Pompeiu's problem on discrete space
(partial difference equations/Hilbert's Nullstellensatz/three squares theorem)

Doron Zeilberger*

The Institute for Advanced Study, Princeton, New Jersey 08540
Communicated by Richard J. Duffin, April 24, 1978

ABSTRACT Let \( \mathcal{S} \) be a finite family of finite subsets of the \( n \)-dimensional lattice \( \mathbb{Z}^n \), and let \( \mathcal{T} \) denote the group of all translations of \( \mathbb{Z}^n \). We shall here consider the Pompeiu problem for the family \( \mathcal{S} \)—namely, to determine when the only function \( f: \mathbb{Z}^n \rightarrow \mathbb{C} \) such that

\[
\sum_{m \in \mathcal{T} \cap \mathcal{S}} f(m) = 0
\]

is the zero function. We would like to formulate the discrete analog of the Pompeiu problem. The discrete counterpart of \( \mathbb{R}^n \) is the \( n \)-dimensional lattice \( \mathbb{Z}^n \), and a subset of \( \mathbb{Z}^n \) is compact iff it is finite. Because there is no notion of continuity in \( \mathbb{Z}^n \), the discrete Pompeiu problem can be stated as follows: Let \( \mathcal{S} \) be a family of finite subsets of the \( n \)-dimensional lattice \( \mathbb{Z}^n \) and let \( \mathcal{T} \) denote the group of all translations on \( \mathbb{Z}^n \). Give necessary and sufficient conditions on the family \( \mathcal{S} \) such that

\[
\sum_{m \in \mathcal{T} \cap \mathcal{S}} f(m) = 0 \quad \text{for all } \mathcal{T}, \mathcal{S} \in \mathcal{S} \quad \text{iff } f \equiv 0. \tag{1}
\]

Note that the system (1) is a system of partial difference equations with constant coefficients. In fact, every finite set \( S \) in \( \mathbb{Z}^n \) defines a partial difference operator \( \mathcal{P}_S f(m) = \sum_{m \in S} f(m + s) \) and system (1) can be written \( \mathcal{P}_S f = 0 \) for every \( S \in \mathcal{S} \).

In the next section we shall consider general systems of partial difference equations with constant coefficients.

2. Systems of partial difference equations with constant coefficients

Let \( \mathcal{F}(\mathbb{Z}^n) \) be the set of complex valued functions on \( \mathbb{Z}^n \); a partial difference operator is a mapping \( \mathcal{F}(\mathbb{Z}^n) \rightarrow \mathcal{F}(\mathbb{Z}^n) \) of the form

\[
\mathcal{P}(m) = \sum_{|\alpha| \leq N} C_\alpha f(m + \alpha), \tag{2}
\]

where \( N \) is an integer, \( C_\alpha \) are some complex constants, \( m = (m_1, \ldots, m_n) \), \( \alpha = (\alpha_1, \ldots, \alpha_n) \) are elements of \( \mathbb{Z}^n \), and \( |\alpha| = \sum_{i=1}^n |\alpha_i| \). The most simple nontrivial partial difference operators are the shifts:

\[
X_i f(m) = f(m + e_i), \quad i = 1, \ldots, n,
\]

where \( e_i = (0, \ldots, 1, 0, \ldots, 0) \) and the 1 is in the \( i \)th place. Writing \( X^a = X_1^{a_1} \cdots X_n^{a_n} \) we get \( X^a f(m) = f(m + \alpha), \alpha \in \mathbb{Z}^n \). Thus, [2] can be written

\[
\mathcal{P}(m) = \sum_{|\alpha| \leq N} C_\alpha f(m + \alpha) = \sum_{|\alpha| \leq N} C_\alpha X^\alpha f(m).
\]

Hence, \( \mathcal{P} = P(X) \), where \( P \) is a polynomial in \( z_1, z_1^{-1}, \ldots, z_n, z_n^{-1} \) i.e., an element of \( \mathcal{A}_n = \mathbb{C}[z_1, z_1^{-1}, \ldots, z_n, z_n^{-1}] \), the space, of trigonometric polynomials. Conversely, given a polynomial \( P, P(X) \) is a partial difference operator. We shall now define an isomorphism between \( \mathcal{F}(\mathbb{Z}^n) \) and \( \mathcal{A}_n \), the dual of \( \mathcal{A}_n \).

For every \( f: \mathbb{Z}^n \rightarrow \mathbb{C} \) define \( f: \mathcal{A}_n \rightarrow \mathbb{C} \) by

\[
\hat{f} \left( \sum_{k \in \mathbb{Z}^n} a_k z^k \right) = \sum a_k f(k).
\]

In particular \( \hat{f}(z^m) = f(m) \). Conversely, given a linear functional \( \mathcal{L} \) on \( \mathcal{A}_n \), then \( \mathcal{L}(m) = f(m) \) is a function on \( \mathbb{Z}^n \) and \( T = \mathcal{L} \). Thus, \( f \rightarrow \mathcal{L} \) is a linear isomorphism between \( \mathcal{F}(\mathbb{Z}^n) \) and \( \mathcal{A}_n \). We shall see that this simple correspondence is very useful. Let \( P(z) = \sum_{|\alpha| \leq N} C_\alpha z^\alpha \) and suppose that \( P(X)f = 0 \), then for every \( m \in \mathbb{Z}^n \)

\[
0 = P(f)(m) = \sum_{|\alpha| \leq N} C_\alpha f(m + \alpha) = \sum_{|\alpha| \leq N} C_\alpha \hat{f}(z^m + \alpha) = \hat{f} \left( \sum_{|\alpha| \leq N} C_\alpha z^m + \alpha \right) = \hat{f}(z^m P(z)).
\]

Because \( z^m \) form a basis of \( \mathcal{A}_n \), we get \( \hat{f}(P(z)u(z)) = 0 \) for every \( u \in \mathcal{A}_n \) iff \( P(X)f = 0 \)—that is, \( P(X)f \equiv 0 \) iff \( \hat{f} \) annihilates the ideal \( P(z)\mathcal{A}_n \). At this stage we can prove our main result.

Theorem 1. Let \( P_1, \ldots, P_N \) be polynomials in \( \mathcal{A}_n \). Then

\[
P_1(X)f = 0 \quad \text{iff} \quad P_1(z)P_2(z) \cdots P_N(z) \text{ have no common zeros in } \mathbb{Z}^n.
\]

Proof: The assumption about \( f \) implies that \( \hat{f} \) annihilates \( P_1(z)P_2(z) \cdots P_N(z) \). Because the variety of common zeros of \( I \) is empty, it follows from Hilbert's Nullstellensatz (ref. 3, p. 157) that the radical of \( I \) is \( \mathcal{A}_n \). But this implies \( I = \mathcal{A}_n \)—i.e., \( f \) is identically zero and consequently \( f \equiv 0 \).

Conversely, suppose that \( |P_1(z)|, \ldots, |P_N(z)| \) do have a common zero in \( \mathbb{C}^n \). Then there exists a \( z_0 \in \mathbb{C}^n \) such that \( P_i(z_0) = 0, i = 1, \ldots, N \). Then \( f(z_0) = z_0^m \) is a nontrivial solution, because \( P_i(X)z_0^m = P_i(z_0)z_0^m = 0, i = 1, \ldots, N \).

3. Solution of Pompeiu's problem

Theorem 1 immediately implies the solution of Pompeiu's problem.

Theorem 2. For \( S \) a finite subset of \( \mathbb{Z}^n \) let \( P_S(z) = \sum_{z \in S} z \). Then \( \sum_{m \in \mathcal{T}(S)} f(m) = 0 \) for every \( S \in \mathcal{S}, \mathcal{T} \) iff the polynomials \( \{P_S, S \in \mathcal{S}\} \) have no common zeros in \( \mathbb{C}^n \).

* Current address: Georgia Institute of Technology, Atlanta, GA 30332.
The following is a discrete analog of Theorem 1 in ref. 1. 

**COROLLARY.** In $\mathbb{Z}^2$ let $\mathcal{S}$ be the family consisting of three squares of sides $M$, $N$, and $K$. Then $f = 0$ is the only solution of system 1 iff $M + 1$, $N + 1$, $K + 1$ are pairwise relatively prime.

**Proof:** Let $S_M$, $S_N$, and $S_K$ be the squares of sides $M$, $N$, and $K$, respectively. Then

$$P_{S_M} = \sum_{m_1=0}^{M} \sum_{m_2=0}^{M} z_1^{m_1} z_2^{m_2}$$

$$= (z_1^{M+1} - 1)/(z_1 - 1)(z_2 - 1).$$

Similarly, $P_{S_K}(z_1, z_2) = (z_1^{K+1} - 1)/(z_1 - 1)(z_2 - 1)$, $P_{S_N}(z_1, z_2) = (z_1^{N+1} - 1)/(z_1 - 1)(z_2 - 1)$. Because

$(z^r - 1)/(z - 1)$, $(z^l - 1)/(z - 1)$ have no common zeros iff $r$ and $l$ are relatively prime, the statement follows from Theorem 1.

This work was supported by Grant MCS77-18723 from the National Science Foundation.