Functional Equations with Permutations of Finite Order

Axel Tong (4H1), Chow Guan Ze (4S1), He Donghang (4S1), Tey Yi Fan (4S1)
Group 8-07
Project Work 2020

Abstract

Given a functional equation of the form $f + f\pi + \cdots + f\pi^{k-1} = g$ where π is a permutation of the underlying set S and g is a given map from S into a commutative ring with unity, we determine necessary and sufficient criteria for the existence of a unique solution for f, and find an explicit expression for the solution. When no unique solution exists, we consider conditions for the existence of a solution, and determine the number of solutions in that case. We discuss suitable generalisations of the solution method, and the extent to which our method applies.

1. Introduction. Let n and k be positive integers such that $k \leq n$. Let R be a commutative ring with unity, and let S be an arbitrary set. Let $\pi : S \to S$ be a bijection of order n (that is, n is the smallest positive integer for which $\pi^n(x) = x$ for all $x \in S$), and let $f, g : S \to R$ be functions satisfying

$$f(x) + f(\pi(x)) + \cdots + f(\pi^{k-1}(x)) = g(x) \tag{1}$$

for all $x \in S$. It is natural to ask for conditions on π, g, n, k so that we can guarantee the existence and uniqueness of such a function f satisfying (1), as well as how we can describe f in the case where it exists.

We will discuss the following three research questions.

1. Under what conditions does (1) have a unique solution, and what is the explicit expression for f?
2. When (1) does not have a unique solution, what are the conditions for the existence of a solution? In this case, what is the size of the solution set?
3. To what extent can we generalise the results of the previous two research questions?

2. Existence and uniqueness of a solution. Let Id be the identity operator on S. In the space of functions $S \to R$, we define addition by $(f+g)(x) = f(x) + g(x)$ for all $x \in S$, and multiplication by functional composition, with $(fg)(x) = f(g(x))$ for all $x \in S$. Then (1) is equivalent to the following equality:

$$f + f\pi + \cdots + f\pi^{k-1} = g.$$

From this, it is evident that right multiplication $n-1$ times by π gives us n distinct equations of the form

$$f\pi^r + f\pi^{r+1} + \cdots + f\pi^{r+k-1} = g\pi^r,$$

for $0 \leq r \leq n-1$, and since $\pi^n = \mathrm{Id}$ by hypothesis, this gives rise to a $n \times n$ linear system in $\{f, f\pi, \ldots, f\pi^{n-1}\}$. In particular, we have the matrix equation

$$\mathcal{M}(n,k) f\Pi = g\Pi, \tag{2}$$

where $\Pi := [\mathrm{Id}, \pi, \ldots, \pi^{n-1}]^T$ and $\mathcal{M}(n,k)$ is defined by

$$[\mathcal{M}(n,k)]_{ij} = \begin{cases} 1 & \text{if } j \equiv i + a \bmod n \text{ for } a \in \{0, 1, \ldots, k-1\} \\ 0 & \text{otherwise.} \end{cases}$$

If $\mathcal{M}$ is invertible, then (2) implies that

$$f\Pi = \mathcal{M}(n,k)^{-1} g\Pi. \tag{3}$$

Now, we recall the following well-known fact, for which a proof can be found in [1].

Proposition 2.1 (Cramer's Rule)**.** *Let M be a $n \times n$ invertible matrix with entries in a commutative ring R with unity. Then the inverse matrix is given by*

$$M^{-1} = (\det M)^{-1} \operatorname{cof}(M)^T,$$

where cof *denotes the cofactor matrix.*

Taking the first entry of both sides in (3) and applying Cramer's rule proves the following result at once, where the c_i are obtained as the cofactors corresponding to the ith entry along the first column of $\mathcal{M}(n,k)$.

Theorem 2.2. *For a commutative ring with unity R, the equation* (1) *has a unique solution for f if and only if* $\det \mathcal{M}(n,k) \in R$ *is a unit, in which case we have*

$$f(x) = (\det \mathcal{M}(n,k))^{-1} \sum_{i=1}^{n} c_i g(\pi^i(x)).$$

Now, we specialise to the case where R is a subfield of $\mathbb{C}$ in order to apply some tools of linear algebra. We start by noting that $\mathcal{M}(n,k)$ is a circulant matrix where the first row is $[\underbrace{1, 1, \ldots, 1}_{k \text{ 1's}}, \underbrace{0, \ldots, 0}_{n-k \text{ 0's}}]$ and every other row is given by a cyclic permutation of the first. Hence, we can apply the following property of circulant matrices.

Lemma 2.3. *Let K be a subfield of $\mathbb{C}$, and let $C \in M_n(K)$ be a circulant matrix defined by*

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \dots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \dots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \dots & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \dots & c_0 \end{bmatrix}$$

where $c_i \in K$ for each $i = 0, 1, \dots, n-1$. Let $p(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. Then

$$\det C = \prod_{j=0}^{n-1} p(\omega_n^j),$$

where $\omega_n := \exp(2\pi i/n)$ is a primitive nth root of unity.

Proof. This is a well-known result. A proof can be found as an immediate consequence of the explicit formula for eigenvalues on page 73 of [2]. □

The polynomial $p(x)$ which appears in the statement of Lemma 2.3 is called the *associated polynomial* of the circulant matrix C. Thus, a circulant matrix C is singular if and only if its determinant $\det C$ is zero, which occurs exactly when ω_n^j is a zero of its associated polynomial p for some $j \in \{0, 1, \dots, n-1\}$.

From the definition, it is clear that the associated polynomial of $\mathcal{M}(n, k)$ is given by $p(x) = 1 + x + \cdots + x^{k-1} = (x^k - 1)/(x - 1)$. Thus, the zeroes of $p(x)$ are exactly the kth roots of unity other than 1. Clearly, there exists a nth root of unity other than 1 which is also a kth root of unity if and only if n and k share a nontrivial common factor. Thus, $\mathcal{M}(n, k)$ is invertible if and only if $\gcd(n, k) = 1$.

In fact, we can explicitly determine the determinant of $\mathcal{M}(n, k)$ in the case where it is invertible. We have the following result.

Theorem 2.4. *The determinant of $\mathcal{M}(n, k)$ is given by*

$$\det \mathcal{M}(n, k) = \begin{cases} k, & \gcd(n, k) = 1, \\ 0, & \gcd(n, k) > 1. \end{cases}$$

Proof. The matrices $\mathcal{M}(n, k)$ are circulant, with associated polynomial $p(x) = 1 + x + \cdots + x^{k-1}$. Note that whenever $x \neq 1$, we have $p(x) = (x^k - 1)/(x - 1)$, so we may write

$$\det \mathcal{M}(n, k) = \prod_{j=0}^{n-1} p(\omega_n^j) = p(1) \prod_{j=1}^{n-1} \frac{\omega_n^{jk} - 1}{\omega_n^j - 1}.$$

In the case where $\gcd(n, k) =: d > 1$, we know that ω_n^k is no longer a primitive nth root of unity, but it is a primitve (n/d)th root of unity. Since $d > 1$, the integer n/d lies in the set

$\{1, 2, \ldots, n-1\}$ from which j takes values in the product, so there is a term in the product where $j = n/d$. For this term, the numerator is $\omega_n^{jk} - 1 = \omega_{n/d}^{n/d} - 1 = 0$, so that the whole product is 0 and the determiant is 0.

It is trivial that $p(1) = k$, so it suffices to show the product $\prod(\omega_n^{jk} - 1)/(\omega_n^j - 1)$ is 1 to show the case when $\gcd(n, k) = 1$. The reason this is true is because of cancellation. The element k in the additive group $\mathbb{Z}/n\mathbb{Z}$ (which is isomorphic to the multiplicative group of roots of unity) always generates the group whenever n, k are coprime. Furthermore, each element is generated in a unique way. Therefore, as j takes all nonzero values in $\mathbb{Z}/n\mathbb{Z}$, every element is represented exactly once, so the cancellation is perfect, proving the result. □

Our main result follows from this and Theorem 2.2.

Theorem 2.5. *The equation* (1) *has a unique solution for f if and only if* $\gcd(n, k) = 1$*, in which case we have*

$$f(x) = \frac{1}{k} \sum_{i=1}^{n} c_i g(\pi^i(x)). \quad \square$$

The values of the constants c_i can be determined in any particular case by explicitly computing the cofactors of the relevant matrix $\mathcal{M}(n, k)$. We do not know of a closed form expression for these constants in the general case.

3. Non-unique solutions. In the case where R is a subfield of $\mathbb{C}$, we have shown that (1) does not have a unique solution when $\gcd(n, k) > 1$. For any fixed $x \in S$, the matrix form (2) implies

$$\mathcal{M}(n, k)(f\Pi)_x = (g\Pi)_x, \tag{4}$$

where $(\cdot)_x$ denotes the evaluation at x. Thus, there exists a solution exactly when $(g\Pi)_x$ lies in the column space of $\mathcal{M}(n, k) \subseteq R^n$ for each $x \in S$. If there exists a particular solution f_0 to (2), then the general solution to this equation is given by

$$(f\Pi)_x = (f_0\Pi)_x + r,$$

for any $r \in \ker \mathcal{M}(n, k)$, so that there are $|\ker \mathcal{M}(n, k)|$ solutions. Thus, there are $|\ker \mathcal{M}(n, k)|^{|S|}$ solutions for f by considering each value of x. In particular, since R is not a finite field (as such fields cannot be embedded in $\mathbb{C}$), then there are infinitely many solutions.

Theorem 3.1. *When R is a subfield of $\mathbb{C}$, the equation* (1) *has either no solution, a unique solution, or infinitely many solutions.*

4. Generalisations. We have obtained complete results in the case where R is a subfield of $\mathbb{C}$. It is worth noting that precise conditions on when a field R can be embedded into $\mathbb{C}$ can be established. We have the following result [3].

Proposition 4.1. *Let K be a field which does not embed into $\mathbb{C}$. Then, either*

1. $|K| > |\mathbb{C}| = \mathfrak{c}$, *or*
2. $\operatorname{char} K > 0$. □

Thus, any field of characteristic 0 which is "not too large" can be embedded into $\mathbb{C}$, so that Theorem 2.5 holds for most fields one cares to consider. In the general case where R is a commutative ring with unity, Theorem 2.2 holds. However, no analogue of Theorem 2.4 can be obtained as the proof of Lemma 2.3 uses properties of polynomials in $\mathbb{C}[x]$, so this is the best result that can be proven.

If R is a commutative ring without unity, noncommutative ring or even an additive group, the original equation (1) still makes sense, but no useful results may be obtained as the matrix form (2) cannot even be obtained, as matrix multiplication by $\mathcal{M}(n,k)$ is not sensible. Thus even analogues of Theorem 2.2 cannot be obtained.

5. Further Extensions. This project has left several questions unanswered. Firstly, does there exist a closed form expression for the constants c_i appearing in 2.5 for general n, k? Numerical testing suggests a periodic pattern in these constants, but their general form remains elusive. Secondly, does there exist a general form of $\det \mathcal{M}(n,k)$ in the case where R is a field of positive characteristic? Combined with Theorem 2.2, this would obtain an analogue of Theorem 2.5 and solve the problem for the case of fields of positive characteristic, which remains unresolved.

Acknowledgements. The authors would like to thank Dr. Ang Lai Chiang for his mentorship and valuable guidance throughout the course of the project.

References

[1] Brunetti, M. (2014). Old and New Proofs of Cramer's Rule. *Applied Mathematical Sciences, 8*, no. 133, 6689-6697. doi:10.12988/ams.2014.49683

[2] Davis, P. J. (1979). *Circulant Matrices.* Wiley, New York. (ISBN 13: 9780471057710, ISBN 10: 0471057711)

[3] Wofsey, E. (2015, October 5). *A field of characteristic zero can be embedded into $\mathbb{C}$?* Mathematics Stack Exchange. Retrieved 16 August, 2020, from https://math.stackexchange.com/q/1464736/