Simultaneous interpolation and P-adic approximation by integer-valued polynomials

Sophie Frisch

Institute of Analysis and Number Theory
Technische Universität Graz
Kopernikusgasse 24, 8010 Graz, Austria
frisch@math.tugraz.at

Abstract. [1] Let D be a Dedekind domain with finite residue fields and $\mathcal{F}$ a finite set of maximal ideals of D. Let $r_0, \ldots, r_n$ be distinct elements of D, pairwise incongruent modulo P^{k_P} for each $P \in \mathcal{F}$, and $s_0, \ldots, s_n$ arbitrary elements of D.
We show that there is an interpolating P^{k_P}-congruence preserving integer-valued polynomial, that is, $f \in \text{Int}(D) = \{g \in K[x] \mid g(D) \subseteq D\}$ with $f(r_i) = s_i$ for $0 \leq i \leq n$, such that, moreover, the function $f\colon D \to D$ is constant modulo P^{k_P} on each residue class of P^{k_P} for all $P \in \mathcal{F}$.

Keywords: Interpolation, polynomials, congruence preserving, P-adic approximation, P-adic Lipschitz functions, Lipschitz maps, integer-valued polynomials, polynomial functions, polynomial mappings, Dedekind domains, commutative rings, integral domains.
Math. Subj. Class. 2010: Primary 13B25; Secondary 12C05, 13F20, 13M10, 11C08, 13F05.

1 Introduction

Let D be a Dedekind domain with finite residue fields, K its quotient field, and

$$\text{Int}(D) = \{f \in K[x] \mid f(D) \subseteq D\}$$

the ring of integer-valued polynomials on D.

We will show that two different feats that can each be accomplished separately by integer-valued polynomials, namely, interpolation of arbitrary functions on D, and, representation of arbitrary functions on D/P^n, where P^n is a power of a maximal ideal P, can actually be accomplished by one and the same polynomial, simultaneously.

We recall some well-known facts. First, about interpolation by integer-valued polynomials: Newton already used polynomials in $\text{Int}(\mathbb{Z})$ to interpolate functions on $\mathbb{Z}$, cf. [1]. More generally, when D is a Dedekind domain with finite residue fields, then, given $r_0, \ldots, r_n \in D$ (distinct) and arbitrary $s_0, \ldots, s_n \in D$, we can find $f \in \text{Int}(D)$ with $f(r_i) = s_i$ for $0 \leq i \leq n$ [3]. If this holds for a

[1] This research was supported by the Austrian Science Fund FWF grant P30934-N35.

domain D, we say that D has the interpolation property. The domains having the interpolation property have been characterized among Noetherian domains and among Prüfer domains [2], and include, as mentioned, all Dedekind domain with finite residue fields.

It turned out that the interpolation property is relevant to the question whether $\mathrm{Int}(D)$ is a Prüfer domain. If D is Prüfer (a necessary condition for $\mathrm{Int}(D)$ to be Prüfer) then $\mathrm{Int}(D)$ is Prüfer if and only if $\mathrm{Int}(D)$ has the interpolation property [2].

Second, about the representation of functions on D/I, where I is an ideal of D: Let $f \in \mathrm{Int}(D)$. We say that f is I-congruence preserving, if, for all $a, b \in D$,

$$a \equiv b \mod I \quad \Longrightarrow \quad f(a) \equiv f(b) \mod I.$$

In that case, f induces a well-defined function on D/I by $f(a+I) = f(a)+I$. Let D be a Dedekind domain with finite residue fields. If I is a power of a maximal ideal of D (and only if I is a power of a maximal ideal), every function on D/I arises from an I-congruence preserving polynomial in $\mathrm{Int}(D)$ in this way. This was shown for $D = \mathbb{Z}$ by Skolem [7] (in the "if" direction) and Rédei and Szele [5,6] (in the "only if" direction), and later generalized to Dedekind domains [4].

If D is a Dedekind domain with finite residue fields, we will show that, given $r_0, \ldots, r_n \in D$ (distinct) and arbitrary $s_0, \ldots, s_n \in D$, and a finite set of powers P^{k_P} of maximal ideals such that the r_i are pairwise incongruent modulo each P^{k_P}, we can find a polynomial $f \in \mathrm{Int}(D)$ with $f(r_i) = s_i$ for $0 \leq i \leq n$ and such that

$$a \equiv b \mod P^{k_P} \quad \Longrightarrow \quad f(a) \equiv f(b) \mod P^{k_P}.$$

for each P^{k_P}, cf. Thm. 1.

A note on terminology: if R is any ring and $f \in R[x]$ a polynomial, $f = \sum_k c_k x^k$ induces a function by substitution of elements of R for the variable: $r \mapsto \sum_k c_k r^k$. A function $\varphi\colon R \to R$ thus arising from a polynomial $f \in R[x]$ is called a polynomial function on R.

When R is an infinite domain, then the polynomial f inducing a polynomial function is uniquely determined by its values on an infinite subset of R. Relying on this one-to-one correspondence between polynomials and polynomial functions, in the case where $R = K$ is an infinite field, we will not be as pedantic about the distinction between polynomials and polynomial functions as would be necessary if we were dealing with finite rings or rings with zero-divisors.

In what follows, when we talk about the function associated to an integer-valued polynomial $f \in \mathrm{Int}(D)$, we always mean the function $f\colon D \to D$ (as opposed to $f\colon K \to K$).

2 Notation and Definitions

We let $\mathbb{N}$ denote the positive integers (natural numbers) and $\mathbb{N}_0$ the non-negative integers. We use "additive" terminology for Lipschitz functions:

Definition 1. *Let R be a commutative ring, $f\colon R \to R$ a function, I an ideal of R, and $n \in \mathbb{N}_0$. We say that f is I-adically n-Lipschitz if, for all $m \in \mathbb{N}$ and all $a, b \in R$*

$$a \equiv b \mod I^{m+n} \quad \Longrightarrow \quad f(a) \equiv f(b) \mod I^m$$

When D is a domain, $g \in \mathrm{Int}(D)$, and I an ideal of D, we will say that g is I-adically n-Lipschitz if the associated function $g\colon D \to D$ is I-adically n-Lipschitz.

We summarize some elementary consequences of this definition.

Remark 1. Let R be a commutative ring, $f\colon R \to R$ a function, and I an ideal of R.

1. I-adically n-Lipschitz implies I-adically N-Lipschitz for all $N \geq n$.
2. If $f\colon R \to R$ is a function induced by a polynomial in $R[x]$ by substitution of the variable, then f is I-adically 0-Lipschitz for all ideals I of R.
3. For fixed I and n, the set of I-adically n-Lipschitz functions on R is closed under addition, subtraction and multiplication and, therefore, forms a subring of the set of all functions R^R.
4. If D is a domain, I an ideal of D and $n \in \mathbb{N}_0$, then the set of $g \in \mathrm{Int}(D)$ that are I-adically n-Lipschitz is a subring of $\mathrm{Int}(D)$.

In what follows, D is always a Dedekind domain with quotient field K, and we always assume $D \neq K$. For such a Dedekind domain, we denote by $\mathrm{Spec}^1(D)$ the set prime ideals of height one, which coincides with the set of maximal ideals of D. For $P \in \mathrm{Spec}^1(D)$, we use v_P to denote the normalized discrete valuation on K associated with P; that is, for $d \in D \setminus \{0\}$, $v_P(d)$ is the maximal exponent v such that $d \in P^v$, and, for an element of $K \setminus \{0\}$ expressed as a fraction a/b with $a, b \in D \setminus \{0\}$, $v_P(a/b) = v_P(a) - v_P(b)$.

Remark 2. Let D a Dedekind domain, $f \in \mathrm{Int}(D)$, and P a maximal ideal of D. If we express f as a fraction $f = g/d$ with $g \in D[x]$ and $d \in D \setminus \{0\}$, we see that f is P-adically $v_P(d)$-Lipschitz. In particular, if $f \in D_P[x]$, then f is P-adically 0-Lipschitz. More generally, if $f \in \mathrm{Int}(D)$ is expressed as a fraction $f = g/d$ with $g \in D_P[x]$ and $d \in D \setminus \{0\}$, then, also, f is P-adically $v_P(d)$-Lipschitz.

Note that $v_P(d)$, in the above remark, is not necessarily the minimal n for which f is P-adically n-Lipschitz (not even if d is relatively prime to the content of g). For instance, when f is a product $f = f_1 \dots f_n$ with $f_i = g_i/d$, $g_i \in D[x]$, then the denominator of f is d^n, but f is P-adically $v_P(d)$-Lipschitz, not just $v_P(d^n)$-Lipschitz, by Remark 1 (3).

We use $\|I\|$ for the norm of an ideal I of D, that is $\|I\| = |D/I|$.

3 *P*-adic Lipschitz constants of interpolating integer-valued polynomials

We recall a Lemma from an earlier paper that we will need for the proof of Lemma 2.

Lemma 1 ([3][Lemma 6.1]). *Let v be a discrete valuation on a field K and R_v its valuation ring. Suppose $g = \sum_{k=0}^{n} d_k x^k$ in $K[x]$ splits over K as*

$$g(x) = d_n(x - b_1)\dots(x - b_m)(x - c_1)\dots(x - c_l),$$

where $v(b_i) < 0$ and $v(c_i) \geq 0$.

Let $\mu = \min_{0\leq k\leq n} v(d_k)$ and set $g_+(x) = (x - c_1)\dots(x - c_l)$ then, for all $r \in R_v$,

$$v\big(g(r)\big) = \mu + v\big(g_+(r)\big).$$

Definition 2. *For q, m integers with $q > 1$ and $m \geq 0$ define*

$$L(q, m) := \frac{1 - q^m}{1 - q}$$

Lemma 2. *Let D be a Dedekind domain with finite residue fields and a_0, a_1 distinct elements of D. For $P \in \mathrm{Spec}^1(D)$, let $m_P = v_P(a_1 - a_0)$.*

For any finite set $\mathcal{F}$ of maximal ideals of D there exists $f \in \mathrm{Int}(D)$ with $f(a_1) = 0$ and $f(a_0) = 1$, and such that f is P-adically $L(\|P\|, m_P)$-Lipschitz for all $P \in \mathcal{F}$.

Proof. By linear substitution we may assume, w.l.o.g., that $a_0 = 0$. Also, we assume w.l.o.g. that $\mathcal{F}$ contains the set

$$\mathcal{P} = \{P \in \mathrm{Spec}^1(D) \mid\ a_1 \in P\} = \{P \in \mathrm{Spec}^1(D) \mid\ m_P > 0\}.$$

The case $\mathcal{P} = \emptyset$ is trivial. Assume $\mathcal{P} \neq \emptyset$. We set $\mathcal{F}_0 = \{P \in \mathcal{F} \mid m_P = 0\}$; such that $\mathcal{F}$ is the disjoint union of $\mathcal{P}$ and $\mathcal{F}_0$.

We will construct a polynomial $g \in K[x]$ with $g(a_1) = 0$, such that for every essential valuation v of D and every $r \in D$, $v\big(g(r)\big) \geq v\big(g(0)\big)$; and then set $f(x) = g(x)/g(0)$.

Let $N = \max_{P\in\mathcal{P}} \|P\|^{m_P}$. Using the Chinese Remainder Theorem modulo P^{m_P+1} for $P \in \mathcal{F}$, we produce a sequence $(b_i)_{i=1}^{N}$ in D with the properties:

1. $b_1 = a_1$
2. For all $P \in \mathcal{F}$, the b_i with $1 \leq i \leq \|P\|^{m_P}$ form a complete system of residues modulo P^{m_P}.
3. For all $P \in \mathcal{F}$, for all $i > \|P\|^{m_P}$, $b_i \equiv 1$ modulo P^{m_P+1}.

Note that no b_i is in P^{m_P+1} for any $P \in \mathcal{F}$, and, in particular, that no b_i is in P for any $P \in \mathcal{F}_0$.

Let $P \in \mathcal{P}$ and $1 \le k \le m_P$. For any given $r \in D$, the number of b_i with $1 \le i \le \|P\|^{m_P}$ in the residue class $r + P^k$ is the same, namely,

$$\gamma_k(P) \coloneqq \|P\|^{m_P - k}.$$

Note that, therefore, for all $P \in \mathcal{P}$ and $1 \le k \le m_P$,

$$\forall r \in D \ \ \big|\{i \mid v_P(r - b_i) \ge k\}\big| \ge \gamma_k(P),$$

with equality holding for all $r \in D \setminus (1 + P)$ (and, actually, for all $r \in D$ in the case where $\|P\|^{m_P} = N$).

Let $\mathcal{Q} = \{Q \in \mathrm{Spec}^1(D) \setminus \mathcal{P} \mid \exists i \ b_i \in Q\}$ and for $Q \in \mathcal{Q}$ let $k_Q = \max_i v_Q(b_i)$. Note that $\mathcal{Q} \cap \mathcal{F} = \emptyset$.

Let $c \in D$ with $v_Q(c) = k_Q + 1$ for all $Q \in \mathcal{Q}$, and $c \equiv 1 \mod P^{m_P+1}$ for all $P \in \mathcal{F}$. Let $\mathcal{Q}' = \{Q \in \mathrm{Spec}^1(D) \mid v_Q(c) > 0\}$. Then $\mathcal{Q} \subseteq \mathcal{Q}'$ and $\mathcal{Q}' \cap \mathcal{F} = \emptyset$.

Let $c_1 = a_1$ and for $1 < i \le N$ let $c_i = c^{-1} b_i$. Then, for every $P \in \mathrm{Spec}^1(D) \setminus \mathcal{Q}'$, and, in particular, for every $P \in \mathcal{F}$, $(c_i)_{i=1}^N$ is a sequence in D_P. Also, for every maximal ideal Q of D that is neither in $\mathcal{Q}'$ nor in $\mathcal{P}$, $v_P(c_i) = 0$ for all i.

We set

$$g(x) = \prod_{i=1}^{N} (x - c_i) = (x - a_1) \prod_{i=2}^{N} (x - c^{-1} b_i)$$

and show that for all essential valuations v of D and all $r \in D$, $v(g(r)) \ge v(g(0))$.

First, assume $P \in \mathcal{P}$. The sequence $(c_i)_{i=1}^N$ enjoys the same properties with respect to PD_P that the sequence $(b_i)_{i=1}^N$ enjoys with respect to P, namely, those c_i with $1 \le i \le \|P\|^{m_P}$ form a complete system of residues modulo $(PD_P)^{m_P}$ and $c_i \equiv 1$ modulo $(PD_P)^{m_P+1}$ for all $i > \|P\|^{m_P}$. Also, no c_i is in P^{m_P+1}.

Consequently, for all $r \in D$, and $1 \le k \le m_P$

$$\big|\{i \mid v_P(r - c_i) \ge k\}\big| = \big|\{i \mid v_P(r - b_i) \ge k\}\big| \ge \gamma_k(P).$$

Let $\gamma_P \coloneqq \sum_{k=1}^{m_P} \gamma_k(P)$. Then

$$v_P\big(g(r)\big) = \sum_{i=1}^{N} v_P(r - c_i) = \sum_{k=1}^{\infty} \big|\{i \mid v_P(r - c_i) \ge k\}\big| \ge$$

$$\ge \sum_{k=1}^{m_P} \big|\{i \mid v_P(r - c_i) \ge k\}\big| = \sum_{k=1}^{m_P} \big|\{i \mid v_P(r - b_i) \ge k\}\big| \ge \gamma_P,$$

while $v_P(g(0)) =$

$$= \sum_{k=1}^{\infty} \big|\{i \mid v_P(c_i) \ge k\}\big| = \sum_{k=1}^{m_P} \big|\{i \mid v_P(c_i) \ge k\}\big| = \sum_{k=1}^{m_P} \big|\{i \mid v_P(b_i) \ge k\}\big| = \gamma_P.$$

Now consider $Q \in \mathcal{Q}'$. Here $v_Q(c_1) = v_Q(a_1) = 0$ and, for all $i > 1$, $v_Q(c_i) < 0$. Let d_k be the coefficient of x^k in g and $\mu = \min_k v_Q(d_k)$. Using Lemma 1, we see that for all $r \in D$,

$$v_Q\big(g(r)\big) = \mu + v_Q(r - a_1) \ge \ \mu \ = \mu + v_Q(a_1) = v_Q\big(g(0)\big).$$

For the remaining essential valuations v of D, $v(c_i) = 0$ for all i, and, therefore, for all $r \in D$, $v\big(g(r)\big) = \sum_i v(r - c_i) \geq 0 = \sum_i v(c_i) = v\big(g(0)\big)$.

Now let $f(x) = g(x)/g(0)$. Then $f(a_1) = 0$, and $f(0) = 1$. Also, $f \in \mathrm{Int}(D)$, because for all $r \in D$ and every essential valuation v of D, $v\big(g(r)\big) \geq v\big(g(0)\big)$ and therefore $v\big(f(r)\big) \geq 0$.

As for the Lipschitz properties: for those $P \in \mathrm{Spec}^1(D)$ for which $v_P(c) = 0$, and, in particular, for all $P \in \mathcal{F}$, g is in $D_P[x]$. f is, therefore, P-adically $v_P(g(0))$-Lipschitz for all $P \in \mathcal{F}$ by Remark 2.

For $P \in \mathcal{F}_0$, $v_P(g(0)) = 0$ and hence f is P-adically 0-Lipschitz for all $P \in \mathcal{F}_0$.

For $P \in \mathcal{P}$,

$$v_P(g(0)) = \gamma_P = \sum_{k=1}^{m_P} \gamma_k(P) = \sum_{k=1}^{m_P} \|P\|^{m_P - k} = \sum_{j=0}^{m_P - 1} \|P\|^j = \frac{1 - \|P\|^{m_P}}{1 - \|P\|}.$$

f is, therefore, P-adically l_P-Lipschitz for all $P \in \mathcal{F}$, for the values of l_P stated in the Lemma.

Corollary 1. *Let D be a Dedekind domain with finite residue fields, $\mathcal{F}$ a finite set of maximal ideals, and $a_0, \ldots, a_n$ distinct elements of D. For each $P \in \mathcal{F}$, let $m_P \geq \max_{1 \leq i \leq n} v_P(a_i - a_0)$.*

Then there exists $f \in \mathrm{Int}(D)$ with $f(a_i) = 0$ for $1 \leq i \leq n$, and $f(a_0) = 1$, and such that f is P-adically $L(\|P\|, m_P)$-Lipschitz for all $P \in \mathcal{F}$.

Proof. For each $1 \leq i \leq n$ and $P \in \mathcal{F}$, let $m_P(i) = v_P(a_i - a_0)$ and $l_P(i) = L(\|P\|, m_P(i))$. Let $f_i \in \mathrm{Int}(D)$ with $f(a_i) = 0$ and $f(a_0) = 1$ and such that f_i is P-adically $L(\|P\|, m_P(i))$-Lipschitz for each $P \in \mathcal{F}$. Such an f_i exists by Lemma 2, and it is P-adically $L(\|P\|, m_P)$-Lipschitz, because $m_P(i) \leq m_P$, and $L(q, m)$ is an increasing function in m for fixed q, and l-Lipschitz implies l'-Lipschitz for all for all $l' \geq l$. Now set $f(x) = \prod_{i=1}^n f_i(x)$.

4 Interpolation by congruence-preserving integer-valued polynomials

Lemma 3. *Let D be a Dedekind domain with finite residue fields and $r_0, \ldots, r_n$ distinct elements of D.*

Let $\mathcal{F}$ be a finite set of maximal ideals of D. For each $P \in \mathcal{F}$, let $k_P \in \mathbb{N}$ such that the r_i are pairwise incongruent modulo P^{k_P} and $l_P = L(\|P\|, k_P - 1)$ as in Definition 2.

Then there exists $f \in \mathrm{Int}(D)$ such that

1. *$f(r_0) = 1$ and, for $1 \leq i \leq n$, $f(r_i) = 0$;*
2. *for each $P \in \mathcal{F}$, for every $r \in D \setminus (r_0 + P^{k_P})$, $f(r) \equiv 0 \mod P^{k_P}$;*
3. *for each $P \in \mathcal{F}$, for every $r \in r_0 + P^{k_P + l_P}$, $f(r) \equiv 1 \mod P^{k_P}$.*

Proof. We will first construct a polynomial $f_P \in \mathrm{Int}(D)$ for each $P \in \mathcal{F}$, in several steps. Fix $P \in \mathcal{F}$.

Extend $r_0, \ldots, r_n$ to a complete set of residues $r_0, \ldots, r_{\|P\|^{k_P}-1}$ modulo P^{k_P}, such that for all $i > n$ and all $Q \in \mathcal{F} \setminus \{P\}$, $r_i \equiv r_1$ modulo Q^{k_Q+1}.

Let C be a subset of $\prod_{Q\in\mathcal{F}} Q^{k_Q}$ containing a complete system of residues of the residue classes of $P^{k_P+l_P}$ contained in P^{k_P}, and with $0 \in C$.

For each $1 \le i < \|P\|^{k_P}$, and $c \in C$, let f_{ic} a polynomial in $\mathrm{Int}(D)$ with $f_{ic}(r_0) = 1$, $f_{ic}(r_i + c) = 0$, and Q-adically l_Q-Lipschitz for all $Q \in \mathcal{F}$, such as we know to exist by Lemma 2 and its Corollary. Set $f_i = \prod_{c\in C} f_{ic}$. Then $f_i(r_i) = 0$ and $f_i(r_0) = 1$. Also, since $\bigcup_{c\in C} r_i + c + P^{k_P+l_P} = r_i + P^{k_P}$ and $f_i(r_i + c) = 0$ for all $c \in C$, the P-adic Lipschitz property implies that for all $r \in r_i + P^{k_P}$, $f_i(r) \equiv 0$ modulo P^{k_P}. Likewise, the Lipschitz properties of the polynomials f_{ic} imply for all $Q \in \mathcal{F}$ that $f_i(r) \equiv 1$ modulo Q^{k_Q} for all $r \in r_0 + Q^{k_Q+l_Q}$.

Let $f_P = \prod_{i=1}^{\|P\|^{k_P}-1} f_i$. Then f_P satisfies

1. $f_P(r_0) = 1$ and $f_P(r_j) = 0$ for $1 \le j \le n$;
2. $f_P(r) \equiv 0$ modulo P^{k_P} for $r \in D \setminus (r_0 + P^{k_P})$;
3. for all $Q \in \mathcal{F}$, for all $r \in r_0 + Q^{k_Q+l_Q}$, $f_P(r) \equiv 1$ modulo Q^{k_Q}.

Having constructed f_P for each $P \in \mathcal{F}$, we set $f = \prod_{P\in\mathcal{F}} f_P$, and f has the desired properties.

Theorem 1. *Let D be a Dedekind domain with finite residue fields, $r_0, \ldots, r_n$ distinct elements of D and $s_0, \ldots, s_n$ arbitrary elements of D.*

Let $\mathcal{F}$ be a finite set of maximal ideals of D. For each $P \in \mathcal{F}$ let $k_P \in \mathbb{N}$ such that the r_i are pairwise incongruent modulo P^{k_P}.

Then there exists $f \in \mathrm{Int}(D)$ such that

1. *$f(r_i) = s_i$ for $0 \le i \le n$; and*
2. *for all $P \in \mathcal{F}$, for all $a, b \in D$,*

$$a \equiv b \mod P^{k_P} \quad \Longrightarrow \quad f(a) \equiv f(b) \mod P^{k_P}.$$

Proof. It suffices to show, for each index i, the existence of a polynomial $h_i \in \mathrm{Int}(D)$ such that

1. $h_i(r_i) = 1$ and $h_i(r_j) = 0$ for $j \ne i$,
2. for all $P \in \mathcal{F}$, for all $r \in D \setminus (r_i + P^{k_P})$, $h_i(r) \equiv 0 \mod P^{k_P}$, and
3. for all $P \in \mathcal{F}$, for all $r \in r_i + P^{k_P}$, $h_i(r) \equiv 1 \mod P^{k_P}$,

because, then, the polynomial $f = \sum_{i=0}^{n} s_i h_i$ does the job.

W.l.o.g., assume $i = 0$. We construct h_0 with the help of Lemma 3:

For each $Q \in \mathcal{F}$, let $l_Q = L(\|Q\|, k_Q - 1)$.

Let C be a subset of $\prod_{Q\in\mathcal{F}} Q^{k_Q}$ containing, for each $Q \in \mathcal{F}$, a complete system of residues of the residue classes of $Q^{k_Q+l_Q}$ contained in Q^{k_Q}, and with $0 \in C$.

For each $d \in C$, $r_0+d, r_1, \ldots, r_n$ satisfy the premises of Lemma 3. Accordingly, let $f_d \in \mathrm{Int}(D)$ such that

1. $f_d(r_0 + d) = 1$ and, for $1 \le i \le n$, $f_d(r_i) = 0$;
2. for each $P \in \mathcal{F}$, for every $r \in D \setminus (r_0 + d + P^{k_P})$, $f_d(r) \equiv 0 \mod P^{k_P}$;
3. for each $P \in \mathcal{F}$, for every $r \in r_0 + d + P^{k_P + l_P}$, $f_d(r) \equiv 1 \mod P^{k_P}$.

and set $g_d = 1 - f_d$.

Since $r_0 + d + P^{k_P} = r_0 + P^{k_P}$ for all $P \in \mathcal{F}$ and $d \in C$, each g_d satisfies

1. $g_d(r_0 + d) = 0$ and, for $1 \le i \le n$, $g_d(r_i) = 1$;
2. for each $P \in \mathcal{F}$, for every $r \in D \setminus (r_0 + P^{k_P})$, $g_d(r) \equiv 1 \mod P^{k_P}$;
3. for each $P \in \mathcal{F}$, for every $r \in r_0 + d + P^{k_P + l_P}$, $g_d(r) \equiv 0 \mod P^{k_P}$.

Now, set $g = \prod_{d \in C} g_d$.

Considering that, for all $P \in \mathcal{F}$, $\bigcup_{d \in C} r_0 + d + P^{k_P + l_P} = r_0 + P^{k_P}$, we see that the polynomial $g = \prod_{d \in C} g_d$ satisfies

1. $g(r_0) = 0$ and, for $1 \le i \le n$, $g(r_i) = 1$;
2. for each $P \in \mathcal{F}$, for every $r \in D \setminus (r_0 + P^{k_P})$, $g(r) \equiv 1 \mod P^{k_P}$;
3. for each $P \in \mathcal{F}$, for every $r \in r_0 + P^{k_P}$, $g(r) \equiv 0 \mod P^{k_P}$.

Finally, we let $h_0 = 1 - g$.

References

1. Cahen, P.J., Chabert, J.L.: Integer-valued polynomials, Mathematical Surveys and Monographs, vol. 48. American Mathematical Society, Providence, RI (1997)
2. Cahen, P.J., Chabert, J.L., Frisch, S.: Interpolation domains. J. Algebra 225(2), 794–803 (2000), http://dx.doi.org/10.1006/jabr.1999.8151
3. Frisch, S.: Interpolation by integer-valued polynomials. J. Algebra 211(2), 562–577 (1999), http://dx.doi.org/10.1006/jabr.1998.7741
4. Frisch, S.: Polynomial functions on finite commutative rings. In: Dobbs, D.E., Fontana, M., Kabbaj, S.E. (eds.) Advances in commutative ring theory (Fez, 1997), Lecture Notes in Pure and Appl. Math., vol. 205, pp. 323–336. Dekker, New York (1999)
5. Rédei, L., Szele, T.: Algebraischzahlentheoretische Betrachtungen über Ringe. I. Acta Math. 79, 291–320 (1947), https://doi.org/10.1007/BF02404701
6. Rédei, L., Szele, T.: Algebraisch-zahlentheoretische Betrachtungen über Ringe. II. Acta Math. 82, 209–241 (1950), https://doi.org/10.1007/BF02398278
7. Skolem, T.: Einige Sätze über Polynome. Avh. Norske Vid. Akad. Oslo. I. 1940(4), 16 (1940)