Biblioteca de la Revista Matemática Iberoamericana
Proceedings of the "Segundas Jornadas de Teoría de Números" (Madrid, 2007), 63–81

Möbius inversion from the point of view of arithmetical semigroup flows

Manuel Benito, Luis M. Navas and Juan Luis Varona

Abstract

Most, if not all, of the formulas and techniques which in number theory fall under the rubric of "Möbius inversion" are instances of a single general formula involving the action or flow of an arithmetical semigroup on a suitable space and a convolution-like operator on functions.

The aim in this exposition is to briefly present the general formula in its abstract context and then illustrate the above claim using an extensive series of examples which give a flavor for the subject. For simplicity and to emphasize the unifying character of this point of view, these examples are mostly for the traditional number theoretical semigroup $\mathbb{N}$ and the spaces $\mathbb{R}$ or $\mathbb{C}$.

1. Introduction

The "Möbius Inversion Formula" in elementary number theory most often refers to the formula

$$\widehat{f}(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d) \widehat{f}\left(\frac{n}{d}\right), \tag{1.1}$$

where f is an arithmetical function, that is, a function on $\mathbb{N}$ with values typically in $\mathbb{Z}$, $\mathbb{R}$ or $\mathbb{C}$; the sum ranges over the positive divisors d of a given

2000 Mathematics Subject Classification: Primary 11A25.
Keywords: Möbius function, Möbius transform, Dirichlet convolution, inversion formula, arithmetical semigroup, flow.

$n \in \mathbb{N}$, and μ is of course the Möbius function, given by

$$\begin{cases} \mu(1) = 1, \\ \mu(n) = 0 \text{ if } n \text{ has a squared factor,} \\ \mu(p_1 p_2 \cdots p_k) = (-1)^k \text{ when } p_1, p_2, \dots, p_k \text{ are distint primes.} \end{cases} \tag{1.2}$$

As is well known, the proper abstract context for this formula is that of *Dirichlet convolution* of arithmetical functions. Namely, if we define $f * g(n) = \sum_{ab=n} f(a)g(b)$, then pointwise addition and $*$ make the set of arithmetical functions into a commutative ring, with identity given by the delta function at 1, defined as $\delta(1) = 1$ and $\delta(n) = 0$ if $n \neq 1$.

The inversion formula then expresses two important facts. The first is that μ is the "Dirichlet inverse" of the constant function 1 with respect to $*$, in other words, $1 * \mu = \mu * 1 = \delta$. Written out, this means

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1. \end{cases} \tag{1.3}$$

The second thing to note is the functional transform nature of the formula. The operation $\widehat{f} = 1 * f$ is called the *Möbius transform* and the inversion formula is then $f = \mu * \widehat{f}$. This type of transform is a discrete analog of the convolution transforms, or "multipliers", whose study forms an extensive branch of harmonic analysis. In this context, the inversion formula is a trivial algebraic consequence of the first fact and the associativity of convolution.

Let us briefly survey some of the most well-known and useful formulas that are also labelled as "Möbius inversion", staying within number theory to preserve the arithmetical flavor of the subject, although there are also interesting and fruitful applications of this concept in other realms, a notable one being combinatorics.

For f a real or complex function, one often finds the inverse pairs

$$\begin{aligned} \widehat{f}(x) &= \sum_{n=1}^{\infty} f(nx), \qquad & f(x) &= \sum_{n=1}^{\infty} \mu(n)\, \widehat{f}(nx) \\ \widehat{f}(x) &= \sum_{n=1}^{\infty} f(x/n), \qquad & f(x) &= \sum_{n=1}^{\infty} \mu(n)\, \widehat{f}(x/n) \end{aligned} \tag{1.4}$$

(see for example [11, § 16.5, Th. 270] or [17, § 20]). It may come as a surprise that Möbius' original inversion formula is *not* (1.1) but rather, the inversion of the transform $\widehat{f}(x) = \sum_n a_n f(x^n)$ for a given analytic function f (see Example 14 and, for a historical survey of inversion, [2]). Riemann famously used inversion in his approximation of the number of primes less than or equal to x by $\sum_{n=1}^{\infty} \mu(n) n^{-1} \operatorname{Li}(x^{1/n})$, so that we may add the transform $\widehat{f}(x) = \sum_{n=1}^{\infty} a_n f(x^{1/n})$ to the mix. Much more recently, in [13], a paper of mathematical physics, one encounters $\sum_{n=1}^{\infty} f(n^a x)$ with $a \in \mathbb{R}$, with inversion formula attributed to Chen.

It is apparent that all these transforms have the form

$$\widehat{f}(x) = \sum_{n=1}^{\infty} a_n f(\varphi(n,x))$$

for some operation φ. Consideration of the separate *proofs* of the corresponding inversion formulas shows that there are again two essential phenomena at work. One is Dirichlet inversion, namely, the coefficient sequence a_n represents an arithmetical function whose Dirichlet inverse is the sequence of coefficients in the inverse transform. This is Möbius' idea, with the special case of the constant sequence $a_n = 1$ being the most common, leading to the Möbius function upon inverting.

The second, and mostly neglected, fact is that the inversion formula holds also because of the following properties of the operation φ:

$$\varphi(n, \varphi(m,x)) = \varphi(nm, x), \qquad \varphi(1,x) = x.$$

This is precisely the definition of a "flow" or "action" of the semigroup $\mathbb{N}$ on a space X which here is $\mathbb{R}$ or $\mathbb{C}$. To emphasize the dynamical aspects of some of the applications, we prefer to use the standard terminology of dynamical systems and call φ a flow.

Now, this observation is not new. In fact, for $\mathbb{N}$-flows on $\mathbb{R}$ and ignoring questions of convergence, this "flow transform", with its corresponding inversion formula, goes back to Cesàro [5] in the 1880s! It may have been too far ahead of its time, since it has been apparently long forgotten. Currently, we recognize a certain "general principle" of Möbius inversion but cite and prove each case separately. Actually, at least in [4], from 1991, it has been partially rediscovered, and perhaps there are other instances.

We feel that the growing number of inversion formulas, not only in number theory, but also especially in physics, bring renewed interest to the flow transform and require a modern rigorous formulation in terms of semigroups acting on topological spaces as well as a study of its algebraic and analytical properties (convolutional properties, convergence, validity of inversion, etc.). We have attempted to begin this study in [3]. Here we will only state the general formulas and point out the associated facts, instead focusing on examples, old and new, to illustrate its use.

2. Inversion for flow transforms

Let us briefly establish the context we need and then proceed to state the general Möbius inversion formula for arithmetical flows.

Recall that an *arithmetical semigroup* S is, in fact, a commutative monoid (there is an identity element 1) having a finite or countably infinite subset $\mathbb{P}$ called the *primes* such that S has unique factorization into primes, namely, every element $n \in S$ different from 1 has an expression as $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where the p_i are distinct primes and the e_i are positive integers, and these data are uniquely determined by n, modulo reordering. In addition, there is a *norm* mapping $\mathbf{N} : S \to \mathbb{R}$ satisfying

(i) $\mathbf{N}(1) = 1$ and $\mathbf{N}(p) > 1$ for $p \in \mathbb{P}$,

(ii) $\mathbf{N}(ab) = \mathbf{N}(a)\mathbf{N}(b)$ for all $a, b \in S$,

(iii) for each $x > 0$ there are only finitely many $s \in S$ with $\mathbf{N}(s) \leq x$.

See [12] for the general theory of arithmetical semigroups and how one can generalize analytic number theory to them, as well as their applications to problems of enumeration of objects in various categories such as those of finite graphs or topological spaces.

If R is a commutative ring, an R-valued arithmetical function on S is simply a function $\alpha : S \to R$. Just as in the case $S = \mathbb{N}$, the set $\mathbb{A}$ of such arithmetical functions is a commutative R-algebra with respect to pointwise sum and generalized Dirichlet convolution, defined by

$$(\alpha * \beta)(n) = \sum_{ab=n} \alpha(a)\beta(b). \tag{2.1}$$

The multiplicative unit is the delta function δ at the identity element of S. If we also define the Möbius function of S just as for $S = \mathbb{N}$, via (1.2), then the relation $1 * \mu = \delta$ holds in general.

Analogously, an arithmetical function α on S is said to be *multiplicative* if $\alpha(nm) = \alpha(n)\alpha(m)$ when n, m are coprime, and *completely multiplicative* if this holds for *every* $n, m \in S$. Multiplicativity is preserved by convolution. The Möbius function is multiplicative.

If S is any semigroup and X is a set, an S-*flow* on X is a map $\varphi : S \times X \to X$ satisfying $\varphi(m, \varphi(n, x)) = \varphi(mn, x)$. If S has a unit, 1 (e.g. if S is an arithmetical semigroup), then we also require that $\varphi(1, x) = x$. If S is a topological semigroup and X a topological space then we require joint continuity of φ.

One may alternatively think of a flow as a representation, in other words, as a semigroup homomorphism of S into the monoid $\mathbb{E}(X)$ of self-maps of X.

Instead of writing $\varphi(s,x)$ we may separate the element of the semigroup and write $\varphi_s(x)$, where $\varphi_s \circ \varphi_t = \varphi_{st}$. We think of the elements of the semigroup as "pushing" the points of X around. In physical applications, s often represents an instant of time.

If S is an arithmetical semigroup, an S-flow on a space X may be regarded as a collection of commuting self-maps of X indexed by the primes, $\{\varphi_p : p \in \mathbb{P}\}$, in addition to the identity map $\varphi_1 = \iota$. By unique factorization, the map corresponding to $n = \prod_{i=1}^{r} p_i^{e_i}$ is the composition

$$\varphi_n = \varphi_{p_1}^{\circ e_1} \circ \cdots \circ \varphi_{p_r}^{\circ e_r}, \tag{2.2}$$

where the superscript circle notation denotes iterated composition.

Let S be an arithmetical semigroup, and φ an S-flow on a space X. Let R be a commutative ring, complete with respect to a valuation $|\cdot|$, and M an R-module, complete with respect to a $|\cdot|$-norm $\|\cdot\|$. We define the *φ-generalized convolution* of an R-valued arithmetical function α on S with a function $f : X \to M$ by

$$(\alpha \odot_\varphi f)(x) = \sum_{n \in S} \alpha(n) f(\varphi(n,x)) = \sum_{n \in S} \alpha(n) f(\varphi_n(x)), \tag{2.3}$$

provided the series converges. Note that $\alpha \odot_\varphi f$ is a new function from X to M. The inspiration for this definition comes from [1, § 2.14] by generalizing to arithmetical semigroups and incorporating the flow. The subscript φ may be dropped for a fixed flow.

In the "classical" transforms mentioned in the introduction, the semigroup is $S = \mathbb{N}$, the space X is usually a subset of $\mathbb{R}$, and the ring R and module M are an appropriate combination of $\mathbb{Z}$, $\mathbb{R}$ or $\mathbb{C}$, with the usual absolute value. The need for more general algebraic structures should be apparent when one recalls other well-known examples of Möbius inversion, using the "standard" formula (1.1), where the range is not a subset of $\mathbb{C}$, such as the expression for the mth cyclotomic polynomial

$$\Phi_n(z) = \prod_{d \mid n} (z^d - 1)^{\mu(n/d)},$$

in which it is $\mathbb{Q}(z)^*$, or that of the product of all monic irreducible polynomials of degree n over the finite field $\mathbb{F}_q$ of q elements (often found in applications to Cryptography),

$$P_n(x) = \prod_{d \mid n} (x^{q^{n/d}} - x)^{\mu(d)},$$

in which it is $\mathbb{F}_q(x)^*$. Hence the usefulness of at least the verbatim generalization of (1.1) to any structure in which we can "add", i.e., to any *abelian group.* However, the elegant interpretation via convolution requires *two* operations, hence most naturally a *ring* structure. Similarly, the functional transforms require addition and also a product of the function by the coefficient sequence, the natural context for a *module.*

These needs are all reconciled by introducing a commutative ring R and an R-module M, and using an "asymmetric" convolution, where one function takes values in R and the other in M. Since an abelian group is a $\mathbb{Z}$-module, this includes the generalization mentioned above. The existence of a canonical homomorphism from $\mathbb{Z}$ to R shows that (1.3) holds whether we consider μ as $\mathbb{Z}$ or as R-valued, thus providing a useful "functoriality".

We shall mostly avoid questions of convergence, which are detailed in [3], in favor of the purely algebraic aspects which yield inversion formulas. The crucial result is the following "mixed associative property" of Dirichlet and φ-convolution:

Theorem 1. *Let S be an arithmetical semigroup, R a complete valued commutative ring, M a complete normed R-module, X a set, and φ an S-flow on X. Given arithmetical functions $\alpha, \beta : S \to R$ and a function $f : X \to M$, we have, under the appropriate convergence hypotheses,*

$$\alpha \odot_\varphi (\beta \odot_\varphi f) = (\alpha * \beta) \odot_\varphi f \tag{2.4}$$

where $*$ denotes Dirichlet convolution (2.1)*, and $\odot_\varphi$ is the "generalized flow convolution" defined in* (2.3)*. In addition, one also has the trivial formula*

$$\delta \odot_\varphi f = f,$$

stating that δ, the identity for $*$, is also a left identity for $\odot_\varphi$.

Proof. Ignoring convergence, this follows directly from the definitions:

$$\begin{aligned}
(\alpha \odot_\varphi (\beta \odot_\varphi f))(x) &= \sum_{n \in S} \alpha(n)(\beta \odot_\varphi f)(\varphi(n, x)) \\
&= \sum_{n \in S} \alpha(n) \sum_{m \in S} \beta(m) f(\varphi(m, \varphi(n, x))) \\
&= \sum_{n,m \in S} \alpha(n)\beta(m) f(\varphi(nm, x)) \\
&= \sum_{k \in S} \left(\sum_{nm=k} \alpha(n)\beta(m) \right) f(\varphi(k, x)) \\
&= \sum_{k \in S} (\alpha * \beta)(k) f(\varphi(k, x)) \\
&= ((\alpha * \beta) \odot_\varphi f)(x).
\end{aligned}$$

■

The main inversion result immediately follows.

Theorem 2. *With notation and hypotheses as in Theorem 1, given an arithmetical function $\alpha : S \to R$, invertible with respect to Dirichlet convolution* (2.1)*, with inverse α^{-1}, then under the appropriate convergence hypotheses, we have the inversion relation*

$$\widehat{f} = \alpha \odot_{\varphi} f, \qquad f = \alpha^{-1} \odot_{\varphi} \widehat{f}. \tag{2.5}$$

Proof. Ignoring convergence (which can be rather subtle!), this is a trivial consequence of Theorem 1. If $\widehat{f} = \alpha \odot_{\varphi} f$, then

$$\alpha^{-1} \odot_{\varphi} \widehat{f} = \alpha^{-1} \odot_{\varphi} (\alpha \odot_{\varphi} f) = (\alpha^{-1} * \alpha) \odot_{\varphi} f = \delta \odot_{\varphi} f = f,$$

and similarly, starting from $f = \alpha^{-1} \odot_{\varphi} \widehat{f}$, we get $\widehat{f} = \alpha \odot_{\varphi} f$. ■

A special case is actual *Möbius* inversion for a flow, namely, formulas involving the Möbius function μ.

Theorem 3. *With notation and hypotheses as in Theorem 1, given a nonzero completely multiplicative arithmetical function $\alpha : S \to R$, then under appropriate convergence conditions, we have the inversion relation*

$$\widehat{f}(x) = \sum_{n \in S} \alpha(n) f(\varphi(n,x)), \qquad f(x) = \sum_{n \in S} \mu(n)\alpha(n)\widehat{f}(\varphi(n,x)). \tag{2.6}$$

The traditional case is $\alpha = 1$, where $\alpha^{-1} = \mu$.

Proof. When α is completely multiplicative, one has $\alpha^{-1} = \mu\alpha$. ■

One way to "ignore" convergence problems is to make the sums *finite* by considering functions f whose support Z is such that the orbit $\{\varphi(n,x) : n \in S\}$ escapes Z as $\mathbf{N}(n) \to \infty$. For example, when $S = \mathbb{N}$, $X = (0,+\infty)$ and $\varphi(n,x) = x/n$, one often takes functions vanishing on $(0,1)$, as we will see in the first example.

3. Examples

Example 1. (*The usual inversion formula*). The "standard" formula (1.1) is actually a consequence of the case $S = \mathbb{N}$, $R = \mathbb{Z}$, $X = (0,+\infty)$, and M an abelian group (with appropriate valuations and norms), using the flow $\varphi(x,n) = x/n$ and convolving with $\alpha = 1$. By Theorem 3, we have the inversion formula

$$\widehat{f}(x) = \sum_{d=1}^{\infty} f\left(\frac{x}{d}\right), \qquad f(x) = \sum_{d=1}^{\infty} \mu(d)\widehat{f}\left(\frac{x}{d}\right), \tag{3.1}$$

under suitable convergence conditions. In particular, let f have support in $[1,+\infty)$. Then the sums in the above formula are finite; therefore, we can forget about topology, and we obtain the special case

$$\widehat{f}(x) = \sum_{d=1}^{\lfloor x\rfloor} f\left(\frac{x}{d}\right), \qquad f(x) = \sum_{d=1}^{\lfloor x\rfloor} \mu(d)\widehat{f}\left(\frac{x}{d}\right). \tag{3.2}$$

Now, to get (1.1), one only need restrict further to functions with support in $\mathbb{N}$, substituting $x = n \in \mathbb{N}$ in the above formula.

Example 2. (***The standard inversion formulas***)**.** We have mentioned some of the following commonly encountered transforms:

$$\sum_{n=1}^{\infty} \alpha(n)f(nx), \quad \sum_{n=1}^{\infty} \alpha(n)f(x/n), \quad \sum_{n=1}^{\infty} \alpha(n)f(x^n), \quad \sum_{n=1}^{\infty} \alpha(n)f(x^{1/n}),$$

the third appearing in Möbius' original inversion formula, from the 1832 paper [14]. These transforms correspond to the semigroup $S = \mathbb{N}$ and X, R, M are usually one of $\mathbb{R}^+ = (0,+\infty)$, $\mathbb{R}$ or $\mathbb{C}$. Möbius essentially treats x as a formal variable, which also fits into our framework. We may call the four flows in these transforms the standard $\mathbb{N}$-flows. Together they cover all the common examples of Möbius inversion.

Example 3. (***Modifications of flows***)**.** Let $\eta : S \to T$ be a semigroup homomorphism and $h : X \to Y$ a homeomorphism. If φ is a T-flow on Y then

$$\psi(s,x) = h^{-1}(\varphi(\eta(s), h(x))) \tag{3.3}$$

is an S-flow on X. This is clearer in the representation notation:

$$\psi_s = h^{-1} \circ \varphi_{\eta(s)} \circ h,$$

revealing the operations of conjugation by h and pullback by η.

The four standard flows in Example 2 may be obtained in this way. In general, start with $S = \mathbb{N}$ and choose a completely multiplicative function $\eta : S \to \mathbb{C}$. This is a homomorphism of S onto the image semigroup $T = \eta(S) \subseteq \mathbb{C}$. X and Y will be appropriate subspaces of $\mathbb{C}$, with $T \cdot Y \subseteq Y$ so that the restriction of multiplication on $\mathbb{C}$ is a T-flow on Y, which we denote by $\pi(t,y) = ty$. Now, consider the resulting modification of π:

$$\varphi(n,x) = h^{-1}(\eta(n)\, h(x)). \tag{3.4}$$

Take $\eta(n) = n^a$ for $a \in \mathbb{C}$. For $a = -1$ and $h(x) = x$ on $X = Y = \mathbb{R}^+$, $\mathbb{R}$ or $\mathbb{C}$, we obtain $\varphi(n,x) = x/n$. For $a = \pm 1$ and $h(x) = \log(x)$ on $X = \mathbb{R}^+$,

$Y = \mathbb{R}$, we obtain x^n and $x^{1/n}$. In general we obtain the flows $n^a x$ and x^{n^a}. The former is used in [13], as we mentioned above. For any $a \in \mathbb{R}$ and $h(x) = \exp x$ on $X = \mathbb{R}$, $Y = \mathbb{R}^+$, we obtain

$$\varphi(n, x) = x + a \log n,$$

which was apparently discovered by Cesàro ([2]), but has not to our knowledge been applied to any problem.

Example 4. (***The Chebyshev flow***)**.** In [9] we have, to our knowledge, a heretofore unknown inversion formula involving the Chebyshev polynomials T_n. The self-maps of $X = [-1, 1]$ given by the polynomials themselves, $\varphi_n(x) = T_n(x) = \cos(n \arccos x)$, define an $\mathbb{N}$-flow on X. The relation $T_n(T_m(x)) = T_{nm}(x)$ is often called the "nesting property".

A priori, the expression $\cos(n \arccos x)$ looks like a special case of (3.4). Note, however, that although $\cos : [0, \pi] \to [-1, +1]$ and $\arccos : [-1, +1] \to [0, \pi]$ are indeed inverse homeomorphisms, multiplication by $n \in \mathbb{N}$ does not yield a self-map of $[0, \pi]$. Of course, cos is defined on $\mathbb{R}$, on which multiplication acts, but arccos is not the inverse of $\cos : \mathbb{R} \to [-1, +1]$.

These difficulties can be avoided in proving $T_n(T_m(x)) = T_{nm}(x)$, by considering x in a small enough interval $[1 - \epsilon, 1]$, where $m \arccos x \in [0, \pi]$, and then using analytic continuation to extend the identity to all x.

Nevertheless, T_n *is* an example of conjugation by a homeomorphism as in (3.3). For instance, let Y be the quotient space of the unit circle $\mathbb{T}$ embedded in $\mathbb{C}$, modulo complex conjugation, that is, identifying points on the "top" and "bottom" halves of $\mathbb{T}$ which are symmetric across the real axis. Then $x \mapsto e^{i \arccos x}$ induces a homeomorphism $h : X \to Y$, whose inverse is the map induced by taking real parts, $\mathrm{Re} : \mathbb{T} \to [-1, +1]$. Since $T_n(x) = \mathrm{Re}(e^{i \arccos x})^n$, the Chebyshev flow is the conjugate via h of the flow induced on Y by the standard flow z^n on $\mathbb{T}$.

An example of inversion for this flow is

$$\widehat{f}(x) = \sum_{n=1}^{\infty} n^{-s} f(T_n(x)), \qquad f(x) = \sum_{n=1}^{\infty} \mu(n) n^{-s} \widehat{f}(T_n(x)) \tag{3.5}$$

(this formula is also related to Example 13). The series converge absolutely if, for example, the function f is bounded and we take $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$.

Example 5. (***Prime-independent flows***)**.** Fix a self-map Φ of a space X and define an S-flow on X by requiring that $\varphi_1 = \iota$ and $\varphi_p = \Phi$ for all primes p (hence the name *prime-independent*). By (2.2), $\varphi(n, x) = \Phi^{\circ \Omega(n)}$, where $\Omega(n)$ is the number of prime factors of n counted with multiplicity.

The convolution transform associated to this flow is

$$(\alpha \odot f)(x) = \sum_{n \in S} \alpha(n)\, f(\Phi^{\circ \Omega(n)}(x)). \tag{3.6}$$

This sum, assuming it is absolutely convergent, can be grouped according to the value of Ω. An easy way to obtain convergent sums is to use Dirichlet series: $\alpha(n) = n^{-s}$ ($s \in \mathbb{C}$ with $\operatorname{Re}(s) > 1$), and bounded f.

Example 6. (*Iterative flows*). Example 5 may be generalized by taking any nonnegative *completely additive* function $\ell : S \to \mathbb{Z}^+$, i.e. satisfying $\ell(nm) = \ell(n) + \ell(m)$ (Ω is such a function), and any self-map $\Phi : X \to X$. Then the ℓ-fold iterates of Φ define an S-flow on X, $\varphi(n, x) = \Phi^{\circ \ell(n)}(x)$, with convolution transform

$$(\alpha \odot f)(x) = \sum_{n \in S} \alpha(n)\, f(\Phi^{\circ \ell(n)}(x)). \tag{3.7}$$

If Φ is invertible, we may drop the requirement that ℓ be nonnegative.

Example 7. (*One prime, more iteration*). An arithmetical semigroup S with just one prime p is isomorphic to $(\mathbb{Z}^+, +, 0)$, where the identity element is 0 and whose unique prime is 1 (and for the norm $\mathbf{N}$ we can take, for instance, $\mathbf{N}(n) = 2^n$). If p is a prime in a larger arithmetical semigroup, we may consider the subsemigroup it generates, denoted by $S = \langle p \rangle$. Of course $\langle p \rangle = \{p^n\}_{n \ge 0}$.

Since every arithmetical semigroup is the direct sum of the semigroups generated by each of its primes, this case is a "building block" for others. Note however that an arbitrary arithmetical function is not determined by its values at the primes.

The Möbius function of $S = \langle p \rangle$ is given by $\mu(1) = 1$, $\mu(p) = -1$ and $\mu(p^n) = 0$ for $n > 1$. To give an S-flow φ on a space X is equivalent to choosing a self-map $\Phi : X \to X$ and declaring $\varphi_p = \Phi$. Then $\varphi_{p^n} = \Phi^{\circ n}$, the n-fold iterate of Φ.

An arithmetical function on $S = \langle p \rangle = \{p^n\}_{n \ge 0}$ with values in a commutative ring R is simply a sequence $\{a_n\}_{n=0}^{\infty}$ in R. If $A = \sum_{n=0}^{\infty} a_n T^n$ is the generating formal power series of the sequence, then the transform and corresponding inversion formula are given by

$$\widehat{f}(x) = \sum_{n=0}^{\infty} a_n f(\Phi^{\circ n}(x)), \qquad f(x) = \sum_{n=0}^{\infty} a_n^*\, \widehat{f}(\Phi^{\circ n}(x)), \tag{3.8}$$

where $\{a_n^*\}$ is the sequence whose generating series A^* is the multiplicative inverse of A as formal power series over R, that is, $AA^* = 1$. This follows because in $(\mathbb{Z}^+, +, 0)$, the "divisors" of $n \in \mathbb{Z}^+$ are the integers $0 \leq k \leq n$, and Dirichlet convolution is given by $(\alpha * \beta)(n) = \sum_{k=0}^{n} \alpha(k)\beta(n-k)$, or from a general structure theorem describing the arithmetical functions as a power series ring. Those familiar with Functional Analysis will recognize a similarity to the so-called "functional calculus".

A completely multiplicative arithmetical function α corresponds to a power sequence $\{a^n\}$, i.e., to the generating series $A = (1 - aT)^{-1}$. Inversion for these transforms is the "telescoping series trick":

$$\widehat{f}(x) = \sum_{n=0}^{\infty} a^n f(\Phi^{\circ n}(x)), \qquad f(x) = \widehat{f}(x) - a\widehat{f}(\Phi(x)) \tag{3.9}$$

(this is a rather trivial case of the formula $\alpha^{-1} = \mu\alpha$).

Essentially the same situation occurs if we take a prime p in any arithmetical semigroup S and define a flow by declaring $\varphi_1 = \iota$, $\varphi_p = \Phi$ and φ_q to be constant for primes $q \neq p$. Since the φ_q must commute, the constant must be independent of q and must be a fixed point a of Φ. Then $\varphi_n = a$ when $n \notin \langle p \rangle$.

Example 8. (*One prime: sums and differences*). For $S = (\mathbb{Z}^+, +, 0)$, with single prime 1, and the space $X = \mathbb{R}$, making 1 act via $\varphi(1, x) = \Phi(x) = x+1$ gives the translation flow $\varphi(n, x) = x+n$. Since the "divisors" of $n \in \mathbb{Z}^+$ are the integers $0 \leq k \leq n$, the classical Möbius inversion formula (1.1) reduces to the trivial (but nonetheless important!) relation between the summation and difference operators:

$$\widehat{f}(n) = \sum_{k=0}^{n} f(k), \qquad f(n) = \widehat{f}(n) - \widehat{f}(n-1). \tag{3.10}$$

Example 9. (*One prime: Vieta's formula for Pi*). Let $S = (\mathbb{Z}^+, +, 0)$, the one-prime arithmetical semigroup. Take $X = \mathbb{C}$ and let 1 act via $\Phi(z) = az$, with $a \in \mathbb{C}$ fixed. Its iterates define the flow $\varphi_n(z) = \Phi^{\circ n}(z) = a^n z$. The corresponding inversion formula is mentioned in [13] with physical applications. Note that if a is not a root of unity, this particular choice also corresponds to the restriction of the multiplication flow to the one-prime arithmetical semigroup $S = \{a^n\}_{n \geq 0} \subseteq \mathbb{C}$. Interestingly, Vieta's formula for π, which is the first recorded "exact formula" for this constant, and also the first infinite product in mathematics, is a special case:

$$\frac{2}{\pi} = \sqrt{\frac{1}{2}} \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}} \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}}} \cdots .$$

To see why this is so, consider the duplication formula for the sine function, $\sin(2z)/(2\sin z) = \cos z$. Let us modify this to $s(z)/s(z/2) = \cos(z/2)$, where $s(z) = z^{-1}\sin z$. Here $a = 1/2$. For the ring R, we take the integers $\mathbb{Z}$ and as $\mathbb{Z}$-module M, the group of nonzero meromorphic functions on $\mathbb{C}$ under multiplication. Thus our notation will be multiplicative rather than additive, and we will have infinite products instead of infinite sums. Now

$$f(z) = (\mu \odot s)(z) = \prod_{n=0}^{\infty} s(z/2^n)^{\mu(n)} = s(z)\cdot s(z/2)^{-1}\cdot 1\cdot 1\cdots,$$

so the duplication formula simply states that $f(z) = \cos(z/2)$, and hence inverting gives the convergent infinite product

$$\frac{\sin z}{z} = s(z) = (1 \odot f)(z) = \prod_{n=0}^{\infty} f(z/2^n) = \prod_{n=1}^{\infty} \cos\frac{z}{2^n} \tag{3.11}$$

which for $z = \pi/2$ turns out to be Vieta's formula. By the way, comparing this with $z = \pi/3$ yields the amusing, but probably useless,

$$\frac{2+\sqrt{3}}{2+\sqrt{2}}\cdot\frac{2+\sqrt{2+\sqrt{3}}}{2+\sqrt{2+\sqrt{2}}}\cdot\frac{2+\sqrt{2+\sqrt{2+\sqrt{3}}}}{2+\sqrt{2+\sqrt{2+\sqrt{2}}}}\cdots = \frac{9}{8}. \tag{3.12}$$

Other functions with "multiplication formulas" yield similar products:

$$\begin{gathered} \frac{\sin z}{z} = \prod_{n=1}^{\infty}\left(1 - \frac{4}{3}\sin^2\frac{z}{3^n}\right), \qquad \frac{z}{\tan z} = \prod_{n=1}^{\infty}\left(1 - \tan^2\frac{z}{2^n}\right), \\ \Gamma(z+1) = 4^z \prod_{n=1}^{\infty} \frac{1}{\sqrt{\pi}}\,\Gamma\left(\frac{1}{2} + \frac{z}{2^n}\right). \end{gathered} \tag{3.13}$$

Example 10. (*"Strange" functions*). Curiously, the simple one-prime semigroup also provides several standard examples in Analysis. We have, for instance, using the iteration of $\Phi(x) = ax$,

$$\sum_{n=1}^{\infty} b^n \cos(\pi a^n x),$$

which is one of Weierstrass' examples of a continous nowhere differentiable function (for suitable real a, b). He also gave

$$\sum_{n=1}^{\infty} \frac{\sin(\pi n^a x)}{\pi n^a},$$

which uses the flow mentioned in Example 3.

If instead we use $\Phi(z) = z^a$, with $a \in \mathbb{C}$ fixed, then $\Phi^{\circ n}(z) = z^{a^n}$. We get another telescoping inversion formula:

$$\widehat{f}(z) = \sum_{n=0}^{\infty} f(z^{a^n}), \qquad f(z) = \widehat{f}(z) - \widehat{f}(z^a). \tag{3.14}$$

For $a = 2$ and $f(z) = z$, the transform $\widehat{f}(z)$ is the standard example of an analytic function which cannot be continued to any point on the unit circle, i.e. this is its natural boundary.

A moment's reflection reveals that the density of the orbits of points under the flow is the reason these examples are "pathological".

Example 11. (***Two primes***)**.** Let S be the arithmetical subsemigroup of $\mathbb{N}$ generated by the primes 2 and 3. Take $X = \mathbb{C}$, $R = \mathbb{Z}$ and M the nonzero meromorphic functions on $\mathbb{C}$. We use the division S-flow $\varphi(n, z) = z/n$. From the formula

$$\frac{\sin(z)\sin(6z)}{\sin(2z)\sin(3z)} = 1 - 4\sin^2(z),$$

but using $s(z) = z^{-1}\sin z$ instead of sin, and dividing z by 6, the left hand side becomes $\mu \odot s$. Inversion gives a "two-prime formula":

$$\frac{\sin z}{z} = \prod_{n,m=1}^{\infty} \left(1 - 4\sin^2 \frac{z}{2^n 3^m}\right), \tag{3.15}$$

which, as might be expected, is the combination of two "one-prime formulas"

$$\prod_{n=1}^{\infty} \left(1 - 4\sin^2 \frac{z}{2^n}\right) = \frac{1}{3}(1 + 2\cos(4z)), \quad \prod_{m=1}^{\infty} \frac{1}{3}\left(1 + 2\cos\frac{4z}{3^m}\right) = \frac{\sin z}{z}.$$

Example 12. (***Multivariable inversion formulas***)**.** In [16] one finds inversion formulas such as

$$\widehat{f}(x) = \sum_{m,n=1}^{\infty} f(n^\alpha m^\beta x), \qquad f(x) = \sum_{m,n=1}^{\infty} \mu(m)\mu(n)\widehat{f}(n^\alpha m^\beta x),$$

with $\alpha, \beta > 0$, or

$$\widehat{f}(x) = \sum_{k=0}^{\infty} f(2^k x), \qquad f(x) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \mu(n)(-1)^{m+1}\frac{1}{mn}\widehat{f}(mnx),$$

where there are double sums. These correspond to the semigroup $S = \mathbb{N} \times \mathbb{N}$ and in general such formulas suggest studying direct sums of arithmetical semigroups. This is done in [3] where more examples are also given.

Example 13. (***Parametric Dirichlet series***)**.** Let us choose $R = \mathbb{C}$ as base ring, so the module M is a complex Banach space. Now, consider two-variable functions $f : \mathbb{C} \times X \to M$ and separate the first variable using the notation $f_s(x) = f(s, x)$. For fixed $s \in \mathbb{C}$, the function $\mathbf{N}(n)^{-s}$ is completely multiplicative. Considering the convolution $\mathbf{N}^{-s} \odot f_s$ leads to the inversion formula

$$(3.16) \qquad \widehat{f}(s,x) = \sum_{n \in S} \frac{f(s,\varphi(n,x))}{\mathbf{N}(n)^s}, \qquad f(s,x) = \sum_{n \in S} \frac{\mu(n)\,\widehat{f}(s,\varphi(n,x))}{\mathbf{N}(n)^s}.$$

These transforms represent Dirichlet series depending on the parameter x. For "reasonable" arithmetical functions they will converge absolutely for $\mathrm{Re}(s)$ large enough (but the bound may depend on x). By multiplying $\mathbf{N}^{-s}$ with completely multiplicative complex-valued functions, we obtain variations of this inversion formula. For example, using Liouville's function $\lambda(n) = (-1)^{\Omega(n)}$, which has inverse $|\mu(n)|$, we have

$$(3.17) \qquad \widehat{f}(s,x) = \sum_{n \in S} \frac{\lambda(n)\,f(s,\varphi(n,x))}{\mathbf{N}(n)^s}, \quad f(s,x) = \sum_{n \in S} \frac{|\mu(n)|\,\widehat{f}(s,\varphi(n,x))}{\mathbf{N}(n)^s}.$$

In [15, § 6.3, pp. 222–223] we find the special case of $S = \mathbb{N}$ and $\varphi(n,x) = x/n$. Using functions with support in $[1, +\infty)$ again makes the sums finite. One also finds $\varphi(n,x) = n^{-s}x$ considering a *real* fixed s and limiting the sum to $n \le x^{1/s}$.

In [3] we generalize the well-known property that the product of the Dirichlet series corresponding to several arithmetical functions is the Dirichlet series corresponding to their convolution. This fact, we recall, is the source of many well-known arithmetical identities involving the Riemann zeta function, such as

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \qquad \frac{\zeta(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s}, \qquad \zeta(s)^2 = \sum_{n=1}^{\infty} \frac{d(n)}{n^s},$$

where $d(n)$ is the number of divisors of n.

Example 14. (***Inversion of Taylor series***)**.** Consider $S = \mathbb{N}$ and $R = X = M = \mathbb{C}$. Inversion of convolution with respect to the exponential $\mathbb{N}$-flow $\varphi(n,z) = z^n$ has the form

$$(3.18) \qquad \widehat{f}(z) = \sum_{n=1}^{\infty} \alpha(n)\, f(z^n), \qquad f(z) = \sum_{n=1}^{\infty} \alpha^{-1}(n)\, f(z^n).$$

For $f(z) = z$, we are inverting a power series and obtaining an expansion for the identity. In his paper [14], we find the following nice example due to Möbius, inverting the Taylor series of the logarithm:

$$-\log(1-z) = \sum_{n=1}^{\infty} n^{-1} z^n, \qquad z = -\sum_{n=1}^{\infty} n^{-1}\mu(n)\log(1-z^n)$$

(convergent for $|z| < 1$). Exponentiating gives the product expansion

$$e^z = \prod_{n=1}^{\infty} (1-z^n)^{-\mu(n)/n}.$$

Substituting $z = p^{-s}$ for prime p and $\mathrm{Re}(s) > 1$, using the Euler product for the Riemann zeta function, $\zeta(s) = \prod_p (1 - 1/p^s)^{-1}$, and taking logarithms, we obtain a formula for the "prime zeta function" attributed to Glaisher:

$$\sum_p \frac{1}{p^s} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \log\zeta(ns), \qquad \mathrm{Re}(s) > 1.$$

From the inversion of the arctangent, whose Taylor series at 0 happens to be convolution with $\chi\rho$, where $\rho(n) = n^{-1}$ and $\chi = \chi_4$ is the non-trivial Dirichlet character modulo 4 ($\chi_4(m) = 0$ for even m and $\chi_4(m) = (-1)^{(m-1)/2}$ for odd m), and since Dirichlet characters are completely multiplicative, we obtain

(3.19)
$$\arctan z = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} z^{2n+1}, \quad z = \sum_{n=0}^{\infty} \frac{(-1)^n \mu(2n+1)}{2n+1} \arctan(z^{2n+1}).$$

Evaluating at $z = 1$ we get

$$\frac{\pi}{4} = \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1}, \qquad \frac{4}{\pi} = \sum_{n=0}^{\infty} \frac{(-1)^n \mu(2n+1)}{2n+1},$$

which is Leibniz's famous formula, and its Möbius inverse. This also follows from Example 13, considering $L(\chi, s)$ at $s = 1$.

Example 15. (*Lambert series*). If $\alpha : \mathbb{N} \to \mathbb{C}$ is an arithmetical function, recall that its associated Lambert series is

(3.20)
$$L_\alpha(z) = \sum_{n=1}^{\infty} \alpha(n) \frac{z^n}{1-z^n},$$

considered as a formal or, if appropriate, a convergent complex series. The Lambert series $L = L_\delta$ associated to the delta function δ is just

$$L(z) = \frac{z}{1-z}.$$

As a complex series, it converges for $|z| < 1$, and its Taylor expansion around 0 is the geometric series $\sum_{n=1}^{\infty} z^n$. In general, the usefulness of Lambert series comes from the general expression relating the Lambert (3.20) and Taylor expansions:

$$\sum_{n=1}^{\infty} \alpha(n) \frac{z^n}{1-z^n} = \sum_{n=1}^{\infty} \beta(n) z^n \qquad \text{with} \quad \beta(n) = \sum_{d|n} \alpha(d). \tag{3.21}$$

In terms of Dirichlet convolution, this reduces to $\beta = \alpha * 1$.

This basic property is easily seen to be a flow-convolution identity for the $\mathbb{N}$-flow $\varphi(n,z) = z^n$. Indeed, let I denote the identity series $I(z) = z$. As we have mentioned in Example 14, the Taylor series with coefficients given by an arithmetical function $\beta : \mathbb{N} \to \mathbb{C}$ is simply $\beta \odot I$. Thus, the geometric series expansion of L is the convolution formula $L = 1 \odot I$. On the other hand, for a given arithmetical function α, its associated Lambert series L_α is clearly $\sum_{n=1}^{\infty} \alpha(n) L(z^n)$, which is just $\alpha \odot L$. Then (3.21) is a consequence of the "mixed associative property" (2.4):

$$L_\alpha = \alpha \odot L = \alpha \odot (1 \odot I) = (\alpha * 1) \odot I = \beta \odot I \quad \text{where} \quad \beta = \alpha * 1.$$

This well-known relation is the source of many interesting formulas (see for example [11, § 17.10, pp. 257–258] or [12, § 58-C, pp. 448–452]), some of which are related to elliptic function q-expansions ([10, § 3.7 and 3.8]). For instance,

$$\sum_{n \text{ odd}} \frac{z^n}{1-z^n} = \sum_{n=1}^{\infty} d(n) z^n, \qquad \sum_{n=1}^{\infty} (-1)^{\Omega(n)} \frac{z^n}{1-z^n} = \sum_{n=1}^{\infty} z^{n^2},$$

where $d(n)$ is the number of divisors of n and $\Omega(n)$ is the number of prime divisors of n with multiplicities; $(-1)^\Omega$ is Liouville's λ function, as in (3.17).

Example 16. (*Möbius inversion of Fourier series*). Applying Möbius inversion to Fourier series goes at least as far back as Chebyshev [7] and appears recently in [8] in a study of a lattice problem in physics.

For example, a sine expansion is a convolution with respect to the multiplication flow. We write the inversion formula as

$$\widehat{f}(x) = \sum_{n=1}^{\infty} \alpha(n) \sin(2\pi n x), \qquad \sin(2\pi x) = \sum_{n=1}^{\infty} \alpha^{-1}(n) \widehat{f}(nx). \tag{3.22}$$

Chebyshev studied the Möbius inverses of the Fourier expansions of the square and triangular waves and obtained the value of some arithmetical sums. By thinking along similar lines we also obtain some curious values of infinite sums. By the triangular wave T we mean the period 1 extension to $\mathbb{R}$ of the function on $[0, 1)$ defined by

$$T(x) = 4x\, 1_{[0,1/4)}(x) + (2 - 4x)\, 1_{[1/4,3/4)}(x) + (4x - 4)\, 1_{[3/4,1)}(x),$$

where 1_A denotes the function which is 1 on A and 0 on A^c. Its Fourier expansion is

$$T(x) = \frac{8}{\pi^2} \sum_{n=0}^{\infty} (-1)^n \frac{\sin(2\pi(2n+1)x)}{(2n+1)^2} = \frac{8}{\pi^2}\, \rho^2 \chi_4 \odot \sin_{2\pi}(x),$$

where $\rho(n) = 1/n$, $\chi_4(n)$ is the nontrivial Dirichlet character modulo 4 (i.e., $\chi_4(m) = (-1)^{(m-1)/2}$ for odd m and $\chi_4(m) = 0$ for even m), and $\sin_{2\pi}$ denotes the function $\sin_{2\pi}(x) = \sin(2\pi x)$. Since $\rho^2\chi_4$ is completely multiplicative, its Dirichlet inverse is $(\rho^2\chi_4)^{-1} = \mu\rho^2\chi_4$, and hence the inversion formula gives

$$\sin(2\pi x) = \frac{\pi^2}{8} \sum_{n=1}^{\infty} \frac{\mu(n)\chi_4(n)}{n^2}\, T(nx).$$

Substituting rational values $x = k/m$ into this expansion yields interesting sums reminiscent of L-series. For example, with $m = 5$ and $x = 1/5$, we have

$$T(n/5) = \frac{2}{5} \times \begin{cases} 0, & \text{if } n \equiv 0 \pmod 5, \\ 2, & \text{if } n \equiv 1 \pmod 5, \\ 1, & \text{if } n \equiv 2 \pmod 5, \\ -1, & \text{if } n \equiv 3 \pmod 5, \\ -2, & \text{if } n \equiv 4 \pmod 5. \end{cases}$$

and since $\sin(2\pi/5) = \sqrt{(5+\sqrt{5})/8}$, we get

(3.23)

$$\frac{5\sqrt{2}\sqrt{5+\sqrt{5}}}{\pi^2} = \sum_{n=1}^{\infty} \frac{\mu(n)\beta(n)}{n^2}, \quad \beta(n) = \begin{cases} 0, & \text{if } \gcd(n, 20) > 1, \\ 2, & \text{if } n \equiv \pm 1 \pmod{20}, \\ 1, & \text{if } n \equiv \pm 3 \pmod{20}, \\ -1, & \text{if } n \equiv \pm 7 \pmod{20}, \\ -2, & \text{if } n \equiv \pm 9 \pmod{20}. \end{cases}$$

In fact these formulas are related to factorizations of the real parts of L-series (more details are given in [3]).

Example 17. (***Multiplication by arbitrary sequences***)**.** Transforms of the form $\sum_{n=1}^{\infty} f(a_n x)$ for essentially *arbitrary* sequences $\{a_n\}$ can be dealt with as Möbius inversion in the monoid of words over a countable alphabet. Since this takes us a little too far afield, we again refer the reader to [3] for more information.

References

[1] Apostol, T. M.: *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, 1976.

[2] Bazant, M.: Möbius, Chebyshev and Cesàro on Series Inversion (course notes). http://www-math.mit.edu/~bazant/teach/IAP99-mobius/mobius-1832.ps

[3] Benito, M., Navas, L. M., and Varona, J. L.: Möbius inversion formulas for flows of arithmetic semigroups. *J. Number Theory* **128** (2008), 390–412.

[4] Breitenfellner, H.: A unified Möbius inversion formula. *C. R. Math. Rep. Acad. Sci. Canada* **13** (1991), 39–42.

[5] Cesàro, E.: Sur l'inversion de certaines séries. *Ann. Mat. Pura Appl. (2)* **13** (1885), 339–351.

[6] Cesàro, E.: Fonctions énumératrices. *Ann. Mat. Pura Appl. (2)* **14** (1887), 141–158.

[7] Chebyshev, P. L.: Note sur différentes séries. *J. Math. Pures Appl. (1)* **16** (1851), 337–346.

[8] Chen, Z., Shen, Y., and Ding, J.: The Möbius inversion and Fourier coefficients. *Appl. Math. Comput.* **117** (2001), no. 2-3, 161–176.

[9] Ciaurri, Ó., Navas, L. M., and Varona, J. L.: A transform involving Chebyshev polynomials and its inversion formula. *J. Math. Anal. Appl.* **323** (2006), 57–62.

[10] Grosswald, E.: *Representations of integers as sums of squares*. Springer-Verlag, New York, 1985.

[11] Hardy, G. M., and Wright, E. M.: *An introduction to the theory of numbers*. Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[12] Knopfmacher, J.: *Abstract analytic number theory*. Second edition. Dover Books on Advanced Mathematics. Dover Publications, New York, 1990.

[13] Li Bo-Zang: A further generalization of the modified Möbius inversion formula. *Chinese Sci. Bull.* **37** (1992), 1220–1223.

[14] Möbius, A. F.: Über eine besondere art von umkehrung der reihen. *J. Reine Angew. Math.* **9** (1832), 105–123.

[15] Nathanson, M. B.: *Elementary methods in number theory*. Graduate Texts in Mathematics **195**. Springer-Verlag, New York, 2000.

[16] Ren, S. Y.: New Möbius inversion formulas. *Phys. Lett. A* **164 (1)** (1992), 1–5.

[17] Schroeder, M. R.: *Number theory in science and communication. With applications in cryptography, physics, digital information, computing and self-similarity*. Second edition. Springer Series in Information Sciences **7**. Springer-Verlag, Berlin, 1986.

Manuel Benito
Instituto Sagasta
Glorieta del Doctor Zubía s/n
26003 Logroño, Spain
mbenit8@palmera.pntic.mec.es

Luis M. Navas
Departamento de Matemáticas
Universidad de Salamanca
Plaza de la Merced 1-4
37008 Salamanca, Spain
navas@usal.es

Juan Luis Varona
Departamento de Matemáticas y Computación
Universidad de La Rioja
Calle Luis de Ulloa s/n
26004 Logroño, Spain
jvarona@dmc.unirioja.es

Research of the second author supported by grant SA30/00B of the JCyL, and research of the third author supported by grant MTM2006-13000-C03-03 of the DGI.