Reconstructing a signal from the knowledge of the norms of its multiples

by Bernard Beauzamy

Société de Calcul Mathématique SA
111 Faubourg Saint Honoré, 75008 Paris

february 1996

Abstract. – A periodic signal f is unknown and is not directly accessible. The only available data are the numbers $\|f.g\|$, for all polynomials g. Which norm $\|.\|$ should be chosen ? We show that if $\|.\|$ is the usual L_2-norm, reconstructing f is impossible but, if $\|.\|$ is Bombieri's norm, the reconstruction can be achieved. We describe the algorithm in detail and study its complexity.

`In application of contract ETCA/CREA/95.01.181, Ministry of Defense, France`

Let us consider a periodic signal f, which is unknown and not directly accessible to any measurement. The receiving device –the captor– gives only a scalar information (that is, in fact, a positive real). However, before treating f, we can perform on it multiplicative transformations, that is, for any g, explicit and known, we can measure fg. The question is : how can we reconstruct f ?

Practically speaking, we wish to compute only a finite number (finite but arbitrarily large) of Fourier coefficients of f, that is to determine the Fourier series of f, truncated at some specified order N : $\sum_{-N}^{N} a_j e^{ijt}$. Since we know that we can multiply by any multiple of e^{it}, we may therefore consider only analytic polynomials, that is assume from the very beginning that f has the form $\sum_0^n a_j e^{ijt}$.

Our question is thus : let f be a polynomial of degree n, with unknown coefficients. If we know the set

$$E_f \;=\; \{\|fg\| \;; g \text{ arbitrary polynomial }\} \tag{1}$$

can we reconstruct f ?

The norm $\|.\|$ can be any norm which makes sense on the space of polynomials. We will consider two of them here. First, the most natural and widely used : the L_2-norm, of which we show that it is inadequate, and then Bombieri's norm, of which we show that it allows the reconstruction of f.

For a polynomial $P = \sum_0^n c_j z^j$, we let

$$\|P\|_2 \;=\; (\sum |c_j|^2)^{1/2} \;=\; \left(\int_0^{2\pi} |P(e^{it})|^2 \,\frac{dt}{2\pi}\right)^{1/2}$$

be the usual norm on $L_2(\Pi)$.

Theorem 1. – *Assume we know the set*

$$E_f \;=\; \{\|fg\|_2 \;; g \text{ arbitrary polynomial}\} \tag{2}$$

then f can be reconstructed only within 3 ambiguities :

– taking the conjugate : f can be replaced by $\overline{f}$,

– multiplication by any function of modulus 1 on the unit circle,

– for each zero a, choosing between a and $-1/\overline{a}$, that is, each monomial $z-a$ cannot be distinguished from $\frac{1}{a}(1-\overline{a}z)$.

So we see that this procedure will not allow any distinction between (for instance) :

$$A(z-z_1)\cdots(z-z_n)$$

and

$$Az_1\cdots z_k(z-1/\overline{z}_1)\cdots(z-1/\overline{z}_k)(z-z_{k+1})\cdots(z-z_n).$$

Proof of Theorem 1. – If E_f is known, so is $\widetilde{E}_f$, defined by

$$\widetilde{E}_f \;=\; \{\|fg\|_2 \;; g \in L_2(\Pi)\}, \tag{3}$$

since trigonometric polynomials are dense in $L_2(\Pi)$.

Let a, $0 \leq a < 2\pi$, and $\varepsilon > 0$, and let us consider the function $g = g_{a,\varepsilon}$ defined by

$$\begin{aligned} g_{a,\varepsilon}(e^{it}) &= 1/\sqrt{2\varepsilon} \ \text{ if } \ |t-a| < \varepsilon, \\ &= 0 \qquad \text{otherwise.} \end{aligned}$$

We have :

$$\begin{aligned} \left(\int_{-\pi}^{\pi} |f(e^{it})|^2 |g_a(e^{it})|^2 \frac{dt}{2\pi}\right)^{1/2} &= \left(\frac{1}{2\varepsilon}\int_{a-\varepsilon}^{a+\varepsilon} |f(e^{it})|^2 \frac{dt}{2\pi}\right)^{1/2} \\ &\to |f(e^{ia})|, \quad \text{when } \ \varepsilon \to 0, \end{aligned}$$

and so we know the set of values $|f(z)|$, $|z| = 1$, that is the function $\varphi(z) = |f(z)|$, $|z| = 1$.

Therefore, we can reconstruct the *outer part* of f, in its decomposition in the Hardy space H^2, by the standard formula :

$$F(z) \ = \ \exp \int_{-\pi}^{\pi} \frac{e^{it}+z}{e^{it}-z} \log(\varphi(e^{it})) \ \frac{dt}{2\pi},$$

and we know that $|F(e^{it})| = \varphi(e^{it}) = |f(e^{it})|$ for every t. If f is a polynomial, F is also a polynomial, of the same degree, with no zero inside the open unit disk D. If f has no zero in D, $F = f$. If f has one root or several roots in D, F is obtained by reflection of these roots : if $f = (z-z_1)\cdots(z-z_n)$, with $|z_1| \leq 1, \ldots, |z_k| \leq 1$, then

$$F \ = \ (1-\overline{z}_1 z)\cdots(1-\overline{z}_k z)(z-z_{k+1})\cdots(z-z_n).$$

This proves the theorem.

Remark. – The ambiguities in the reconstruction of f come from the obvious fact that the tool we use –namely the L_2-norm–, employs only the values of f on the unit circle, and that $|z-a| = |1-\overline{a}z|$ if $|z| = 1$. If we had taken f in H^2 (not just a polynomial), we would get a similar result : we can reconstruct the outer part of f ; we have no information on its inner part m (Blaschke factor and singular part), since it satisfies $|m(z)| = 1$, $|z| = 1$.

We now study the same question, but this time using Bombieri's norm. We will see that the result is now satisfactory : reconstructing f is possible, up to the multiplication by a complex number of modulus 1, of course.

The proper frame will be here that of homogeneous polynomials in many-variables (as in Beauzamy-Bombieri-Enflo-Montgomery [1] and Beauzamy-Dégot [2]). The case of an ordinary one-variable polynomial $\sum_0^n a_j z^j$ is deduced from the homogeneous two-variable $\sum_0^n a_j z^j z'^{n-j}$, just by taking $z' = 1$.

So let

$$P(x_1, \ldots, x_N) \ = \ \sum_{|\alpha|=n} a_\alpha \ x_1^{\alpha_1} \cdots x_N^{\alpha_N}$$

be a homogeneous polynomial in N variables, with degree n.

We have $|\alpha| = \alpha_1 + \cdots + \alpha_N$. Bombieri's norm, which depends on the degree, is defined by the expression :

$$[P] \ = \ \left(\sum_{|\alpha|=m} \frac{|a_\alpha|^2 \alpha!}{m!}\right)^{1/2} \tag{4}$$

where $\alpha! = \alpha_1! \cdots \alpha_N!$. The reader is referred to Beauzamy–Dégot [2] and Reznick [3] for the basic properties of this norm.

Theorem 2. – *Let P be a homogeneous polynomial in N variables, with degree n, and unknown coefficients. If we know the set*

$$F_P \;=\; \{[PQ]\;;\varphi \;\text{ homogeneous polynomial in N variables, with degree } \leq \text{n}\}, \tag{5}$$

we can reconstruct P, up to the multiplication by a complex scalar of modulus 1.

Proof of Theorem 2. – The proof we give now follows the lines indicated by the referee : it is shorter than the one we originally gave.

First, from the knowledge of (5), we deduce, by the usual polarization formulas, the knowledge of all the scalar products

$$A_k(\alpha,\beta) \;=\; [x_1^{\alpha_1}\cdots x_N^{\alpha_N}P, \quad x_1^{\beta_1}\cdots x_N^{\beta_N}P] \tag{6}$$

for all $k \leq n$ and all α, β, with $|\alpha| = |\beta| = k$.

Indeed, each scalar product (6) can be computed from the four numbers

$$\big[(x_1^{\alpha_1}\cdots x_N^{\alpha_N} \;\pm\; x_1^{\beta_1}\cdots x_N^{\beta_N})P\big], \quad \big[(x_1^{\alpha_1}\cdots x_N^{\alpha_N} \;\pm\; i\; x_1^{\beta_1}\cdots x_N^{\beta_N})P\big]. \tag{7}$$

We observe, at this stage, that we won't use all the set (5), but only the scalar products (6), so we need only the quantities (7) : there are $4\binom{N+m-1}{m}$ such numbers.

Now, from the numbers (6), we will deduce the knowledge of all the numbers

$$B_k(\alpha,\beta) \;=\; [P, x_1^{\beta_1}\cdots x_N^{\beta_N}D^\alpha P] \tag{8}$$

for all $k \leq n$, all α, β, with $|\alpha| = |\beta| = k$.

Indeed, for $k = 1$, we have (see [2])

$$\begin{aligned}[x_iP, x_jP] \;&=\; \frac{1}{n+1}\;[P, \frac{\partial}{\partial x_i}\;(x_jP)]\\ &=\; \frac{1}{n+1}\;[P, \frac{\partial x_j}{\partial x_i}P] + \frac{1}{n+1}\;[P, x_j\;\frac{\partial P}{\partial x_i}]\end{aligned}$$

and so

$$[P, x_j\frac{\partial P}{\partial x_i}] \;=\; (n+1)[x_iP, x_jP] - \delta_{ij}[P,P],$$

where $\delta_{ij} = 0$ if $i \neq j$, $= 1$ if $i = j$.

So we have the formula

$$[P, x_1^{\beta_1}\cdots x_N^{\beta_N}D^\alpha P] \;=\; (n+1)[x_1^{\alpha_1}\cdots x_N^{\alpha_N}P, x_1^{\beta_1}\cdots x_N^{\beta_N}P] - \delta_{\alpha,\beta}\;[P,P]$$

or

$$B_1(\alpha,\beta) \;=\; (n+1)\;A_1(\alpha,\beta) - \delta_{\alpha,\beta}\;A_0(\alpha,\beta).$$

Now, assume $B_1(\alpha,\beta),\ldots,B_{k-1}(\alpha,\beta)$ can be computed from $A_0(\alpha,\beta),\ldots,A_{k-1}(\alpha,\beta)$. We compute the numbers $B_k(\alpha,\beta)$, where $|\alpha| = |\beta| = k$. Take any coordinate $\alpha_j \geq 1$, say for instance $\alpha_1 \geq 1$. Then, as before :

$$\begin{aligned}[x_1^{\alpha_1}\cdots x_N^{\alpha_N}P,\; x_1^{\beta_1}\cdots x_N^{\beta_N}P] \;&=\; \frac{1}{n+k}[x_1^{\alpha_1-1}x_2^{\alpha_2}\cdots x_N^{\alpha_N}P,\; \beta_1x_1^{\beta_1-1}x_2^{\beta_2}\cdots x_N^{\beta_N}P]\\ &+\; \frac{1}{n+k}[x_1^{\alpha_1-1}x_2^{\alpha_2}\cdots x_N^{\alpha_N}P, x_1^{\beta_1}\cdots x_N^{\beta_N}D_1P],\end{aligned}$$

and so

$$[x_1^{\alpha_1-1}x_2^{\alpha_2}\cdots x_N^{\alpha_N}P,\ x_1^{\beta_1}\cdots x_N^{\beta_N}D_1P] \ =$$
$$(n+k)\ A_k(\alpha,\beta)-\beta_1\ A_{k-1}(\alpha_1-1,\alpha_2,\ldots,\alpha_N\ ;\ \beta_1-1,\beta_2,\ldots,\beta_N),$$

from which one deduces all the numbers

$$[x_1^{\alpha_1-1}x_2^{\alpha_2}\cdots x_N^{\alpha_N}P,\ x_1^{\beta_1}\cdots x_N^{\beta_N}D_1P] \tag{9}$$

for all $\alpha,\ \beta,\ |\alpha|=|\beta|=k$. From these numbers one deduces as before the numbers

$$[x_1^{\alpha_1-2}x_2^{\alpha_2}\cdots x_N^{\alpha_N}P, x_1^{\beta_1}\cdots x_N^{\beta_N}D_1^2\ P],$$

and so on, until all derivatives are transferred to the right-hand side, and we get $B_k(\alpha,\beta)$.

Remark. The computation of $B_k(\alpha,\beta)$ can be made more explicit, using the differential identity proved in [2] (Theorem 12). Indeed, with the present notation, this theorem gives, if $|\alpha|=|\beta|=m$, degree $P=n$:

$$[x_1^{\alpha_1}\cdots x_N^{\alpha_N}P,\ x_1^{\beta_1}\cdots x_N^{\beta_N}P] \ =$$
$$\frac{1}{(m+n)!}\sum_{k\geq 0}(n-m+k)!\sum_{|\gamma|=k}\frac{\alpha!\beta!}{(\alpha-\gamma)!(\beta-\gamma)!\gamma!}\ [D^{\beta-\gamma}P,\ D^{\alpha-\gamma}P]\cdot$$

The term with $k=0$ in the right-hand side gives $[D^\beta P, D^\alpha P]$, that is $[P, x_1^{\beta_1}\cdots x_N^{\beta_N}D^\alpha P]$, and the terms for $k\geq 1$ correspond to $B_j(\alpha,\beta)$, with $j<m$.

When all the $B_k(\alpha,\beta),\ k\leq n$ are known, let us take $|\alpha|=|\beta|=n$. We have

$$B_n(\alpha,\beta) \ = \ [P, x_1^{\beta_1}\cdots x_N^{\beta_N}D^\alpha P] \ = \ \frac{1}{n!}\ [D^\beta P, D^\alpha P] \ = \ \frac{\alpha!\beta!}{n!}\ \overline{a_\alpha}\ a_\beta. \tag{10}$$

So we know all the numbers $\overline{a_\alpha}a_\beta$. Taking for instance $\alpha=(1,0,\ldots,0)$ and $\beta=\alpha$, we get $|a_{1,0,\ldots,0}|^2$ (or any other term if this one is zero), so $a_{1,0,\ldots,0}$ is known up to a complex factor of modulus 1. All other coefficients a_β are then deduced from (10). This finishes the proof of Theorem 2.

Remark. Pratical computation of Bombieri's norm $[P]$, for a homogeneous polynomial P of degree n in N variables, can be made in two ways :

– from the coefficients of the polynomials, using the definition (4), if these coefficients are known,

– from the values of $P(z)$ inside the unit disk, using an integral formula, such as Boyd's :

$$[P] \ = \ \frac{n+1}{\pi}\int_0^{2\pi}\int_0^{\infty}\frac{|P(re^{i\theta})|^2}{(1+r^2)^{n+2}}\ rdrd\theta.$$

References

[1] B. Beauzamy, E. Bombieri, P. Enflo, H. Montgomery : Products of polynomials in many variables. *Journal of Number Theory*, vol. 36, 2, oct. 1990, 219–245.

[2] B. Beauzamy, J. Dégot : Differential identities, *Transactions of the A.M.S.*, vol. 347, no 7, July 1995, pp. 2607-2619.

[3] Reznick, Bruce : An inequality for products of polynomials. *Proceedings A.M.S.*, vol. 117, 4, 1993, pp. 1063–1073.