omega)/K$).

(P2) For each $z \in \mathbb{Z}_p$, $f(z) = \sum_\omega \hat{f}_\omega \omega^{-z}$ (here $\sum_\omega$ means $\lim_{N\to\infty} \sum_{\omega \in C_{p^N}}$).

(P3) If $f \neq 0$ then $v_p(\hat{f}_\omega)$ achieves its minimum value $W(f)$ for $\omega \in \mathbb{T}_p$ but only finitely often. In this case we put

$$M(f) = \max\{r \geq 0 \mid \text{there exists } \omega \in C_{p^r} \setminus C_{p^{r-1}} \text{ with } v_p(\hat{f}_\omega) = W(f)\}$$

(where, by convention, $C_{p^{-1}} = \emptyset$).

The Fourier coefficients $\{\hat{f}_\omega\}$ ($\omega \in \mathbb{T}_p$) of f have many properties (see e.g. [3; 4; 5]) but the properties (P) are all that we need here. However, it is worth noting that the asymptotic behavior of $\{\hat{f}_\omega\}$ determines (and is determined by) the derivative f'. In particular, for $\omega \in \mathbb{T}_p$, $v_p(\hat{f}_\omega)$ tends to $\inf_{x \in \mathbb{Z}_p} v_p(f'(x))$ off finite subsets of $\mathbb{T}_p$.

We will prove the following result (in Section 4).

THEOREM. *Let $f: \mathbb{Z}_p \to K$ be a uniformly differentiable function with $f \neq 0$ and K a tame finite extension of $\mathbb{Q}_p$. Then f has no zero on some coset of $p^{M(f)}\mathbb{Z}_p$ in $\mathbb{Z}_p$.*

3. Examples

We first illustrate some basic features of the main theorem with several simple examples (where f is locally constant and so $f' = 0$).

EXAMPLE 1. The condition in the theorem that K be tame is a necessary one. For let $\sigma \in C_{p^2} \setminus C_{p^1}$ and put $K = \mathbb{Q}_p(\sigma)$. Define $f: \mathbb{Z}_p \to K$ by putting $f(z) = \sum_{\omega \in C_{p^1}} a_\omega \omega^{-z} - \sigma^{-z}$ for all $z \in \mathbb{Z}_p$ where each $a_\omega = \sum_{i=0}^{p-1} \sigma^{-i}\omega^i/p$. Then clearly $v_p(a_\omega) = 1/(p-1) - 1/(p(p-1)) - 1 < 0$, and so $M(f) = 1$ yet $f(i) = 0$ for $0 \leq i \leq p-1$.

EXAMPLE 2. Let $N \geq 1$. Define $f: \mathbb{Z}_p \to \mathbb{Q}_p$ by putting $f(z) = \sum_{\omega \in C_{p^N}} \omega^{-z}/p^N$ for all $z \in \mathbb{Z}_p$ so that f is the characteristic function of $p^N\mathbb{Z}_p$. Clearly $M(f) = N$, f has no zero on $p^N\mathbb{Z}_p$ but does have a zero on each coset of $p^{N-1}\mathbb{Z}_p$ in $\mathbb{Z}_p$ (which shows that the theorem is "best possible" in some sense).

EXAMPLE 3. Let K be a tame finite extension of $\mathbb{Q}_p$ with $K \subseteq \mathbb{C}_p$, and let $N \geq 1$. Suppose that $q(x) = \sum_{k=0}^{p^{N-1}(p-1)-1} q_k x^k \in K[x]$ is a nonzero polynomial of degree less than $p^{N-1}(p-1)$. Define $f: \mathbb{Z}_p \to K$ by putting $f(z) = \sum_{\omega \in C_{p^N}} q(\omega)\omega^{-z}$ for all $z \in \mathbb{Z}_p$. Then a simple calculation shows that $f(j) = 0$ for $p^{N-1}(p-1) \leq j \leq p^N - 1$ so that f has a zero in each coset of $p^{N-1}\mathbb{Z}_p$ in $\mathbb{Z}_p$. Therefore, by the theorem, $M(f) = N$; that is, $v_p(q(\omega))$ achieves its minimum value for $\omega \in C_{p^N}$ when $\omega \in C_{p^N} \setminus C_{p^{N-1}}$. (Note that the conditions on $q(x)$ given above are actually needed here.)

We next consider the case when f is a nonconstant polynomial function and first prove a general proposition giving an upper bound for $M(f)$ in terms of the behavior of f'. Note that although the asymptotic behavior of $\{\hat{f}_\omega\}$ is always controlled by f', it is difficult to convert this into a meaningful bound for $M(f)$ unless f is a polynomial function (or, more generally, a locally analytic function).

PROPOSITION. *Let $f: \mathbb{Z}_p \to K$ be a nonconstant polynomial function and let*

$$f'(z) = \sum_{r=0}^{N} b_r \binom{z+r}{r} \quad \textit{for all } z \in \mathbb{Z}_p$$

("Mahler-type" expansion of f'). Put $s = \max\{r \mid 0 \le r \le N$ and $v_p(b_r) = \min_{0\le t\le N} v_p(b_t)\}$, and

$$L = \min_{s<i\le N} \left(\frac{v_p(b_i) - v_p(b_s)}{i-s} \right) \quad (\textit{take } L = \infty \textit{ if } s = N).$$

Suppose that $M \in \mathbb{N}$, $M \ge 1$, is such that $1/(p^{M-1}(p-1)) < L$. Then $M(f) \le M$. (Hence, by the theorem, if K is a tame finite extension of $\mathbb{Q}_p$ with $K \subseteq \mathbb{C}_p$ then f has no zero on some coset of $p^M\mathbb{Z}_p$ in $\mathbb{Z}_p$.)

Proof. Using standard properties of p-adic Fourier series and the associated convolution multiplication $*$ (see e.g. [3] or [5]), it is easily shown that

$$f(z) = c + \sum_{r=0}^{N} b_r (-1)^r z^{*(r+1)} \quad \text{for some } c \in K.$$

Hence, for $\omega \in \mathbb{T}_p$ ($\omega \ne 1$), $\hat{f}_\omega = \sum_{r=0}^{N} b_r (-1)^r (\omega-1)^{-(r+1)}$ (since $\hat{z}_\omega = 1/(\omega-1)$ where $z: \mathbb{Z}_p \to \mathbb{Z}_p$ is the identity function). Now, by the hypothesis on M, if $\omega \notin C_{p^{M-1}}$ (so that $v_p(\omega-1) \le 1/(p^{M-1}(p-1))$) then

$$v_p(\hat{f}_\omega) = v_p(b_s(-1)^s(\omega-1)^{-(s+1)}).$$

Clearly, this latter strictly increases with the order of $\omega \in \mathbb{T}_p$. Hence we immediately deduce that $M(f) \le M$, as required. □

REMARK 1. The proposition does in fact still hold for *any* subfield K of $\mathbb{C}_p$. Indeed, by substituting the formula for $\hat{f}_\omega$ (given in the proof) directly into formula (*) of Section 4, it is easy to reduce to the case when $K = \mathbb{Q}_p$. (Note that now M may be greater than $M(f)$.)

REMARK 2. It is interesting to compare the bound $1/(p^{M-1}(p-1)) < L$ of the proposition with the "trivial bound" $p^M > N+1$ which gives rise to the same conclusion concerning the zeros of f (just using the fact that the degree of f is at most $N+1$).

EXAMPLE 4. Let $p = 3$ and define $f: \mathbb{Z}_3 \to \mathbb{Q}_3$ by putting $f(z) = z^3 + z^2 - 2z$ for all $z \in \mathbb{Z}_3$. Then

$$f'(z) = 6\binom{z+2}{2} - 7\binom{z+1}{1} - \binom{z+0}{0}$$

and so $s = 1$ and $L = ((1-0)/(2-1)) = 1$. Thus we can take $M = 1$. By the proposition it follows that $M(f) \le 1$ and so, by the theorem, f has no zero on some coset of $3\mathbb{Z}_3$ in $\mathbb{Z}_3$. (Of course, f actually has zeros $0, 1, -2$ and $M(f) = 1$.)

EXAMPLE 5. Let $p = 3$ and define $f: \mathbb{Z}_3 \to \mathbb{Q}_3$ by putting $f(z) = z^3 - z$ for all $z \in \mathbb{Z}_3$. Then

$$f'(z) = 6\binom{z+2}{2} - 9\binom{z+1}{1} + 2\binom{z+0}{0}$$

and so

$$s = 0 \quad \text{and} \quad L = \min\left\{\left(\frac{2-0}{1-0}\right), \left(\frac{1-0}{2-0}\right)\right\} = \frac{1}{2}.$$

Thus we can take $M = 2$. Therefore, by the proposition, $M(f) \le 2$. (Of course, f in fact has zeros $0, 1, -1$, one in each coset of $3\mathbb{Z}_3$ in $\mathbb{Z}_3$ and so, by the theorem, $M(f) = 2$.)

4. Proof of the Main Theorem

We will need the following standard result concerning the trace over a tame finite extension K of $\mathbb{Q}_p$ (see e.g. [4, Lemma 2.1]).

LEMMA. *Let $\omega \in \mathbb{T}_p$, $\omega \ne 1$, have order p^r (so $v_p(\omega - 1) = 1/(p^{r-1}(p-1))$). Then, for all $x \in K(\omega)$,*

$$v_p(\text{trace}(x)) \ge v_p(x) + r - 1 - 1/(p-1) + 1/(p^{r-1}(p-1)),$$

where the trace is taken from $K(\omega)$ to K.

Now let $f: \mathbb{Z}_p \to K$ be uniformly differentiable with $f \ne 0$. Let $M = M(f)$ and suppose that f has a zero in each coset of $p^M\mathbb{Z}_p$ in $\mathbb{Z}_p$. In order to prove the main theorem we must now obtain a contradiction.

Suppose then that f has a zero at each of $z_0, z_1, \ldots, z_{p^M-1}$ (say), where $v_p(z_i - i) \ge M$ for $0 \le i \le p^M - 1$. Put $X = \inf_{\omega \in \mathbb{T}_p \setminus C_{p^M}} v_p(\hat{f}_\omega)$ so that $X > W(f)$ while, for some $\sigma_1 \in C_{p^M}$ (say), $v_p(\hat{f}_{\sigma_1}) = W(f)$.

By property (P2) of Section 2 we have

$$0 = f(z_i) = \sum_{\sigma \in C_{p^M}} \hat{f}_\sigma \sigma^{-z_i} + \sum_{\omega \notin C_{p^M}} \hat{f}_\omega \omega^{-z_i}$$

for $0 \le i \le p^M - 1$. Multiplying by $\sigma_1^{z_i}$ and summing for $0 \le i \le p^M - 1$, we obtain

$$0 = p^M \hat{f}_{\sigma_1} + \sum_{i=0}^{p^M-1} \sum_{\omega \notin C_{p^M}} \hat{f}_\omega (\sigma_1 \omega^{-1})^{z_i}$$

(since $\sigma^{-z_i} = \sigma^{-i}$ for $\sigma \in C_{p^M}$) and so

$$\hat{f}_{\sigma_1} = -\sum_{i=0}^{p^M-1} \sum_{R=M}^{\infty} \sum_{\omega \in C_{p^{R+1}} \setminus C_{p^R}} \frac{\hat{f}_\omega (\sigma_1 \omega^{-1})^{z_i}}{p^M}.$$

Therefore, in order to obtain the required contradiction, it is clearly enough to show that for each $R \geq M$,

$$v_p\left(\sum_{i=0}^{p^M-1} \sum_{\omega \in C_{p^{R+1}} \setminus C_{p^R}} \hat{f}_\omega (\sigma_1 \omega^{-1})^{z_i}\right) \geq X + M \qquad (*)$$

(since $X > W(f) = v_p(\hat{f}_{\sigma_1})$).

We consider the two cases (a) $R > M$ and (b) $R = M$ separately.

Case (a) $R > M$: In this case,

$$\sum_{\omega \in C_{p^{R+1}} \setminus C_{p^R}} \hat{f}_\omega \omega^{-z_i}$$

is clearly a "sum of traces $K(\omega)/K$" (by property (P1)) and so (by the lemma) has v_p-value at least $X + R - 1/(p-1) + 1/(p^R(p-1)) > X + M$. Hence (*) holds, as required.

Case (b) $R = M$: We first show that in this case, without loss of generality, we may suppose that each $z_i = i$. For

$$\sum_{\omega \in C_{p^{M+1}} \setminus C_{p^M}} \hat{f}_\omega (\sigma_1 \omega^{-1})^{z_i} - \sum_{\omega \in C_{p^{M+1}} \setminus C_{p^M}} \hat{f}_\omega (\sigma_1 \omega^{-1})^{i}$$
$$= \sum_{\omega \in C_{p^{M+1}} \setminus C_{p^M}} \hat{f}_\omega (\omega^{-z_i} - \omega^{-i}) \sigma_1^i$$

(since $v_p(z_i - i) \geq M$ and $\sigma_1 \in C_{p^M}$). Now, by property (P1),

$$\sum_{\omega \in C_{p^{M+1}} \setminus C_{p^M}} \hat{f}_\omega (\omega^{-z_i} - \omega^{-i})$$

is again a "sum of traces $K(\omega)/K$" and so, by the lemma, has v_p-value at least

$$X + M - 1/(p-1) + 1/(p^M(p-1)) + v_p(\omega^{-z_i} - \omega^{-i}) > X + M,$$

as required (since $v_p(\omega^{-z_i} - \omega^{-i}) \geq 1/(p-1)$ as $v_p(z_i - i) \geq M$ and $\omega \in C_{p^{M+1}}$).

It remains therefore to show that (*) holds in the case when $R = M$ and each $z_i = i$. Now

$$\sum_{i=0}^{p^M-1} \sum_{\omega \in C_{p^{M+1}} \setminus C_{p^M}} \hat{f}_\omega (\sigma_1 \omega^{-1})^i$$
$$= \sum_{\omega \in C_{p^{M+1}} \setminus C_{p^M}} \hat{f}_\omega (1 - (\sigma_1 \omega^{-1})^{p^M})(1 - \sigma_1 \omega^{-1})^{-1}$$
$$= \sum_{\omega \in C_{p^{M+1}} \setminus C_{p^M}} \hat{f}_\omega (1 - \omega^{-p^M})(1 - \omega^{-1})^{-1}\left(1 - \left(\frac{\sigma_1^{-1} - 1}{\omega^{-1} - 1}\right)\right)^{-1} \sigma_1^{-1}$$

(since $\sigma_1^{p^M} = 1$; note that $(1 - \sigma_1 \omega^{-1})^{-1}$ has been rewritten so as to avoid the necessity of taking traces over $K(\sigma_1)$ since in general $K(\sigma_1)$ will not be tame over $\mathbb{Q}_p$)

$$= -\sum_{l=0}^{\infty} \sum_{\omega \in C_{p^{M+1}} \setminus C_{p^M}} \hat{f}_\omega (1-\omega^{-p^M})(\omega^{-1}-1)^{-l-1}(\sigma_1^{-1}-1)^l \sigma_1^{-1}$$

(on taking the binomial expansion of $(1-((\sigma_1^{-1}-1)/(\omega^{-1}-1)))^{-1}$; note that $v_p((\sigma_1^{-1}-1)/(\omega^{-1}-1)) > 0$ since $\sigma_1 \in C_{p^M}$ while $\omega \in C_{p^{M+1}} \setminus C_{p^M}$).

For each $l \geq 0$, the v_p-value of the internal sum above is at least

$$X+M-1/(p-1)+1/(p^M(p-1))+1/(p-1)-1/(p^M(p-1)) = X+M$$

(again using property (P1) and the lemma; note that $v_p(1-\omega^{-p^M}) = 1/(p-1)$ and $v_p(\omega^{-1}-1) = 1/(p^M(p-1))$). Hence (*) holds in this case also, as required. □

References

[1] E. F. Beckenbach and R. Bellman, *Inequalities,* Springer, Berlin, 1961.

[2] H. Dym and H. P. McKean, *Fourier series and integrals,* Academic Press, New York, 1972.

[3] C. F. Woodcock, *A spectral valuation on the ring of p-adic integers,* J. London Math. Soc. (2) 25 (1982), 223–234.

[4] ———, *Spectral properties of tame functions on the ring of p-adic integers,* J. London Math. Soc. (2) 30 (1984), 407–418.

[5] ———, *p-adic Fourier series,* p-adic Methods and their applications (A. J. Baker and R. J. Plymen, eds.), pp. 167–193, Oxford Univ. Press, New York, 1992.

Institute of Mathematics and Statistics
The University
Canterbury, Kent, CT2 7NF
England

C.F.Woodcock@ukc.ac.uk