OPTIMAL APPROXIMATION IN HENSELIAN FIELDS

Asim Naseem, Khurram Shabbir, *Shahid Ahmad, Aansa Islam
Department of Mathematics, GCU Lahore
*Corresponding Author's email: dr.shahidahmad@gcu.edu.pk

ABSTRACT: *A non-empty subset S of a valued field K is said to have the optimal approximation property if every element in the field K has a closest approximation in S. This property relates to the model theory of valued fields, which was introduced by F.V. Kuhlmann in* [1]. *The notion becomes more involved when the set S is the image of a polynomial map on K. In this paper, we present some classes of polynomials over a henselian discretely valued field, whose image set has optimal approximation property*.

Keywords: Valued fields, henselian fields, optimal approximation, polynomials

1. INTRODUCTION

We denote the set of natural numbers, integers, rational numbers and real numbers by **N**, **Z**, **Q** and **R**, respectively. For a prime number p, $\mathbf{F}_p$ denotes the finite field with p elements. For a valued field (K,v) we will denote its value group by vK, valuation ring by R and the residue class field by K_v. For $a\epsilon K$, va denotes its value and for $a\epsilon R$, $\bar{a}$ denotes the residue class of a. The reduction of a polynomial $f(X)\epsilon K[X]$ in K_v is denoted by $\bar{f}(X)$. For the basic facts of valuation theory and model theory, we refer the reader to [2,3,4,5].

For any extension field L of K, there is at least one extension w of v from K to L, i.e., $w|_K=v$ (cf. [2], Theorem 3.1.2). A valued field (K,v) is called *henselian* if the valuation v can be uniquely extended to each algebraic extension of the field K. This holds if and only if (K,v) satisfies the following lemma:

Lemma 1.1. (Hensel's Lemma) Let $f(X)\epsilon R[X]$ be a polynomial such that $\bar{f}(X)\epsilon K_v[X]$ has a simple root $\alpha\epsilon K_v$. Then $f(X)$ has a root $a\epsilon R$ such that $\bar{a}=\alpha$.

Every valued field (K,v) admits a *henselization*, i.e., a minimal (separable) algebraic extension field which is henselian. All henselizations of (K,v) are isomorphic, therefore we talk of *the* henselization and denote it by K^h. A valued extension (L,w) of (K,v) is called *immediate* if $vK=vL$ and $K_v=L_w$. For instance, completion and henselization of a valued field are immediate extensions. A valued field is called *(algebraically) maximal* if it does not possess any proper immediate (algebraic) extension. An algebraically maximal field or a maximal field is always henselian but not vice versa (see [6], 3.6).

A subset S of (K,v) is said to have the *Optimal Approximation Property* (OA) if for all $a\epsilon K$, the set

$v(a\text{-}S)=\{v(a\text{-}s) : s\epsilon S\}$

has a maximal element in $vK\cup\{\infty\}$. The notion of optimal approximation was introduced by F.V. Kuhlmann in [1] while studying the elementary properties of the valued field $\mathbf{F}_p((t))$ equipped with the usual t-adic valuation v_t. The followings are some useful implications given in [7].

Lemma 1.2. Every compact subset of (K,v) has OA. Every set which has OA is closed in (K,v).

This approximation property relates to the model theory of valued fields since it is elementary for definable S. The image

$S=\{ f(a_1,\ldots, a_n) : a_1,\ldots, a_n \epsilon K\}$

of K under a polynomial $f\,\epsilon K[X_1,\ldots, X_n]$ is definable, so the question arises: *when this image has OA*? Following answers to the later question was given in [7] and [1].

For convenience, we use the following definition:

Definition 1.3. A polynomial $f\epsilon K[X_1,\ldots, X_n]$ has OA in (K,v) if the image of K under f has OA.

In [1], F.V. Kuhlmann proved that any polynomial in one variable over an algebraically maximal field has OA. It is also shown that if (K, v) is maximal, then any *additive polynomial* in several variables satisfying an additional condition, has OA in (K,v). In [7], by removing the additional condition, Lou van den Dries and F.V. Kuhlmann showed that any additive polynomial in several variables has OA in $(\mathbf{F}_p((t)),v_t)$.

All the valued fields considered above are not just henselian but they also have some more fruitful properties. For instance, $\mathbf{F}_p((t))$ is a discrete, locally compact valued field and this last feature is actually used to prove the result given in [7].

In this paper, we consider (K,v) to be henselian with $vK=\mathbf{Z}$ and present some classes of polynomials in one variable that have OA. The situation considered is more general in some sort as an algebraically maximal field or a maximal field is always henselian but not vice versa.

2. POLYNOMIALS HAVING OA PROPERTY

In the following, we will present the mentioned classes of polynomials. For this, we gather some required information.

Let S be a non-empty subset of a valued field (K,v). If S does not have OA then there are two possibilities: For some $x\epsilon K$, either

1. $v(x\text{-}S)$ has no maximum but $v(x\text{-}S)<\alpha$ for some $\alpha\epsilon vK$, or
2. $v(x\text{-}S)$ is cofinal in vK.

If the value group vK is isomorphic to $\mathbf{Z}$, then it dismisses the first possibility. The second possibility implies that there exists a sequence $(s_\alpha)_{\alpha\epsilon\mathbf{N}}$ in S such that $v(x\text{-} s_\alpha)$ is cofinal in vK. This means that the sequence $(s_\alpha)_{\alpha\epsilon\mathbf{N}}$ has limit $x\epsilon K\backslash S$ and consequently it shows that the set S is not closed in (K,v). Thus S closed in (K,v) dismisses the second possibility and we have a converse to Lemma 1.2.

Proposition 2.1. Let the field K be equipped with a discrete rank 1 valuation v. Then a non-empty subset S of K has OA if and only if it is closed in (K,v).

For (K,v) with $vK=\mathbf{Z}$, throughout we assume $\pi\epsilon K$ to be a *uniformizer*, i.e., $v(\pi)=1$. Then any $x\epsilon K^\times$ can be uniquely written as: $x=\pi^n u$, where $n=v(x)$ and $u\epsilon R^\times$. For any non-empty subset S of a valued field (K,v) with $vK=\mathbf{Z}$, we define:

$S^*=\{s\pi^{-v(s)} : s\epsilon S \backslash\{0\}\}$,

so-called the set of associated units of S. We use the following criteria to establish our desired results. The proof is straightforward, therefore omitted.

Proposition 2.2: Let (K,v) be a discrete rank 1 valued field. A non-empty subset S of K has OA if $v(S)$ and $v(u\text{-}S^*)$ have maximum for all $u\,\epsilon R^\times\backslash S^*$.

Let $f(X)=a_0+a_1X+\ldots+a_nX^n\epsilon K[X]$. For any $m\epsilon\mathbf{Z}$, we define the polynomial

$f_m(X):=\pi^{-M}f(\pi^m X)$,
where $M=\min_{1\leq i\leq n}\{v(a_i)+im\}$. Note that the polynomial $f_m(X)\epsilon R[X]$.

Lemma 2.3. Let (K,v) be henselian with $vK=\mathbf{Z}$. For $f(X)\epsilon K[X]$, the set $vf(K)$ has maximum if for every $m\epsilon\mathbf{Z}$, the polynomial $\bar{f}_m(X)\epsilon K_v[X]$ has no non-zero root in K_v.

Proof: Let $f(X)=a_0+a_1X+\ldots+a_nX^n$ and $\varphi(X):=a_n^{-1}f(X)$. Since $\varphi_m(X)=a_n^{-1}\pi^{Mc}f_m(X)$, where $c=v(a_n)$ and $vf(a)=v\varphi(a)+v(a)$ for all $a\epsilon K$, therefore we may assume $f(X)$ is monic. Further, since $f(X)=a(X)b(X)$ implies that $f_m(X)=a_m(X)b_m(X)$, therefore we assume that $f(X)$ is irreducible. Now, let E be the splitting field for $f(X)$ and let $\alpha=\alpha_1,\alpha_2,\ldots,\alpha_n\epsilon E$ be the roots of $f(X)$, then $f(X)=\prod_{1\leq i\leq n}(X-\alpha_i)$. Let w be the unique extension of v from K to E and $a\epsilon K$. Then
$vf(a)=v(\prod_{1\leq i\leq n}(a-\alpha_i))=\sum_{1\leq i\leq n} w(a-\alpha_i)$.
For $\alpha\epsilon E$, there exist $\sigma_i\epsilon Aut(E/K)$ such that $\sigma_i(\alpha)=\alpha_i$. Since $\sigma_i(a)=a$ for all $a\epsilon K$, therefore the above expression can be written as:
$vf(a)=\sum_{\sigma\epsilon Aut(E/K)} w\circ\sigma(a-\alpha)$.
Since E/K is normal, therefore by Conjugation theorem (Theorem 3.2.5 of [2]), every extension of v is of the form $w\circ\sigma$. But (K,v) is henselian, which implies that $w=w\circ\sigma$ for all $\sigma\epsilon Aut(E/K)$. Hence $vf(a)=nw(a-\alpha)$. Now, if $v(a)\neq w(\alpha)\epsilon wE$, then $vf(a)\leq nw(\alpha)$. Since $w(\alpha)\epsilon wE$ and E/K is algebraic, therefore wE can be considered as additive subgroup of $\mathbf{R}$ (see [2], Corollary 3.2.5). Hence the set $\{vf(a) : a\epsilon K, v(a)\neq w(\alpha)\}$ is bounded in $\mathbf{Z}$. For otherwise case, we have $v(a)=w(\alpha)=m\epsilon\mathbf{Z}$. Then $a=\pi^m u$ for some $u\ \epsilon R^\times$ and $f_m(u)=\pi^{-M}f(a)$, where $M=\min_{1\leq i\leq n}\{v(a_i)+im\}$. Since $\bar{f}_m(X)$ has no non-zero root in K_v, therefore $\bar{f}_m(\bar{u})\neq 0$. But this means that $vf_m(u)=0$ and consequently, $vf(a)=M$. This shows that $vf(K)$ is bounded in $\mathbf{Z}$ and consequently $vf(K)$ has maximum. □

Now we present promised results.

Theorem 2.4. Let (K,v) be henselian with $vK=\mathbf{Z}$. A polynomial $f(X)\epsilon K[X]$ has OA if for every $m\epsilon\mathbf{Z}$,

1. $\bar{f}_m(X)$ has no non-zero root in K_v, and
2. $\bar{f}_m(X)-\bar{u}\epsilon K_v[X]$ is separable for all $u\epsilon R^\times$.

Proof: Using the first condition, Lemma 2.3 implies that $vf(K)$ has maximum. Hence by proposition 2.2, it is sufficient to show that the set $v(u-f(K)^*)$ has maximum for all $u\epsilon R^\times\backslash f(K)^*$. First we claim that $f(K)^*=\cup_{m\epsilon\mathbf{Z}} f_m(R^\times)$. Indeed, since $f_m(X)\epsilon R[X]$, therefore for any $u\epsilon R^\times$, we have $vf_m(u)\geq 0$. The first condition implies that $\bar{f}_m(\bar{u})\neq 0$ for all $u\epsilon R^\times$. Thus $vf_m(u)=0$ and $vf(\pi^m u)=M$ for all $u\epsilon R^\times$. Hence we conclude that $f_m(R^\times)=f(K_m)^*$, where $K_m=\{a\epsilon K : va=m\}$. Consequently
$f(K)^*=\cup_{m\epsilon\mathbf{Z}} f_m(R^\times)$
as claimed. Now, let $u\epsilon R^\times\backslash f(K)^*$, then $u\epsilon R^\times\backslash f_m(R^\times)$ for all $m\epsilon\mathbf{Z}$. If $\bar{u}\epsilon\bar{f}_m(K_v)$ for some $m\epsilon\mathbf{Z}$, then this means that $\bar{u}=\bar{f}_m(\bar{a})$ for some $a\ \epsilon R^\times$. Hence by the second condition, $\bar{a}\epsilon K_v$ is a (simple) root of the separable polynomial $\bar{f}_m(X)-\bar{u}\epsilon K_v[X]$. Thus by Hensel's Lemma, there exists $e\epsilon R^\times$ such that $\bar{a}=\bar{e}$ and e is a root of $f_m(X)-u\epsilon R^\times[X]$. This means that $u=f_m(e)\epsilon f_m(R^\times)$, which is a contradiction as u does not belong to $f_m(R^\times)$. Thus $\bar{u}$ does not belong to $\bar{f}_m(K_v)$ for all $m\epsilon\mathbf{Z}$, i.e., $\bar{u}\neq\bar{f}_m(\bar{a})$ for all $a\epsilon R^\times$ and $m\epsilon\mathbf{Z}$. This means that $v(u-f_m(K)^*)=\{0\}$ for all $m\epsilon\mathbf{Z}$ and hence consequently $v(u-f(K)^*)=\{0\}$. Hence the proof is now completed.

The most easy example of a polynomial which satisfies the conditions of the above Theorem is $f(X)=X^n\epsilon K[X]$, where (K,v) is henselian with $vK=\mathbf{Z}$ and n is not divisible by *char* K_v. Hence by the above theorem, the image $f(K)=K^n$ has OA in (K,v). Particularly for any $n\epsilon\mathbf{N}$ which is not divisible by the prime p, the polynomial $f(X)=X^n$ or more generally $f(X)=(aX+b)^n$, $a\neq 0$ has OA in $(\mathbf{F}_p((t)),v_t)$. Since n is coprime with p, therefore the above polynomial is not additive in general. Hence, this trivial example lies in the counter part of the polynomials given in [7].

Remark 2.5. The condition (K,v) to be henselian cannot be omitted from the hypothesis of Theorem 2.4. For instance, take the valued field $(\mathbf{Q},v_5)$ which is not henselian. The polynomial $f(X)=X^2$ satisfies both the conditions of Theorem 2.4, but $f(X)=X^2$ does not have OA in $(\mathbf{Q},v_5)$ as the set $v(-1-\mathbf{Q}^2)$ is cofinal in $\mathbf{Z}$. Indeed, note that $i\epsilon\mathbf{Q_5}$ (since the polynomial $X^2+1\epsilon\mathbf{F}_5[X]$ has simple roots 2 and 3 in $\mathbf{F}_5$, therefore by Hensel's lemma $f(X)=X^2+1$ has a root i in $\mathbf{Q_5}$. Now since $(\mathbf{Q_5},v_5)$ is complete, therefore there exists a sequence $(s_n)_n$ in $\mathbf{Q}$ such that $s_n\rightarrow i$. Since X^2 is a continuous function, it implies that $s^2_n\rightarrow -1$, i.e., the sequence s^2_n does not converge in $\mathbf{Q}^2$. Hence the set $\{v(-1-s^2_n)_n\}$ is unbounded in $\mathbf{Z}$ and consequently the set $v(-1-\mathbf{Q}^2)$ has no maximum in $\mathbf{Z}$.

By using Theorem 2.4 and Proposition 1.5.1 of [4], one can derive the following particular case of the result proved in Lemma 13 of [1].

Lemma 2.6. Let K be a finite extension of either $\mathbf{Q}_p$ or $\mathbf{F}_p((t))$. Then every monic polynomial $f(X)$ in $R[X]$ of degree relatively prime to p has OA.

Proof: Since $f(X)\epsilon R[X]$ is monic therefore one gets for $m<0$: $f_m(R^\times)=f(K^m)^*$ and $f(K\backslash R)^*=\cup_{m<0} f_m(R^\times)$. Since $\bar{f}_m(X)=X^n$ satisfies both conditions of Theorem 2.4, therefore by following the proof of Theorem 2.4, one can conclude that $f(K\backslash R)$ has OA in (K,v). Moreover, (K,v) locally compact implies that the valuation ring R is compact (see Proposition 1.5.1 of [4]). As f is a continuous function (being a polynomial), it implies that $f(R)$ is also compact. Thus by Lemma 1.2, $f(R)$ has OA. Since $f(K)=f(K\backslash R)\cup f(R)$, therefore it implies that the polynomial $f(X)$ has OA in (K,v). □

The above result requires our valued field to be locally compact but now we content to henselian valued field.

Theorem 2.7. Let (K,v) be henselian with $vK=\mathbf{Z}$. Let $f(X)=\sum_{r\leq i\leq n} a_iX^i\epsilon R[X]$ such that r and n be not divisible by *char* K_v, and $a_r,a_n\epsilon R^\times$. Then $f(X)$ has OA if the polynomial $\bar{f}(X)\epsilon K_v[X]$ satisfies conditions 1 and 2 of Theorem 2.4.

Proof: Observe that: $\bar{f}_m(X)=\bar{a}_nX^n$ for $m<0$, $\bar{f}_m(X)=\bar{a}_rX^r$ for $m<0$ and $\bar{f}_m(X)=\bar{f}(X)$ for $m=0$. Both the polynomials $\bar{a}_nX^n$ and $\bar{a}_rX^r$ satisfy the conditions of Theorem 2.4. Hence if $\bar{f}(X)$ also satisfies the conditions, then by Theorem 2.4, $f(X)$ has OA.

We conclude with an example, which is constructed by using the above Theorem.

Example 2.8. Let (K,v) be any henselian field with $vK=\mathbf{Z}$ and *char* $K_v=p>0$. Let $\varphi(X)\epsilon K_v[X]$ be a polynomial which has no non-zero root in K_v. Then for $q=p^d$, $d\epsilon\mathbf{N}$, the polynomial $\bar{f}(X)=X\,\varphi(X^q)\epsilon K_v[X]$ has no non-zero root in K_v. Moreover, $\bar{f}(X)-\bar{u}$ is separable for all $u\epsilon R^\times$. Hence $\bar{f}(X)$ satisfies conditions 1 and 2 of Theorem 2.4. Further Theorem 2.7 implies that any lifting of $\bar{f}(X)$, of the form $\sum_{r\leq i\leq n} a_iX^i\epsilon R[X]$ such that r and n are not divisible by p, has OA. In particular, the polynomial $f(X)=X^{10}+2X^4+X$ over $(\mathbf{Q}^h,v_3)$ has OA (since $\bar{f}(X)=X^{10}+2X^4+X$ in $\mathbf{F}_3[X]$ is obtained by taking $\varphi(X)=X^3+2X+1$ and $d=1$).

REFERENCES

[1]. F.V. Kuhlmann, *Elementary properties of power series fields over finite fields*, J. symb. logic, **43(66)**, 771-791(2001).

[2]. A. Engler, A. Prestel, *Valued fields*, Springer-Verlag, Inc., New-York, 2005.

[3]. F.V. Kuhlmann, Valuation Theory, http://math.usask.ca/˜fvk/Fvkbook.htm

[4]. J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Inc., New-York, 1999.

[5]. F.G. Schilling, *The theory of valuations*, Amer. Math. Soc., New-York, 1950.

[6]. F.V. Kuhlmann, *The defect*, Comm. Alg., Springer, 277-318 (2011).

[7]. L. Dries, F.V. Kuhlmann, *Images of additive polynomials in* $\boldsymbol{F}_q((t))$ *have the optimal approximation property*, Canad. Math. Bull., **45**, 71-79(2002).

[8]. F.V. Kuhlmann, *A short introduction to model theoretic algebra*, (2012).