Ramanujan Sums in the Context of Signal Processing—Part I: Fundamentals

P. P. Vaidyanathan, *Fellow, IEEE*

Dedicated to the memory of Srinivasa Ramanujan

***Abstract*—The famous mathematician S. Ramanujan introduced a summation in 1918, now known as the Ramanujan sum $c_q(n)$. For any fixed integer q, this is a sequence in n with periodicity q. Ramanujan showed that many standard arithmetic functions in the theory of numbers, such as Euler's totient function $\phi(n)$ and the Möbius function $\mu(n)$, can be expressed as linear combinations of $c_q(n), 1 \leq q \leq \infty$. In the last ten years, Ramanujan sums have aroused some interest in signal processing. There is evidence that these sums can be used to extract periodic components in discrete-time signals. The purpose of this paper and the companion paper (Part II) is to develop this theory in detail. After a brief review of the properties of Ramanujan sums, the paper introduces a subspace called the Ramanujan subspace $\mathcal{S}_q$ and studies its properties in detail. For fixed q, the subspace $\mathcal{S}_q$ includes an entire family of signals with properties similar to $c_q(n)$. These subspaces have a simple integer basis defined in terms of the Ramanujan sum $c_q(n)$ and its circular shifts. The projection of arbitrary signals onto these subspaces can be calculated using only integer operations. Linear combinations of signals belonging to two or more such subspaces follows certain specific periodicity patterns, which makes it easy to identify periods. In the companion paper (Part II), it is shown that arbitrary finite duration signals can be decomposed into a finite sum of orthogonal projections onto Ramanujan subspaces.**

***Index Terms*—Periodic components, periodic subspaces, Ramanujan subspaces, Ramanujan sums.**

I. INTRODUCTION

IN 1918 the famous Indian mathematician Srinivasa Ramanujan introduced a trigonometric summation, now called the Ramanujan sum. This sum has the form [13]

$$c_q(n) = \sum_{\substack{k=1 \\ (k,q)=1}}^{q} e^{j2\pi kn/q} \tag{1}$$

Here the notation (k, q) denotes the greatest common divisor (gcd) of k and q. Thus $(k, q) = 1$ means that k and q are coprime. For example if $q = 10$, the coprime values of k are $k = 1, 3, 7$, and 9 so that

$$c_{10}(n) = e^{j2\pi n/10} + e^{j6\pi n/10} + e^{j14\pi n/10} + e^{j18\pi n/10}.$$

Ramanujan's motivation in introducing this sum was to show that several standard arithmetic functions in the theory of numbers can be expressed as linear combinations of $c_q(n)$, that is,

$$x(n) = \sum_{q=1}^{\infty} \alpha_q c_q(n), \quad n \geq 1. \tag{2}$$

An arithmetic function is an infinite sequence defined for $1 \leq n \leq \infty$, and is usually (but not necessarily) integer valued. Examples include the Möbius function $\mu(n)$, Euler's totient function $\phi(n)$, the von Mangoldt function $\Lambda(n)$, and the Riemann-zeta function $\zeta(s)$[6]. The Ramanujan expansion (2) was derived in [13] for many arithmetic functions.

Interesting applications of Ramanujan sums in the context of signal processing have been examined by a number of authors [3], [8], [10]–[12], [14], [17]. Equation (2) is sometimes referred to as the *Ramanujan Fourier transform* expansion (i.e., α_q are the RFT coefficients) [12]. Applications in the representation of periodic signals was demonstrated by Planat (e.g., see [12]). Time-frequency analysis of signals based on Ramanujan expansions was considered in a letter by Sugavaneswaran [17], based on the 2D version of Ramanujan sums. An application in cardiology was described in [8]. A very insightful connection between Ramanujan sums and the proof of the famous *twin-prime conjecture* was established by Gadiyar and Padma in [4] based on the possibility of a Wiener-Kintchine like formula for Ramanujan expansions. The conjecture itself has been proved recently by Yitang Zhang in a famous paper [22].

The Ramanujan sum (1) has period q in the argument n. Unlike sines and cosines, the quantity $c_q(n)$ is always *integer valued* (Section III), which is often an attractive property. Understandably, therefore, this has inspired signal processing researchers to use an expansion of the form (2) to look for periodic components in a signal $x(n)$. However, since each term $c_q(n)$ in (2) is only one of many possible period-q signals (including, for example, sines and cosines), there is no evidence that this representation is always the most appropriate. In fact we will see that a direct use of (2) for finite duration signals is not satisfactory for many reasons. Also, unlike in the case of infinite-duration arithmetic-sequences, the components in (2) lose orthogonality in the finite duration case.

Manuscript received January 10, 2014; revised April 20, 2014; accepted April 21, 2014. Date of publication June 18, 2014; date of current version July 18, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Hing Cheung So. This work was supported in parts by the ONR grant N00014-11-1-0676, and the Information Science and Technology (IST) initiative of the California Institute of Technology.

The author is with the Department of Electrical Engineering, 136-93, California Institute of Technology, Pasadena, CA 91125 USA (e-mail: ppvnath@systems.caltech.edu).

Digital Object Identifier 10.1109/TSP.2014.2331617

One of the goals of this paper is to replace each $c_q(n)$ with an entire subspace of period-q signals which we call the Ramanujan subspace $\mathcal{S}_q$ (Section IV). This space has dimension $\phi(q)$ (Euler's totient function, see Section I-A) and contains $c_q(n)$ as one member. We will study several properties of this subspace, such as periodicity properties, autocorrelation properties, and projection properties. The results obtained in the process will allow us to develop applications of Ramanujan sums based on a more solid theoretical footing. They lead to the developments reported in the companion paper [21], which introduces new representations for finite duration (FIR) signals in terms of Ramanujan sums. These are somewhat similar to time-frequency representations. The most important point is that an arbitrary finite duration signal can be decomposed into a sum of a finite number of orthogonal projections $x_{q_i}(n)$ belonging to Ramanujan subspaces $\mathcal{S}_{q_i}$, with each component representing a periodic component of $x(n)$. This is useful in extracting hidden periods in finite duration signals. We will see that an arbitrary finite duration signal can be projected onto the Ramanujan subspace $\mathcal{S}_q$ to obtain the period-q component of that signal. Furthermore, such a projection can be computed using integer operations alone (Section IV-C).

We believe there has not been a full length paper in these transactions, dedicated to the Ramanujan sum or its signal processing applications. The review in Section II, and the material in the Appendix ensure that the paper is self contained and accessible to readers of the transactions. To our knowledge all material in this paper and the companion paper [21] are new, except for the review in Section II.

A. Outline and Notations

The detailed outline for this paper (Part 1) is as follows. In Section II we review Ramanujan sums and mention some of its well-known properties which are crucial to all discussions. In Section III we present a recursive way to compute Ramanujan sums. This is important from a signal processing view point, as the recursive computations can be done entirely using integer operations, unlike a direct use of the definition (1). In Section IV we introduce a new class of subspaces called the Ramanujan subspaces. Several properties of these subspaces are also presented. It is shown that the projection matrix for this subspace is essentially an integer circulant matrix, which makes it attractive from a computational viewpoint. In Section V we study the properties of autocorrelations of signals belonging to the Ramanujan subspaces, and show that this subspace is closed under the operation of circular cross-correlation. These properties, besides their theoretical importance, are also useful in the denoising applications presented in [21]. A detailed study of periodicity properties of signals belonging to Ramanujan subspaces is presented in Section VI. Unlike arbitrary periodic signals, the signals belonging to Ramanujan spaces have certain unique periodicity properties which make them attractive for decomposition of arbitrary signals into periodic components. This will become more clear in Section VI, and again when we use Ramanujan representations in [21] for extracting periodicities. The following notations are used throughout:

1) $W_q = e^{-j2\pi/q}$ is the qth root of unity, and $\mathbb{C}^q$ the q dimensional space of complex vectors. For a matrix $\mathbf{A}$, the transpose, conjugate, and transpose-conjugate are denoted as $\mathbf{A}^T$, $\mathbf{A}^*$ and $\mathbf{A}^\dagger$ respectively.
2) The abbreviations *lcm* and *gcd* stand for least common multiple and greatest common divisor, respectively.
3) The notation (k, q) represents the gcd of the integers k and q. So $(k, q) = 1$ means that k and q are coprime, that is, they have no common factor other than unity.
4) The quantity $\phi(q)$ is the *Euler's totient function*[6]. It is equal to the number of integers k in $1 \leq k \leq q$ satisfying $(k, q) = 1$. For example if $q = 10$, then the integers $1, 3, 7$ and 9 are coprime to q, so $\phi(10) = 4$.
5) The notation $q_i|q$ means that q_i is a divisor of q (i.e., a factor of q). For example, if $q = 10$, the divisors are $q_1 = 1, q_2 = 2, q_3 = 5, q_4 = 10$.
6) $\mathcal{S}_q$ denotes the Ramanujan subspace associated with the integer q. It is defined in Section IV.
7) The symbol $\diamondsuit$ is used as end-marker for Theorems, lemmas, and definitions. The symbol $\triangledown\ \triangledown\ \triangledown$ is used as end marker for proofs.

Reference [20] is a brief conference version containing some of the ideas in the paper.

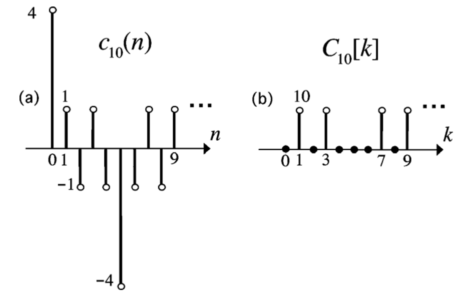


Fig. 1. (a), (b) Plots of the Ramanujan sum $c_{10}(n)$ and its DFT $C_{10}[k]$.

II. Review of Ramanujan Sums

The qth Ramanujan sum ($q \geq 1$) is a sequence in n defined as

$$c_q(n) = \sum_{\substack{k=1\\(k,q)=1}}^{q} e^{j2\pi kn/q} = \sum_{\substack{k=1\\(k,q)=1}}^{q} W_q^{-kn} \tag{3}$$

Thus the summation runs over only those values of k that are coprime to q. So, the sum (3) has precisely $\phi(q)$ terms, and

$$c_q(0) = \phi(q) \tag{4}$$

From (3) we see that $c_q(n)$ is periodic:

$$c_q(n + q) = c_q(n) \tag{5}$$

Equation (3) also shows that the DFT of $c_q(n)$ is

$$C_q[k] = \begin{cases} q & \text{if } (k, q) = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

For example, see Fig. 1 which shows $c_{10}(n)$ and $C_{10}[k]$. Equation (6) can be regarded as the defining property of the qth Ramanujan sum.

If $(k,q)=1$ then it follows that $(q-k,q)=1$ as well. Since $W_q^{(-(q-k))}=W_q^k=(W_q^{-k})^*$ it then follows that the summation in (3) is real valued. Thus (3) can be written as

$$c_q(n)=\sum_{\substack{k=1\\(k,q)=1}}^{q}\cos\frac{2\pi kn}{q} \tag{7}$$

which was Ramanujan's original definition [13]. Summarizing, $c_q(n)$ can be written in these forms:

$$c_q(n)=\sum_{\substack{k=1\\(k,q)=1}}^{q}W_q^{kn}=\sum_{\substack{k=1\\(k,q)=1}}^{q}W_q^{-kn}=\sum_{\substack{k=1\\(k,q)=1}}^{q}\cos\frac{2\pi kn}{q} \tag{8}$$

From (7) it is clear that $c_q(n)$ is a *real* sequence. Furthermore it is *symmetric*, that is, $c_q(n)=c_q(-n)$, or in view of periodicity,

$$c_q(n)=c_q(q-n) \tag{9}$$

which is consistent with the fact that the DFT $C_q[k]$ is real. Thus any Ramanujan sum $c_q(n)$ is a real, symmetric, and periodic sequence in n. Here are the first few Ramanujan sequences, shown for one period $0\le n\le q-1$.

$$\begin{aligned}
c_1(n)&=1\\
c_2(n)&=1,-1\\
c_3(n)&=2,-1,-1\\
c_4(n)&=2,0,-2,0\\
c_5(n)&=4,-1,-1,-1,-1\\
c_6(n)&=2,1,-1,-2,-1,1\\
c_7(n)&=6,-1,-1,-1,-1,-1,-1\\
c_8(n)&=4,0,0,0,-4,0,0,0\\
c_9(n)&=6,0,0,-3,0,0,-3,0,0\\
c_{10}(n)&=4,1,-1,1,-1,-4,-1,1,-1,1
\end{aligned} \tag{10}$$

Notice that $c_q(n)$ is always *integer-valued.* Ramanujan proved this by establishing a relation between $c_q(n)$ and the Möbius function (Section II-B). An independent proof is given in Section III (Corollary 1).

1) Relation to Primitive Roots: We know that α is a *qth root of unity* if $\alpha^q=1$. We say that α is a *primitive* qth root of unity if $\alpha^q=1$, but $\alpha^n\neq 1$ for any positive integer $n<q$. Now, W_q^{-k} is a primitive qth root of unity if and only if $(q,k)=1$.[1] So the Ramanujan sum $c_q(n)$ can be defined as the sum of nth powers of *all* the qth primitive roots of unity.

A. Further Properties of Ramanujan Sums

We now present further properties of Ramanujan sums which can be of interest in signal processing research. For completeness most proofs are included either here or in the Appendix.

1) *Sum and sum-of-squares.* By definition, for $q>1$ the DFT $C_q[k]=0$ for $k=0$. Thus

$$\sum_{n=0}^{q-1}c_q(n)=0,\quad \text{for } q>1. \tag{11}$$

Next, by Parseval's relation for DFTs, we have $\sum_{n=0}^{q-1}c_q^2(n)=\sum_{k=0}^{q-1}C_q^2[k]/q=q^2\phi(q)/q=q\phi(q)$ from (6). Thus

$$\sum_{n=0}^{q-1}c_q^2(n)=q\phi(q) \tag{12}$$

2) *Orthogonality.* Any two Ramanujan sums $c_{q_1}(n)$ and $c_{q_2}(n)$ are orthogonal in the sense that

$$\sum_{n=0}^{m-1}c_{q_1}(n)c_{q_2}(n)=0,\quad q_1\neq q_2. \tag{13}$$

where

$$m=\mathrm{lcm}(q_1,q_2). \tag{14}$$

More generally, it is also true that

$$\sum_{n=0}^{m-1}c_{q_1}(n)c_{q_2}(n-l)=0, q_1\neq q_2 \tag{15}$$

for any integer l. Since $c_{q_2}(n)$ has period q_2, the argument $(n-l)$ can be interpreted modulo q_2. Equation (15) follows from the fact that whenever $(k_i,q_i)=1$, the two sequences $x_1(n)=W_{q_1}^{-k_1n},\ x_2(n)=W_{q_2}^{-k_2n}$ $(q_1\neq q_2)$ are orthogonal over an interval of length m, that is,

$$\sum_{n=0}^{m-1}W_{q_1}^{-k_1n}W_{q_2}^{k_2n}=0 \tag{16}$$

(see Appendix). Combined with (12), (13) yields

$$\sum_{n=0}^{m-1}c_{q_1}(n)c_{q_2}(n)=q_1\phi(q_1)\delta(q_1-q_2) \tag{17}$$

where $m=\mathrm{lcm}(q_1,q_2)$ is the common period of $c_{q_1}(n)$ and $c_{q_2}(n)$.

3) *Nonoverlapping DFT.* A second way to see the orthogonality property (13) is to rewrite

$$\begin{aligned}
c_{q_1}(n)&=\sum_{\substack{k_1=1\\(k_1,q_1)=1}}^{q_1}W_{q_1}^{-k_1n}=\sum_{\substack{k_1=1\\(k_1,q_1)=1}}^{q_1}W_m^{-k_1l_1n}\\
&=\frac{m}{q_1}\sum_{\substack{k_1=1\\(k_1,q_1)=1}}^{m}W_m^{-k_1l_1n}
\end{aligned} \tag{18}$$

we see that $c_{q_1}(n)$, regarded as a period-m sequence has nonzero DFT coefficients only at $k=k_1l_1$ where $(k_1,q_1)=1$. Similarly $c_{q_2}(n)$, regarded as a period-m sequence has nonzero DFT coefficients only at $k=k_2l_2$ where $(k_2,q_2)=1$. But these nonzero DFT points do not overlap because $k_1l_1=k_2l_2$ implies $k_1m/q_1=k_2m/q_2$, i.e., $k_1/q_1=k_2/q_2$ which is not possible (since $(k_1,q_1)=(k_2,q_2)=1$). *Thus, the DFT coefficients of two different Ramanujan sequences never overlap.* Hence, by Parseval's relation, (13) follows.

[1]*Proof.* $(W_q^{-k})^n=1$ if and only if $kn=ql$ for some integer l, i.e., $k/q=l/n$. There is no $n<q$ satisfying this if and only if $(k,q)=1$.

4) *Prime q.*[2] If q is a prime number, then

$$c_q(n) = \begin{cases} q-1 & \text{if } n = \text{mul.of } q \\ -1 & \text{otherwise.} \end{cases} \tag{19}$$

This is clearly seen in the examples $c_3(n), c_5(n), c_7(n)$, in (10). The proof is as follows: if q is prime then $(k,q)=1$ for all k in $1 \le k \le q-1$. Thus

$$c_q(n) = \sum_{k=1}^{q-1} W_q^{-kn} = \sum_{k=0}^{q-1} W_q^{-kn} - 1 \tag{20}$$

from which the desired result follows.

5) *Power of prime.* If $q = p^m$ for some prime p and integer $m > 1$ then (see Appendix)

$$c_{p^m}(n) = \begin{cases} 0 & \text{if } p^{m-1} \not| \, n \\ -p^{m-1} & \text{if } p^{m-1}|n \text{ but } p^m \not| \, n \\ p^{m-1}(p-1) & \text{if } p^m|n \end{cases} \tag{21}$$

For example, $c_4(n), c_8(n)$ and $c_9(n)$ in (10) can be readily computed using this.

6) *Multiplicative property.* A function $f(n)$ is said to be multiplicative if $f(n_1n_2) = f(n_1)f(n_2)$ whenever $(n_1,n_2)=1$. For example it can be shown that the Euler totient $\phi(n)$ and the Möbius function $\mu(n)$ (Section II-B) are multiplicative [6]. It turns out that Ramanujan sequences $c_q(n)$ are multiplicative in q, that is, whenever, q_1 and q_2 are coprime

$$c_{q_1q_2}(n) = c_{q_1}(n)c_{q_2}(n) \tag{22}$$

This was first shown by Hardy in 1921 [5], and a proof is included in the Appendix). Returning to the examples in (10) we now see that $c_6(n)$ can be obtained by inspection of $c_2(n)$ and $c_3(n)$, and similarly $c_{10}(n)$ from $c_2(n)$ and $c_5(n)$.

B. Relation to Möbius Function

Finally we mention without proof some relations between Ramanujan-sums and the Möbius function $\mu(n)$ defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^K & \text{if } n = p_1p_2\ldots p_K \\ 0 & \text{otherwise.} \end{cases} \tag{23}$$

Here p_i are distinct primes. Note that $\mu(n)=0$ if and only if n has a square factor, e.g., $\mu(2^2\times 3)=0, \mu(2^3\times 5)=0$, and so forth. Ramanujan showed [13] that

$$c_q(n) = \sum_{d|(q,n)} \mu\left(\frac{q}{d}\right) d \tag{24}$$

Another relation between $c_q(n)$ and $\mu(n)$ is [6]

$$c_q(n) = \frac{\mu(\rho)\phi(q)}{\phi(\rho)}, \quad \text{where} \quad \rho = \frac{q}{(q,n)} \tag{25}$$

This was first proved by Hölder in 1936 (see [5, p. 271]). Setting $n=1$ we have $\rho = q$ so that

$$c_q(1) = \mu(q), \quad \text{that is,} \quad \mu(q) = \sum_{\substack{k=1 \\ (k,q)=1}}^{q} W_q^k \tag{26}$$

In fact, for any n coprime to q we have $(q,n)=1$, so $\rho = q$ in (25), which yields the result

$$c_q(n) = \mu(q), \quad \text{whenever } (q,n) = 1. \tag{27}$$

III. Recursive Computation of Ramanujan Sums

We now show that $c_q(n)$ can be computed recursively in the following sense: if we know $c_q(n)$ for $q < Q$, then we can form a integer linear combination of these to find $c_Q(n)$. So, starting from $c_1(n)=1$, we can compute $c_q(n)$ recursively for all $q>1$, and this will involve only additions and subtractions. A by product is an independent proof of the fact that $c_q(n)$ are themselves integers.

In the definition of the Ramanujan sum (3) we have the set of rationals k/q appearing in the exponent, where q is fixed, and $(k,q)=1$. This set of irreducible rationals $\{k/q\}$ has only $\phi(q)$ elements, unlike the set of *all* rationals

$$\mathcal{S}_1 = \left\{ \frac{h}{q} \,\middle|\, 1 \le h \le q \right\} \tag{28}$$

which has q elements. It is clear that $\mathcal{S}_1$ can be written as a union of irreducible rationals. Thus consider

$$\mathcal{S}_2 = \left\{ \frac{a}{d} \,\middle|\, 1 \le a \le d,\ (a,d)=1,\ d|q \right\} \tag{29}$$

Then $\mathcal{S}_1 = \mathcal{S}_2$.[3] For example if $q=6$, then

$$\mathcal{S}_1 = \left\{\frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}, \frac{6}{6}\right\} \tag{30}$$

$$\text{and} \quad \mathcal{S}_2 = \left\{1\right\} \cup \left\{\frac{1}{2}\right\} \cup \left\{\frac{1}{3}, \frac{2}{3}\right\}, \cup \left\{\frac{1}{6}, \frac{5}{6}\right\} \tag{31}$$

So $\mathcal{S}_1 = \mathcal{S}_2$ indeed. This elementary observation leads to the following useful result [6]:

Theorem 1: Let $F(x)$ be any function of x, and consider evaluating the sum of uniformly spaced samples at $x = h/q$, where $1 \le h \le q$, and q is a fixed positive integer. Then

$$\sum_{h=1}^{q} F\left(\frac{h}{q}\right) = \sum_{d|q} \sum_{\substack{a=1 \\ (a,d)=1}}^{d} F\left(\frac{a}{d}\right) \tag{32}$$

Thus we can compute the sum of samples in two stages. ◊

For example if $F(x)=1$ for all x, then the left hand side is q and the inner sum on the right side is $\phi(d)$ (Euler's totient). So (32) yields

$$\sum_{d|q} \phi(d) = q, \tag{33}$$

[2]An integer p is a prime if $p>1$, and its only divisors are 1 and p.

[3]If $x \in \mathcal{S}_1$, then $x = h/q$ and can be rewritten as a/d by canceling the gcd between h and q. So, $x \in \mathcal{S}_2$ as well. Conversely, suppose $y \in \mathcal{S}_2$. Then $y = a/d$ where $a \le d$ and d is a divisor of q. So we can rewrite $y = al/q$ for some integer l. Clearly $al \le q$, so $y \in \mathcal{S}_1$. So $\mathcal{S}_1 = \mathcal{S}_2$.

a well known result [6]. As a second example let $F(x)=e^{j2\pi nx}$ where n is a fixed integer. Now (32) yields

$$\sum_{h=1}^{q} e^{j\frac{2\pi h}{q}n}=\sum_{d|q}\sum_{\substack{a=1\\(a,d)=1}}^{d} e^{j\frac{2\pi a}{d}n} \tag{34}$$

The left hand side is $q\delta((n))_q$ where $\delta((n))_q=1$ if $n=0$ mod q, and zero otherwise. The inner sum on the right hand side is precisely the Ramanujan sum $c_d(n)$. Thus (34) implies

$$\sum_{d|q} c_d(n)=q\delta((n))_q \tag{35}$$

So we have proved the following:

Theorem 2. Recursion: The Ramanujan sum $c_q(n)$ can be expressed in terms of lower order Ramanujan sums as follows:

$$c_q(n)=q\delta((n))_q-\sum_{\substack{q_k|q\\q_k<q}} c_{q_k}(n) \tag{36}$$

where $q_k|q$ denotes that q_k are divisors of q. ♢

When q is a prime, $q_1=1$ and $q_2=q$, so (36) yields another proof of (19). Equation (36) gives us a recursive way to compute $c_q(n)$ by starting from $c_1(n)=1$. For example, $c_{10}(n)=10\delta((n))_{10}-c_1(n)-c_2(n)-c_5(n)$, and $c_5(n)=5\delta((n))_5-c_1(n)$. Only simple addition and subtraction operations are involved. It follows from this by induction that $c_q(n)$ is an integer for all n. So we have found yet another proof of the following result:

Corollary 1. Integer Values: The Ramanujan sums $c_q(n)$ are integer valued for all $q\geq 1$ and all n. ♢

The fact that $c_q(n)$ is integer-valued can also be seen from (24) or from (25). Yet another way to prove it is by repeatedly using the multiplicative property (22) and the fact that $c_q(n)$ has integer values when q is a power of prime (see (21)). Note that in vector form (35) takes the form

$$[1 \quad 0 \quad \ldots \quad 0]^T=\frac{1}{q}\sum_{q_i|q}\mathbf{c}_{q_i} \tag{37}$$

where $\mathbf{c}_{q_i}$ represents q/q_i periods of $c_{q_i}(n)$.

IV. The Ramanujan Periodic Subspace $\mathcal{S}_q$

Consider the representation of an arbitrary signal $x(n)$ using an expansion of the form (2). Here the attempt is to represent the period-q component of $x(n)$ by the sequence $c_q(n)$. But $c_q(n)$ is only one of many possible period-q signals, and there is no reason to expect arbitrary period-q components to be representable by $c_q(n)$. In this section we will show that starting from $c_q(n)$ we can actually generate an entire subspace $\mathcal{S}_q$ of period-q signals with dimension $\phi(q)$, which we call the *Ramanujan subspace*. Such a subspace captures a much broader class of period-q signals and has an integer basis consisting of $c_q(n)$ and its shifted relatives. We will see in [21] that by combining a finite number of such "periodic" subspaces, any finite duration signal can be represented.

The purpose of this section is to define this subspace and develop some of its mathematical properties. Starting from $c_q(n)$ let use first define the $q\times q$ integer circulant matrix shown below:

$$\mathbf{B}_q=\begin{bmatrix} c_q(0) & c_q(q-1) & c_q(q-2) & \ldots & c_q(1)\\ c_q(1) & c_q(0) & c_q(q-1) & \ldots & c_q(2)\\ c_q(2) & c_q(1) & c_q(0) & \ldots & c_q(3)\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ c_q(q-2) & c_q(q-3) & c_q(q-4) & \ldots & c_q(q-1)\\ c_q(q-1) & c_q(q-2) & c_q(q-3) & \ldots & c_q(0)\end{bmatrix} \tag{38}$$

For example

$$\mathbf{B}_5=\begin{bmatrix} c_5(0) & c_5(4) & c_5(3) & c_5(2) & c_5(1)\\ c_5(1) & c_5(0) & c_5(4) & c_5(3) & c_5(2)\\ c_5(2) & c_5(1) & c_5(0) & c_5(4) & c_5(3)\\ c_5(3) & c_5(2) & c_5(1) & c_5(0) & c_5(4)\\ c_5(4) & c_5(3) & c_5(2) & c_5(1) & c_5(0)\end{bmatrix} =\begin{bmatrix} 4 & -1 & -1 & -1 & -1\\ -1 & 4 & -1 & -1 & -1\\ -1 & -1 & 4 & -1 & -1\\ -1 & -1 & -1 & 4 & -1\\ -1 & -1 & -1 & -1 & 4\end{bmatrix} \tag{39}$$

So, every column is obtained by a circular downward shift of the previous column. Equivalently every row is a circular right shift of the preceding row. A number of simple properties of this matrix are evident:

1) The 0th row is the time-reversed Ramanujan sum $c_q(q-n)$.
2) Since $c_q(q-n)=c_q(n)$, we see that $\mathbf{B}_q$ is symmetric, that is, $\mathbf{B}_q^T=\mathbf{B}_q$. In fact it is Hermitian (since real).
3) Being circulant, the matrix is also Toeplitz, that is, all elements along any line parallel to diagonal are identical.

Definition 1. Ramanujan Space: The column space of $\mathbf{B}_q$ will be called the Ramanujan subspace $\mathcal{S}_q$. ♢

Clearly $c_q(n)$, and all its circularly shifted versions, belong to this space. We will see that the matrix $\mathbf{B}_q$ has rank $\phi(q)$, so the space $\mathcal{S}_q\in\mathbb{C}^q$ has dimension $\phi(q)$. In fact we will show that the first $\phi(q)$ columns (or any $\phi(q)$ consecutive columns) are linearly independent, and form a basis for this space.

A. Diagonalizing With a DFT

We know any circulant matrix is diagonalized by the DFT matrix. That is,

$$\mathbf{B}_q=\mathbf{W}^{-1}\mathbf{\Lambda}_q\mathbf{W}=\frac{\mathbf{W}^{\dagger}\mathbf{\Lambda}_q\mathbf{W}}{q} \tag{40}$$

where $\mathbf{W}$ is the $q\times q$ DFT matrix, and

$$\mathbf{\Lambda}_q=\begin{bmatrix} C_q[0] & 0 & \ldots & 0\\ 0 & C_q[1] & \ldots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \ldots & C_q[q-1]\end{bmatrix} \tag{41}$$

Here $C_q[k]$ are the DFT coefficients of the Ramanujan sequence $c_q(n)$, that is,

$$C_q[k]=\sum_{n=0}^{q-1} c_q(n)W^{nk}=\begin{cases} q & \text{if } (k,q)=1\\ 0 & \text{otherwise.}\end{cases} \tag{42}$$

Since $\mathbf{W}/\sqrt{q}$ is unitary, we see that (40) is equivalent to $\mathbf{B}_q\mathbf{W}^\dagger = \mathbf{W}^\dagger\mathbf{\Lambda}_q$. By conjugating both sides and using the facts that $c_q(n)$ and $C_q[k]$ are real and $\mathbf{W} = \mathbf{W}^T$, we get

$$\mathbf{B}_q\mathbf{W} = \mathbf{W}\mathbf{\Lambda}_q \tag{43}$$

So the columns of $\mathbf{W}$ are the eigenvectors of $\mathbf{B}_q$, with corresponding eigenvalues $C_q[k]$. Some further conclusions for future use:

1) *Rank and dimension.* There are $\phi(q)$ nonzero eigenvalues, and $\mathbf{B}_q$ has rank $\phi(q)$. So $\mathcal{S}_q$ has dimension $\phi(q)$.
2) *Positive semidefiniteness.* Since $\mathbf{B}_q$ is Hermitian with nonnegative eigenvalues $\in \{0, q\}$, it is positive semidefinite.
3) *Factorization.* The circulant $\mathbf{B}_q$ can be factorized as

$$\mathbf{B}_q = \underbrace{\mathbf{V}}_{q\times\phi(q)} \underbrace{\mathbf{V}^\dagger}_{\phi(q)\times q} \tag{44}$$

where $\mathbf{V}$ a submatrix of the DFT matrix $\mathbf{W}$ obtained by retaining the "coprime columns", i.e., columns numbered k_i such that $(k_i, q) = 1$. This follows directly from (40) by using (41) and (42). For example, let $q = 4$. Then since $k_1 = 1$ and $k_2 = 3$ are the only indices coprime to 4, we have

$$\mathbf{B}_4 = \begin{bmatrix} 2 & 0 & -2 & 0 \\ 0 & 2 & 0 & -2 \\ -2 & 0 & 2 & 0 \\ 0 & -2 & 0 & 2 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 1 \\ W & W^3 \\ W^2 & W^6 \\ W^3 & W^9 \end{bmatrix} \begin{bmatrix} 1 & W^{-1} & W^{-2} & W^{-3} \\ 1 & W^{-3} & W^{-6} & W^{-9} \end{bmatrix} \tag{45}$$

where $W = W_4 = e^{-j2\pi/4}$. We see from (44) that the column space of $\mathbf{B}_q$ is the column space of $\mathbf{V}$, and is spanned by the $\phi(q)$ columns

$$\begin{bmatrix} 1 \\ W^{k_1} \\ W^{2k_1} \\ \vdots \\ W^{(q-1)k_1} \end{bmatrix}, \begin{bmatrix} 1 \\ W^{k_2} \\ W^{2k_2} \\ \vdots \\ W^{(q-1)k_2} \end{bmatrix}, \ldots, \begin{bmatrix} 1 \\ W^{k_{\phi(q)}} \\ W^{2k_{\phi(q)}} \\ \vdots \\ W^{(q-1)k_{\phi(q)}} \end{bmatrix} \tag{46}$$

where $W = e^{-j2\pi/q}$ and $(k_i, q) = 1$.

So the relationship between the Ramanujan space $\mathcal{S}_q$ and the DFT matrix can be summarized as follows:

Theorem 3. Ramanujan Spaces and DFT Matrices: The Ramanujan subspace $\mathcal{S}_q \subset \mathbb{C}^q$ is identical to the space spanned by those $\phi(q)$ columns (46) of the $q \times q$ DFT matrix $\mathbf{W}$, whose column indices k are coprime to q. $\diamondsuit$

B. Integer Basis for the Ramanujan Space $\mathcal{S}_q$

The basis for $\mathcal{S}_q$ obtained from the DFT matrix is not an integer basis. We now identify $\phi(q)$ columns of the integer matrix $\mathbf{B}_q$ which can form an integer basis for $\mathcal{S}_q$. Even though the rank of $\mathbf{B}_q$ is $\phi(q)$, an arbitrary set of $\phi(q)$ columns of $\mathbf{B}_q$ may not independent. For example although $\mathbf{B}_4$ has rank 2, the first and third columns of $\mathbf{B}_4$ are parallel (see (45)). However, we can prove:

Theorem 4. Consecutive Columns: Consider a submatrix $\mathbf{S}$ of the circulant $\mathbf{B}_q$ obtained by retaining any consecutive $\phi(q)$ columns, i.e., columns $l, l+1, \ldots, l+\phi(q)-1$ for some l. This submatrix has rank $\phi(q)$. $\diamondsuit$

The integer l in the theorem can take any value in the range $0 \le l \le q-1$. The quantities $l+1$, $l+2$, etc., are to be interpreted modulo q, as we shall see from the proof.

Proof of the Theorem: The submatrix described in the theorem can be written as

$$\mathbf{S} = \underbrace{\mathbf{V}}_{q\times\phi(q)} \underbrace{\mathbf{V}_1}_{\phi(q)\times\phi(q)} \tag{47}$$

where $\mathbf{V}_1$ has ith row

$$\begin{bmatrix} \alpha_i^l & \alpha_i^{l+1} & \ldots & \alpha_i^{l+\phi(q)-1} \end{bmatrix} = \alpha_i^l \begin{bmatrix} 1 & \alpha_i & \ldots & \alpha_i^{\phi(q)-1} \end{bmatrix}$$

Here $\alpha_i = W^{-k_i}$, with $(k_i, q) = 1$. So, each row is a Vandermonde vector (except for the scale factor α_i^l which is factored out) and furthermore, α_i is distinct for different rows. To see this observe, for example, that $\alpha_1 = \alpha_2$ if and only if $W^{(k_1-k_2)} = 1$, that is $k_1 - k_2 = kq$ for some integer k. But since $0 \le k_1 < k_2 \le q-1$, it is plain that $|k_1 - k_2| < q$ so the preceding is possible if and only if $k = 0$ which contradicts $k_1 \ne k_2$. This proves α_i are distinct. The matrix $\mathbf{V}_1$ is therefore of the form

$$\mathbf{V}_1 = \mathbf{\Lambda}\mathbf{V}_2 \tag{48}$$

where $\mathbf{\Lambda}$ is a diagonal matrix with nonzero diagonal elements and $\mathbf{V}_2$ is $\phi(q) \times \phi(q)$ with row-Vandermonde structure. Thus $\mathbf{V}_1$ is nonsingular. Since $\mathbf{V}$ is column-Vandermonde with distinct elements on the 1st row, it has rank $\phi(q)$. The product $\mathbf{S}$ therefore has rank $\phi(q)$. $\triangledown\triangledown\triangledown$

In this work we will be especially interested in the submatrix $\mathbf{C}_q$ of $\mathbf{B}_q$, obtained by retaining the *first* $\phi(q)$ columns. We have

$$\mathbf{C}_q = \underbrace{\mathbf{V}}_{q\times\phi(q)} \underbrace{\mathbf{U}}_{\phi(q)\times\phi(q)} \tag{49}$$

where $\mathbf{U}$ is a submatrix of the DFT matrix obtained by retaining the first $\phi(q)$ columns, and the $\phi(q)$ rows who's indices are coprime to q. Here are some examples: $\mathbf{C}_1 = 1$,

$$\mathbf{C}_2 = \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \; \mathbf{C}_3 = \begin{bmatrix} 2 & -1 \\ -1 & 2 \\ -1 & -1 \end{bmatrix}, \; \mathbf{C}_4 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \\ -2 & 0 \\ 0 & -2 \end{bmatrix}$$

From the preceding theorem $\mathbf{C}_q$ has full rank $\phi(q)$, and spans the Ramanujan space $\mathcal{S}_q$. We can summarize this result as follows:

Theorem 5: The Ramanujan sum $c_q(n)$ and its $\phi(q) - 1$ consecutive circular shifts (i.e., the first $\phi(q)$ columns of the circulant matrix $\mathbf{B}_q$) constitute an integer basis for the Ramanujan space $\mathcal{S}_q \subset \mathbb{C}^q$. $\diamondsuit$

Thus $x(n) \in \mathcal{S}_q$ if and only if it can be expressed in either one of the following equivalent forms:

$$x(n) = \sum_{l=0}^{\phi(q)-1} \beta_l c_q(n-l) = \sum_{\substack{1\le k\le q \\ (k,q)=1}} \alpha_k W_q^{kn} \tag{50}$$

Whereas the $\phi(q)$ circularly shifted Ramanujan sequences $\{c_q(n-l)\}$ form an integer basis for the Ramanujan space $\mathcal{S}_q$, the $\phi(q)$ sequences W_q^{kn} (with $(k,q)=1$) form a complex (DFT-style, orthogonal) basis. We will see that $\{c_q(n-l)\}$ is a non-orthogonal basis unless q is a power of two (Lemma 2). A simple consequence of the preceding theorem is the following:

Theorem 6. Shift Invariance: The subspace $\mathcal{S}_q \subset \mathbb{C}^q$ is a circularly shift invariant subspace, that is, if $x(n) \in \mathcal{S}_q$, then $x(n-k) \in \mathcal{S}_q$ where the shift is interpreted as a circular shift modulo q. $\diamondsuit$

Proof: We know $x(n) \in \mathcal{S}_q$ if and only if $x(n) = \sum_{l=0}^{\phi(q)-1} \beta_l c_q(n-l)$. So

$$x(n-k) = \sum_{l=0}^{\phi(q)-1} \beta_l c_q(n-l-k). \tag{51}$$

For fixed k and l, the sequence $s(n) \triangleq c_q(n-l-k)$ is a column of the circulant matrix $\mathbf{B}_q$ (since the shift is interpreted modulo q). So $x(n-k)$ is in the column space of $\mathbf{B}_q$, i.e., $x(n-k) \in \mathcal{S}_q$. $\triangledown\triangledown\triangledown$

1) A Caution About the Notation: We defined $\mathcal{S}_q$ as a $\phi(q)$-dimensional subspace of vectors in $\mathbb{C}^q$, spanned by columns of $\mathbf{C}_q$. For visualization we sometimes regard the elements of $\mathcal{S}_q$ as period-q sequences. Moreover we will sometimes need to define matrices which are repetitions of rows of $\mathbf{C}_q$, such as

$$\mathbf{G}_q = \begin{bmatrix} \mathbf{C}_q \\ \mathbf{C}_q \\ \vdots \\ \mathbf{C}_q \end{bmatrix} \tag{52}$$

If there are r repetitions then the column space of this matrix is a subspace of $\mathbb{C}^{qr}$. But it is obvious that this space is determined entirely by $\mathcal{S}_q \subset \mathbb{C}^q$. To avoid a multitude of notations we shall continue to refer to this as the space $\mathcal{S}_q$, and the sizes of the vectors (e.g., qr) are usually clear from the context. So, when we say that $x(n) \in \mathcal{S}_q$, it is understood that the vector of size q is extended periodically to obtain the sequence $x(n)$.

C. The Projection Matrix for $\mathcal{S}_q$

Recall now that a square matrix $\mathbf{P}$ is a projection if $\mathbf{P}^2 = \mathbf{P}$, and an orthogonal projection if it is also Hermitian. With the circulant $\mathbf{B}_q$ defined as in (38), consider now the Hermitian matrix

$$\mathbf{P}_q = \frac{\mathbf{B}_q}{q} \tag{53}$$

We have

$$\mathbf{P}_q^2 = \frac{\mathbf{V}\mathbf{V}^\dagger\mathbf{V}\mathbf{V}^\dagger}{q^2} = \frac{\mathbf{V}\mathbf{V}^\dagger}{q} = \mathbf{P}_q \tag{54}$$

where we have used $\mathbf{V}^\dagger\mathbf{V} = q\mathbf{I}_{\phi(q)}$. Thus, $\mathbf{P}_q$ is an *orthogonal projection*. Since the column space of $\mathbf{B}_q$ is $\mathcal{S}_q$ it follows that $\mathbf{P}_q$ is the projection onto $\mathcal{S}_q$. Given an arbitrary vector $\mathbf{x} \in \mathbb{C}^q$, this projection can be calculated as

$$\mathbf{x}_q = \mathbf{P}_q\mathbf{x} = \frac{\mathbf{B}_q\mathbf{x}}{q}, \tag{55}$$

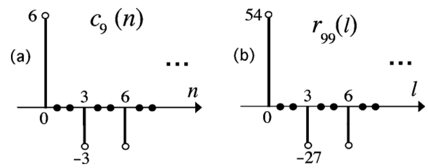


Fig. 2. (a), (b) Plots of the Ramanujan sum $c_9(n)$ and its autocorrelation.

Since $\mathbf{B}_q$ has integer elements bounded by $c_q(0) = \phi(q)$ the projection $\mathbf{P}_q\mathbf{x}$ can be calculated by simple integer operations (binary shifts and adds) on the (possibly complex) elements of $\mathbf{x}$ and dividing the result by q. We will find this especially useful when analyzing finite duration signals in terms of their periodic components ([21, Sec. V.C]).

Since $\mathbf{B}_q$ is a circulant, the projection operation represents a circular convolution of $\mathbf{x}$ with the Ramanujan sum. Computing this circular convolution using the DFT requires complex operations, whereas direct multiplication using $\mathbf{B}_q$ would only require integer operations. Since $\mathcal{S}_q$ is also the column space of the $q \times \phi(q)$ matrix $\mathbf{C}_q$ of rank $\phi(q)$, the projection can also be written as $\mathbf{P}_q = \mathbf{C_q}(\mathbf{C_q}^\dagger\mathbf{C}_q)^{-1}\mathbf{C_q}^\dagger$. But there is no need to compute the complicated right hand side, as the projection can be expressed directly as $\mathbf{B}_q/q$.

V. Correlations of Sequences in $\mathcal{S}_q$

The elements in the Ramanujan subspace $\mathcal{S}_q$ have very beautiful properties. One of these is that the (circular) cross correlation of any two elements in $\mathcal{S}_q$ belongs to $\mathcal{S}_q$. That is, $\mathcal{S}_q$ is closed under the correlation operation. To show this we first prove the following:

Theorem 7: The Ramanujan sum $c_q(n)$ has the following circular autocorrelation:

$$r_{qq}(l) \triangleq \sum_{n=0}^{q-1} c_q(n)c_q(n-l) = qc_q(l), \tag{56}$$

where $(n-l)$ is to be interpreted modulo q because $c_q(n)$ has periodic q. $\diamondsuit$

So a plot of $r_{qq}(l)$ looks the same as $c_q(l)$ (Fig. 2). The correlation is zero only for those lags l for which $c_q(l)$ itself is zero. Also, the maximum correlation is $qc_q(0) = q\phi(q)$.

Proof of Theorem 7: Since $r_{qq}(l)$ is the circular correlation, its q-point DFT is given by

$$R_{qq}[k] = C_q[k]C_q^*[k] = \begin{cases} q^2 & (k,q)=1 \\ 0 & \text{otherwise.} \end{cases} \tag{57}$$

The right hand side is $qC_q[k]$ (see (6)). So $r_{qq}(l) = qc_q(l)$ indeed. $\triangledown\triangledown\triangledown$

A second way to understand (56) is as follows: since $\mathbf{P}_q = \mathbf{B}_q/q$ is an orthogonal projection, we have $\mathbf{B}_q^2 = q\mathbf{B}_q$, which can be rewritten as $\mathbf{B}_q^T\mathbf{B}_q = q\mathbf{B}_q$. The element by element reading of this equation yields (56) indeed! We next prove:

Theorem 8: Let $x(n)$ and $y(n)$ be in $\mathcal{S}_q$, and let $R_{xy}(k)$ be their circular cross-correlation, that is, $R_{xy}(k) = \sum_{n=0}^{q-1} x(n)y^*(n-k)$, where the shift is interpreted modulo q. Then $R_{xy}(k) \in \mathcal{S}_q$ as well. $\diamondsuit$

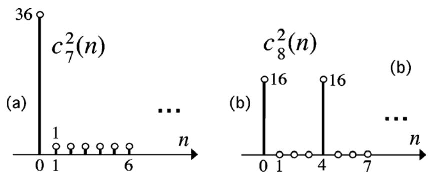


Fig. 3. (a), (b) Plots of $c_q^2(n)$ for $q = 7$ (a prime) and $q = 8 = 2^3$. Plots of $R_{qq}^2(l)$ are proportional to this.

Proof: Substituting $x(n) = \sum_{l=0}^{\phi(q)-1} \beta_l c_q(n-l)$ and $y(n) = \sum_{l=0}^{\phi(q)-1} \gamma_l c_q(n-l)$ in the expression for $R_{xy}(k)$ and simplifying, it follows that

$$\begin{aligned} R_{xy}(k) &= \sum_{n=0}^{q-1} x(n) y^*(n-k) \\ &= \sum_{l=0}^{\phi(q)-1} \sum_{i=0}^{\phi(q)-1} \beta_l \gamma_i^* \sum_{n=0}^{q-1} c_q(n-l) c_q^*(n-i-k) \\ &= q \sum_{l=0}^{\phi(q)-1} \sum_{i=0}^{\phi(q)-1} \beta_l \gamma_i^* c_q(k+i-l) \quad (\text{from } (56)) \end{aligned} \tag{58}$$

Since $s(k) \triangleq c_q(k+i-l)$ is a shifted version of $c_q(k)$, it belongs to the space $\mathcal{S}_q$. So $R_{xy}(k)$ is a linear combination of sequences in $\mathcal{S}_q$, which shows that $R_{xy}(k) \in \mathcal{S}_q$. $\bigtriangledown\bigtriangledown\bigtriangledown$

A. Concentration of Autocorrelation

Next consider the energy $\sum_{n=0}^{q-1} c_q^2(n)$. We proved in Section II-A that $\sum_{n=0}^{q-1} c_q^2(n) = q\phi(q)$. Since $c_q^2(0) = \phi^2(q)$, the "sidelobe" energy is

$$\sum_{n=1}^{q-1} c_q^2(n) = q\phi(q) - \phi^2(q) = \phi(q)(q - \phi(q)) \tag{59}$$

The significance is this: since the (circular) autocorrelation of $c_q(n)$ is proportional to $c_q(l)$, the ratio

$$\eta = \frac{\sum_{n=1}^{q-1} c_q^2(n)}{\sum_{n=0}^{q-1} c_q^2(n)} = \frac{q - \phi(q)}{q} = 1 - \frac{\phi(q)}{q} \tag{60}$$

determines the fraction of energy of autocorrelation which leaks into the nonzero lags. For example if q is prime, $\phi(q) = q-1$ and $\eta = 1/q$, whereas when q is highly composite as in $q = 2^m$, we have $\phi(q) = 2^{m-1}$ and $\eta = 1/2$. That is,

$$\eta = \begin{cases} 1/q & \text{if } q \text{ is prime,} \\ 1/2 & \text{if } q = 2^m \end{cases} \tag{61}$$

For prime q the leakage is small and for highly composite q the leakage is large. Fig. 3 shows examples of plots of $c_q^2(n)$ in $0 \le n \le q-1$ for prime q and power-of-two q. In fact, whenever q is even, we have $c_q(q/2) = -c_q(0)$ (see below) which shows that for all even $q > 2$, there is lot of leakage. This is a consequence of the following result proved in the Appendix).

Lemma 1: The Ramanujan sum $c_q(n)$ has $|c_q(n)| \le c_q(0) = \phi(q)$ for $0 \le n \le q-1$, and furthermore, $|c_q(n)| = c_q(0)$ if and only if q is even and $n = q/2$, in which case $c_q(q/2) = -c_q(0) = -\phi(q)$. $\diamondsuit$

Thus, among all even q, the leakage is least severe when q is a power of two. The leakage η is a useful parameter if $c_q(n)$ is used, for example as a transmitted pulse and the receiver uses a matched filter to extract the transmitted information.

B. Orthogonality of Columns of $\mathbf{C}_q$

From the autocorrelation result of Theorem 7, a number of useful properties of the matrix $\mathbf{C}_q$ can be derived. Since the inner product of any two columns of $\mathbf{C}_q$ (or those of the square matrix $\mathbf{B}_q$) is precisely the autocorrelation (56) (with $l =$ difference of column indices), we have

$$\mathbf{C}_q^T \mathbf{C}_q = q \begin{bmatrix} c_q(0) & c_q(1) & c_q(2) & \dots \\ c_q(1) & c_q(0) & c_q(1) & \dots \\ c_q(2) & c_q(1) & c_q(0) & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} \tag{62}$$

This is a $\phi(q) \times \phi(q)$, nonsingular and Toeplitz (but not circulant) matrix. It is clear that *columns i and $i+l$ of $\mathbf{C}_q$ are orthogonal if and only if $c_q(l) = 0$*. We now examine a number of cases:

1) *Prime q.* Since $c_q(n) = \phi(q)$ or -1 in this case, $c_q(n) \ne 0$ for any n. So no two columns of $\mathbf{C}_q$ (or $\mathbf{B}_q$) can be orthogonal when q is prime.
2) *Power-of-prime q.* As a second example suppose $q = p^m$ (power of prime), with $m > 1$. Then we know from Section II-A that $c_q(n) = 0$ if and only if n is not a multiple of p^{m-1}. For example with $q = 3^2 = 9$, $c_9(n) = 0$ if and only if n is not a multiple of 3:

$$c_9(n) = 6, 0, 0, -3, 0, 0, -3, 0, 0 \tag{63}$$

Indeed, any two columns of $\mathbf{C}_9$ (or $\mathbf{B}_9$) separated by $1, 2, 4, 5, 7,$ or 8 are therefore orthogonal. But columns i and $i+3$ (or i and $i+6$) are not orthogonal. More generally, $c_q(n)$ has the following form for $0 \le n \le q-1$:

$$(p-1)p^{m-1}, 0, \dots 0, -p^{m-1}, 0, \dots, 0, -p^{m-1}, 0, \dots$$

where the nonzero values $-p^{m-1}$ occur for $n = p^{m-1}, 2p^{m-1}, \dots$ Now when $q = p^m$, we have

$$\phi(q) = q\Big(1 - \frac{1}{p}\Big) = p^{m-1}(p-1) \tag{64}$$

So as l is incremented from 1 to $\phi(q)-1$, the quantity $c_q(l)$ will surely assume the nonzero value $-p^{m-1}$ at least once, if $p > 2$. Thus there will surely exist a pair of columns in $\mathbf{C}_q$ with a nonzero inner product. So the columns of $\mathbf{C}_q$ cannot be pairwise orthogonal for $q = p^m$ if $p > 2$.

Now consider $q = 2^m$, that is, q is a power of 2. From Section II-A we know that

$$c_q(n) = \begin{cases} 2^{m-1} & \text{for } n = 0 \\ -2^{m-1} & \text{for } n = q/2 = 2^{m-1} \\ 0 & \text{otherwise.} \end{cases} \tag{65}$$

in the fundamental range $0 \le n \le q-1$. For example

$$c_8(n) = 4, 0, 0, 0, -4, 0, 0, 0 \tag{66}$$

Since $\phi(m) = 2^{m-1}$ it follows in particular that when $q = 2^m$,

$$c_q(n) = 0 \quad \text{for} \quad 1 \leq n \leq \phi(q) - 1 \tag{67}$$

This implies that any pair of columns in $\mathbf{C}_q$ is orthogonal. For example, examine the columns of

$$\mathbf{C}_8 = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \\ -4 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \\ 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & -4 \end{bmatrix} \tag{68}$$

Since the nonzero elements in any two columns never overlap, it follows that columns are pairwise orthogonal. That is, the integer basis for $\mathcal{S}_q$, provided by the columns of $\mathbf{C}_q$, is an orthogonal basis. Summarizing, we have proved this:

Lemma 2: The $q \times \phi(q)$ matrix $\mathbf{C}_q$ has pairwise orthogonal columns, that is,

$$\mathbf{C}_q^T \mathbf{C}_q = \alpha \mathbf{I} \tag{69}$$

if q is a power of two, i.e., $q = 2^m$. Here $\alpha = \sum_{n=0}^{q-1} c_q^2(n) = q\phi(q) = 2^{2m-1}$. But if $q = p^m$ for some prime $p > 2$, then there is at least one pair of columns of $\mathbf{C}_q$ that is not orthogonal. $\diamondsuit$

VI. Periodicity Properties of Ramanujan Spaces

Strictly speaking, $x(n)$ is said to have period N if N is the *smallest* integer such that $x(n+N) = x(n)$ for all n. Usually when two periodic signals $x_1(n)$ and $x_2(n)$ are added, the period of the sum is assumed to be the lcm L of individual periods. But the period can actually be smaller. Thus, consider the example

$$\begin{aligned} x_1(n) &= \ldots\ 0,1,0,1,0,1,\ldots \quad (\text{period } 2) \\ x_2(n) &= \ldots\ 0,0,2,0,0,2,\ldots \quad (\text{period } 3) \\ x_1(n) + x_2(n) &= \ldots\ 0,1,2,1,0,3,\ldots \quad (\text{period } 6). \end{aligned}$$

Here the period of $x_1(n) + x_2(n)$ is $\text{lcm}\ (2,3) = 6$. But in the example

$$\begin{aligned} x_1(n) &= \ldots\ 0,1,0,1,0,1,\ldots \quad (\text{period } 2) \\ x_2(n) &= \ldots\ 1,0,1,0,1,0,\ldots \quad (\text{period } 2) \\ x_1(n) + x_2(n) &= \ldots\ 1,1,1,1,1,1,\ldots \quad (\text{period } 1), \end{aligned} \tag{70}$$

the period of $x_1(n) + x_2(n)$ is 1, which is a divisor of the $\text{lcm}\ (2,2) = 2$. We will see, however, that if we add signals belonging to Ramanujan spaces, the period of the result is exactly equal to the lcm of the periods of the components. This is a special property of Ramanujan spaces, and will be useful later when we develop the Ramanujan periodicity transform for arbitrary signals [21]. So we provide a systematic study here.

A. Basic Facts About Periodicity

First, we know that if a signal $x(n)$ has period N, then $x(n) = x(n+lN)$ for any integer l. The lemma below asserts that there cannot be any other repetition intervals, other than *multiples* of N.

Lemma 3: Let $x(n)$ be a sequence with period N. Suppose $x(n) = x(n+M)$ for all n, for some other integer M as well. Then $M = lN$ for some integer l. $\diamondsuit$

Proof: Since $x(n) = x(n+N) = x(n+M)$, we have

$$x(n) = x(n + i_1 N + i_2 M) \quad \forall n \tag{71}$$

for all integers i_1, i_2. Let $(N, M) = g$. Then there exist integers i_1, i_2 such that $i_1 N + i_2 M = g$ (Euclid's theorem [6], [19]). So, we also have

$$x(n) = x(n+g) \tag{72}$$

If $M \neq lN$ for integer l, then the gcd (M, N) has to be less than N, that is, $g < N$. But since (72) is true, this contradicts the fact that N is the period (smallest repetition interval). So $M = lN$. $\triangledown\triangledown\triangledown$

Lemma 4: Suppose

$$x(n) = \sum_{i=1}^{K} x_i(n) \tag{73}$$

where $x_i(n)$ has period N_i. Let $L = \text{lcm}\,(N_1, N_2, \ldots N_K)$. Then the period of $x(n)$ is a divisor of L. $\diamondsuit$

Proof: Since $x_i(n) = x_i(n+N_i)$, it follows that $x_i(n) = x_i(n+L)$ for each i. So $x(n) = x(n+L)$. If N is the actual period of $x(n)$, then from Lemma 3 it follows that $L = lN$ for some integer l. So N is a divisor of L. $\triangledown\triangledown\triangledown$

Note that the set of divisors of L includes 1 and L. So, depending on the situation, the period of the sum can be either the lcm L, or a divisor of L smaller than L.

B. Periodicity and Ramanujan Spaces

Given an arbitrary sum of the form

$$x(n) = \sum_{k=1}^{q} a_k W_q^{kn} \tag{74}$$

it is clear that $x(n) = x(n+q)$ because $W_q^{kn} = W_q^{k(n+q)}$ for each k. But the period of $x(n)$ can in general be q or a divisor $< q$. In this subsection we will prove the following result:

Theorem 9: Let $\{k_1, k_2, \ldots k_L\}$ be the set of k for which $a_k \neq 0$ in (74). Let

$$(k_1, k_2, \ldots k_L, q) = g. \tag{75}$$

Then the period of $x(n)$ is exactly q/g. In particular, $x(n)$ has period q if and only if

$$(k_1, k_2, \ldots k_L, q) = 1, \tag{76}$$

that is, there is no factor > 1 common to all k_i and q. $\diamondsuit$

Before we prove the theorem, we mention an immediate consequence:

Theorem 10: The Ramanujan sum

$$c_q(n) = \sum_{\substack{1\le k\le q\\(k,q)=1}} W_q^{-kn} \tag{77}$$

and more generally all the signals

$$x(n) = \sum_{l=0}^{\phi(q)-1} \beta_l c_q(n-l) = \sum_{\substack{1\le k\le q\\(k,q)=1}} \alpha_k W_q^{kn} \tag{78}$$

in the Ramanujan space $\mathcal{S}_q$ have period *exactly* equal to q. In particular, it cannot be *smaller* than q. ♢

Proof: In (77), and more generally in (78), we have $(k,q)=1$ for each k such that $a_k \neq 0$. So (76) is satisfied rather trivially. ▽ ▽ ▽

Some points worth noting:

1) Besides Ramanujan-space signals, there are many other examples where (76) is satisfied, such as (a) cases where the set $\{k_1, k_2, \ldots k_L\}$ includes $k_1 = 1$, (b) cases where there is a coprime pair k_i, k_l, and (c) the case where some k_i is coprime to q.
2) Consider the following sum (which is not a Ramanujan sum):

$$x(n) = W_6^{2n} + W_6^{3n}. \tag{79}$$

This is a case where $q=6, k_1=2$, and $k_2=3$. Since $(k_1,k_2,6)=1$, the period is indeed 6.

The following result is important for our discussion, especially in the proof of Theorem 9.

Theorem 11: Let $\{k_1, k_2, \ldots k_L\}$ be the set of k for which $a_k \neq 0$ in (74). Let N be a divisor of q so that q/N is an integer. Then $x(n) = x(n+N)$ if and only if every k_i is a multiple of q/N, that is,

$$k_i = l_i \frac{q}{N} \tag{80}$$

for some integer l_i. ♢

Proof: First assume $x(n) = x(n+N)$. We have

$$\sum_{k=1}^{q} a_k W_q^{k(n+N)} = \sum_{k=1}^{q} a_k W_q^{kn}, \quad \forall n \tag{81}$$

That is,

$$\sum_{k=1}^{q} W_q^{kn} a_k (1 - W_q^{kN}) = 0, \quad \forall n \tag{82}$$

With $\mathbf{W}$ denoting the $q\times q$ DFT matrix this can be rewritten as

$$\mathbf{W}\begin{bmatrix} 0 \\ a_1(1-W_q^N) \\ a_2(1-W_q^{2N}) \\ \vdots \\ a_{q-1}(1-W_q^{(q-1)N}) \end{bmatrix} = \mathbf{0} \tag{83}$$

Since $\mathbf{W}$ has rank q this is possible if and only if

$$a_k(1-W_q^{kN}) = 0, \quad \text{for } 1\le k\le q-1. \tag{84}$$

that is, if and only if $1 - W_q^{k_iN} = 0$ for $1 \le i \le L$. This happens if and only if $k_iN = l_iq$ for some integer l_i, which is equivalent to (80). Conversely if (80) holds then $W_q^{k_in} = W_q^{l_iqn/N} = W_N^{l_in}$ which shows that $x(n) = x(n+N)$. ▽ ▽ ▽

Proof of Theorem 9: We are now ready to prove Theorem 9. If the period $N < q$ (so $N|q$), then from Theorem 11 we know that $k_i = l_iM$. Here the integer $M = q/N > 1$ is a factor of q, so that $(k_1, k_2, \ldots k_L, q) \ge M > 1$. This shows that if (76) holds then $M=1$, that is, the period $N=q$. So, (76) is sufficient to ensure that the period is q. Next assume (76) is violated, that is, (75) holds for some $g>1$. Then

$$k_i = gl_i, \quad q = gr \tag{85}$$

for appropriate integers l_i and r. So we can rewrite $x(n)$ as

$$x(n) = \sum_{i=1}^{L} a_{k_i} W_q^{k_in} = \sum_{i=1}^{L} a_{k_i} W_r^{l_in} \tag{86}$$

where $(l_1, l_2, \ldots l_L, r) = 1$. But we just proved that if this holds then $x(n)$ has period exactly $r = q/g$. This completes the proof. ▽ ▽ ▽

C. Linear Combination of Ramanujan-Space Signals

Now consider a set of Ramanujan spaces $\mathcal{S}_{q_m}$, where q_m are positive integers. Let $x_m(n) \in \mathcal{S}_{q_m}$, that is,

$$x_m(n) = \sum_{l=0}^{\phi(q_m)-1} \beta_{ml} c_{q_m}(n-l) = \sum_{\substack{1\le k\le q_m\\(k,q_m)=1}} \alpha_{mk} W_{q_m}^{kn} \tag{87}$$

and define

$$x(n) = \sum_{m=1}^{K} x_m(n) \tag{88}$$

Also let

$$N = \mathrm{lcm}(q_1, q_2, \ldots, q_K) \tag{89}$$

We know from Lemma 4 that $x(n)$ has period equal to N or one of its divisors. We shall prove a stronger result, namely, that the period of the sum $x(n)$ is exactly equal to the lcm of the individual periods — it *cannot* be smaller. This is a special property enjoyed by any set of Ramanujan subspaces $\mathcal{S}_{q_m}$.

Theorem 12: With $x_m(n) \in \mathcal{S}_{q_m}$ where q_m are positive integers, the sum (88) has period exactly equal to N, assuming that none of the $x_m(n)$ is identically zero. ♢

Proof: Since $x_m(n)$ has period q_m, it is clear that $x(n) = x(n+N)$. Let N_a be the period of $x(n)$. So N_a is a divisor of N (Lemma 4), that is,

$$N = N_a N_b. \tag{90}$$

We only have to prove that $N_a = N$. First let us understand the implication of $x(n) = x(n + N_a)$: from (87) and (88) we have

$$x(n) = \sum_{m=1}^{K} \sum_{\substack{1 \le k \le q_m \\ (k,q_m)=1}} \alpha_{mk} W_{q_m}^{kn} \tag{91}$$

So, $x(n + N_a) = x(n)$ implies

$$\sum_{m=1}^{K} \sum_{\substack{1 \le k \le q_m \\ (k,q_m)=1}} \alpha_{mk} \Big(W_{q_m}^{kN_a} - 1 \Big) W_{q_m}^{kn} = 0 \tag{92}$$

for all n. But since $W_{q_m}^{kn} = W_q^{(\prod_{l \neq m} q_l)kn}$, where $q = \prod_m q_m$, the preceding is equivalent to

$$\sum_{m=1}^{K} \sum_{\substack{1 \le k \le q_m \\ (k,q_m)=1}} W_q^{(\prod_{l \neq m} q_l)kn} \alpha_{mk} \Big(W_{q_m}^{kN_a} - 1 \Big) = 0 \tag{93}$$

for all n. Notice that since $W_{q_m}^{k}$ are distinct for $1 \le k \le q_m$, the numbers $W_q^{(\prod_{l \neq m} q_l)k}$ are distinct for $1 \le k \le q_m$. Since $W_q^q = 1$, we only need to write (93) for $0 \le n \le q-1$. Thus (93) is satisfied if and only if

$$\mathbf{W}_q \Big(\sum_{m=1}^{K} \mathbf{v}_m \Big) = \mathbf{0} \tag{94}$$

where the row index is $0 \le n \le q-1$, and each $q \times 1$ vector $\mathbf{v}_m$ has possibly nonzero elements only at locations that are multiples of $\prod_{l \neq m} q_l$. Since $\mathbf{W}_q$ is nonsingular it follows that

$$\sum_{m=1}^{K} \mathbf{v}_m = \mathbf{0} \tag{95}$$

We now argue that the nonzero elements in any two vectors, say $\mathbf{v}_1$ and $\mathbf{v}_2$, do not overlap. Indeed, if there is such an overlap then

$$k_1 q_2 q_3 \ldots q_K = q_1 k_2 q_3 \ldots q_K \tag{96}$$

for some k_1, k_2. So $k_1/q_1 = k_2/q_2$. Since the q_i are distinct and since $(k_i, q_i) = 1$, this is not possible. This shows that the nonzero elements in the vectors $\mathbf{v}_m$ do not overlap. So (95) implies that $\mathbf{v}_m = \mathbf{0}$ for each m individually. Since the nonzero components of these vectors come from $\alpha_{mk}(W_{q_m}^{kN_a} - 1)$ (see (93)), it follows that

$$\alpha_{mk} \Big(W_{q_m}^{kN_a} - 1 \Big) = 0 \tag{97}$$

for each q_m, for all k such that $1 \le k \le q_m$ and $(k, q_m) = 1$. Now return to the goal which is to prove that $N_a = N$. Assume the contrary, namely $N_a < N$ and $N_b > 1$ in (90). Since N is the lcm of $\{q_i\}$ it then follows that there exists at least one q_i which is not a divisor of N_a. Say, q_1 is not a divisor of N_a. Now consider $W_{q_1}^{kN_a}$, where $(k, q_1) = 1$. Since k is coprime to q_1 and N_a not a multiple of q_1, it follows that

$$W_{q_1}^{kN_a} \neq 1 \tag{98}$$

But from (97)

$$\alpha_{1k} \Big(W_{q_1}^{kN_a} - 1 \Big) = 0 \tag{99}$$

which can only be satisfied if $\alpha_{1k} = 0$ for $(k, q_1) = 1$ (with $1 \le k \le q_1$). This is equivalent to saying that $x_1(n) = 0$ for all n (see (87)). But since none of the $x_m(n)$ is identically zero, this is impossible, which proves that $N_a = N$, i.e., the period of $x(n)$ is exactly N. $\triangledown\triangledown\triangledown$

D. Summary: Ramanujan Space $\mathcal{S}_q$ and Periodicity

As mentioned in Section II (after (10)), W_q^k is a primitive qth root of unity if and only if $(k, q) = 1$. In this case $W_q^{kn} = 1$ only when n is a multiple of q. Equivalently, $x(n) = W_q^{kn}$ has period q (and not less) if and only if $(k, q) = 1$. With this in mind, let us reexamine Ramanujan spaces.

1) The Ramanujan space $\mathcal{S}_q$ has signals of the form

$$x(n) = \sum_{\substack{1 \le k \le q \\ (k,q)=1}} \alpha_k W_q^{kn}. \tag{100}$$

The Ramanujan sum $c_q(n)$ is just one member in $\mathcal{S}_q$. *Each term* above has period q, and the sum also has period q (see Theorem 10). Notice also that the "frequencies" of the individual terms

$$\omega_k = \frac{2\pi k}{q} \tag{101}$$

are different from each other although the periods are all identical. So the Ramanujan space is a space of signals which can have $\phi(q)$ different frequency components W_q^{kn} (with $(k, q) = 1$), all with *the same period* q. Notice the departure from continuous-time, where two sinusoids $e^{j\omega_1 t}$ and $e^{j\omega_2 t}$ with different frequencies ω_1, ω_2 necessarily have different periods ($2\pi/\omega_1 \neq 2\pi/\omega_2$).

2) We know W_q^{kn} does not have any periodic components other than q (when $(k, q) = 1$). We can say that the Ramanujan space $\mathcal{S}_q$ is an extension of this idea. It is the linear space of *all* q-periodic signals $x(n)$ such that (a) each frequency component W_q^{kn} of $x(n)$ has period exactly q, and (b) signals in $\mathcal{S}_q$ *cannot* contain frequency components W_m^{kn} with periods less than q.

3) Any linear combination of signals in $\mathcal{S}_q$ also has period exactly q because $\mathcal{S}_q$ is a linear space. Thus adding two period-q signals from $\mathcal{S}_q$ does not change the period (unlike the example in (70)).

4) Finally, if we add signals from two or more Ramanujan spaces $\mathcal{S}_{q_i}$ (with each signal periodically extended for convenience), the result has period equal to the lcm of the q_i's. The period *cannot* be smaller (Theorem 12), unlike the example in (70).

5) Consider next a sum such as $y(n) = W_3^n + W_2^n$. Since we can rewrite $y(n) = W_6^{2n} + W_6^{3n}$ and since $\gcd(2, 3, 6) = 1$, it follows from Theorem 9 that $y(n)$ has period 6. The individual frequency components have different periods 2 and 3, and this signal does not belong to $\mathcal{S}_q$ for any q. It is a sum of signals from $\mathcal{S}_2$ and $\mathcal{S}_3$.

VII. Concluding Remarks

In this paper we reviewed Ramanujan sums, and introduced Ramanujan subspaces based on circulant matrices defined from Ramanujan sums. Several properties of these subspaces were analyzed in depth, such as the periodicity properties, correlation properties, and projection properties. The applications of these results in signal representation and in the identification of periodic components will be presented in the companion paper [21].

Appendix

Proof of (21) ($q =$ power of prime):

First note that $(p^m, k) = 1$ is equivalent to $(p, k) = 1$, so that

$$c_{p^m}(n) = \sum_{\substack{k=1\\(k,p)=1}}^{p^m} W_{p^m}^{kn} = \sum_{i=0}^{p^{m-1}-1} \sum_{\substack{l=1\\(l,p)=1}}^{p} W_{p^m}^{(ip+l)n} \tag{102}$$

where we have decomposed k as $k = ip + l$, and used the fact that $(k,p) = 1$ is equivalent to $(l,p) = 1$. We therefore have

$$c_{p^m}(n) = \left(\sum_{i=0}^{p^{m-1}-1} W_{p^{m-1}}^{in}\right)\left(\sum_{\substack{l=1\\(l,p)=1}}^{p} W_{p^m}^{ln}\right) \tag{103}$$

The first summation is

$$\sum_{i=0}^{p^{m-1}-1} W_{p^{m-1}}^{in} = \begin{cases} 0 & \text{if } p^{m-1} \nmid n \\ p^{m-1} & \text{if } p^{m-1} | n \end{cases} \tag{104}$$

So the second sum needs to be evaluated only when $n = p^{m-1}r$ for integer r, and its value is

$$\begin{aligned}\sum_{\substack{l=1\\(l,p)=1}}^{p} W_{p^m}^{lp^{m-1}r} &= \sum_{\substack{l=1\\(l,p)=1}}^{p} W_p^{lr} \\ &= c_p(r) = \begin{cases} p-1 & \text{if } p|r \\ -1 & \text{otherwise.}\end{cases}\end{aligned} \tag{105}$$

where $c_p(r)$ is the Ramanujan sequence for prime p (see (19)). Note that the condition "$p|r$" above is the same as $p^m|n$. Similarly, "otherwise" corresponds to "$p^{m-1}|n$ but $p^m \nmid n$". So, by combining (104) and (105) we arrive at (21).

Proof of Orthogonality ((15) and (16)):

Since $m = q_1 l_1 = q_2 l_2$ for some integers l_i, we can write

$$\sum_{n=0}^{m-1} W_{q_1}^{-k_1 n} W_{q_2}^{k_2 n} = \sum_{n=0}^{m-1} W_m^{(k_2 l_2 - k_1 l_1)n} \tag{106}$$

which is zero unless $k_2 l_2 - k_1 l_1 = \text{mul. of } m$. But since $1 \leq k_i < q_i$, we have $k_i l_i < m$, so $|k_2 l_2 - k_1 l_1| < m$, and (106) is zero unless $k_2 l_2 - k_1 l_1 = 0$, that is, $k_2 m/q_2 = k_1 m/q_1$ or equivalently $k_2/q_2 = k_1/q_1$. But since $(k_1, q_1) = (k_2, q_2) = 1$, this is not possible. This proves (16). The orthogonality property (15) follows immediately from (16). Thus

$$\begin{aligned}&\sum_{n=0}^{m-1} c_{q_1}(n) c_{q_2}(n-l) \\ &= \sum_{n=0}^{m-1} c_{q_1}(n) c_{q_2}^*(n-l) \\ &= \sum_{\substack{k_1=1\\(k_1,q_1)=1}}^{q_1} \sum_{\substack{k_2=1\\(k_2,q_2)=1}}^{q_2} W_{q_2}^{-k_2 l} \sum_{n=0}^{m-1} W_{q_1}^{-k_1 n} W_{q_2}^{k_2 n} = 0\end{aligned} \tag{107}$$

because the innermost sum is zero for $q_1 \neq q_2$.

Proof of Multiplicative Property (22):

We use the fact that Euler's totient function $\phi(q)$ is multiplicative (page 64, [6]), that is, $\phi(q_1 q_2) = \phi(q_1)\phi(q_2),$ if $(q_1, q_2) = 1$. We have

$$\begin{aligned}c_{q_1}(n) c_{q_2}(n) &= \sum_{\substack{k_1=1\\(k_1,q_1)=1}}^{q_1} \sum_{\substack{k_2=1\\(k_2,q_2)=1}}^{q_2} W_{q_1}^{-k_1 n} W_{q_2}^{k_2 n} \\ &= \sum_{\substack{k_1=1\\(k_1,q_1)=1}}^{q_1} \sum_{\substack{k_2=1\\(k_2,q_2)=1}}^{q_2} W_{q_1 q_2}^{(k_2 q_1 - k_1 q_2)n}\end{aligned} \tag{108}$$

In the above summations, k_1 takes on $\phi(q_1)$ values and k_2 takes $\phi(q_2)$ values. Thus, the double summation has $\phi(q_1)\phi(q_2) = \phi(q_1 q_2)$ terms. We now claim that these values of $k_2 q_1 - k_1 q_2$ are coprime to $q_1 q_2$. Assume this is not the case, that is, let $(k_2 q_1 - k_1 q_2, q_1 q_2) = g > 1$. Since g is a factor of $q_1 q_2$, it must be a factor of one of them, say q_1 (since $((q_1, q_2) = 1)$. Since g is also a factor of $k_2 q_1 - k_1 q_2$, it follows that the second term $k_1 q_2$ has the factor g. But since $(k_1, q_1) = (q_2, q_1) = 1$, this is a contradiction. Since the $\phi(q_1 q_2)$ values of $k_2 q_1 - k_1 q_2$ are coprime to $q_1 q_2$, we can indeed rewrite (108) as

$$c_{q_1}(n) c_{q_2}(n) = \sum_{\substack{k=1\\(k,q_1 q_2)=1}}^{q_1 q_2} W_{q_1 q_2}^{kn} = c_{q_1 q_2}(n) \tag{109}$$

Proof of Lemma 1:

First consider even q, and examine $c_q(q/2)$. Since $W_q^{q/2} = -1$, we have

$$c_q(q/2) = \sum_{\substack{1 \leq k \leq q\\(k,q)=1}} W_q^{kq/2} = \sum_{\substack{1 \leq k \leq q\\(k,q)=1}} (-1)^k \tag{110}$$

But since $(k, q) = 1$ and q is even, k has to be odd, so this reduces to $c_q(q/2) = -\phi(q)$. Thus, for any even q, we have $c_q(0) = -c_q(q/2) = \phi(q)$. Conversely, suppose $|c_q(n)| = c_q(0)$ for some n in $1 \leq n < q$. Then all the terms in the sum

$$c_q(n) = \sum_{\substack{1 \leq k \leq q\\(k,q)=1}} W_q^{kn} \tag{111}$$

are identical, that is $W_q^{(k_1-k_2)n} = 1$ for all k_1, k_2 such that $(k_i, q) = 1$. This implies $(k_1 - k_2)n = lq$ for integer l. That is, $(k_1 - k_2)/q = l/n$ for all k_1 and k_2 coprime to q (with l depending on k_1, k_2 of course). In particular this has to be true for $k_1 = q - 1$ and $k_2 = 1$ (which are both coprime to q) so that

$$\frac{q-2}{q} = \frac{l}{n} \tag{112}$$

This is possible for n in $1 \leq n < q$ only if q and $q - 2$ had a common factor > 1. But since q and $q-2$ differ by two the only possible common factor is 2, that is, $q = 2m, q-2 = 2(m-1)$. Thus q has to be even. $\triangledown \triangledown \triangledown$

ACKNOWLEDGMENT

The author wishes to thank Prof. B. Ramamurthi, Director of the Indian Institute of Technology, Chennai, for drawing my attention to [4] (and to [11], [12] via Dr. Gadiyar of the Vellore Institute of Technology). Subsequent enthusiastic remarks on this work from Dr. Gadiyar and Dr. Padma (VIT) are gratefully acknowledged.

REFERENCES

[1] T. M. Apostol, *Mathematical Analysis*. Dedham, MA, USA: Addison-Wesley, 1974.

[2] R. D. Carmichael, "Expansions of arithmetical functions in infinite series," in *Proc. London Math. Soc.*, 1932, pp. 1–26.

[3] N.-X. Chen, Z.-D. Chen, and Y.-C. Wei, "Multidimensional inverse lattice problem and a uniformly sampled arithmetic Fourier transform," *Phys. Rev. E*, vol. 55, no. 1, pp. R5–R8, Jan. 1997.

[4] H. G. Gadiyar and R. Padma, "Ramanujan-Fourier series, the Wiener-Khintchine formula, and the distribution of prime numbers," *Physica A*, vol. 269, pp. 503–510, 1999.

[5] G. H. Hardy, "Note on Ramanujan's trigonometrical function $c_q(n)$, and certain series of arithmetical functions," in *Proc. Cambridge Philosoph. Soc.*, 1921, vol. 20, pp. 263–71.

[6] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*. New York, NY, USA: Oxford Univ. Press, 2008.

[7] J. Maddox, "Möbius and problems of inversion," *Nature*, vol. 344, no. 29, p. 377, Mar. 1990.

[8] L. T. Mainardi, M. Bertinelli, and R. Sassi, "Analysis of T-wave alternans using the Ramanujan Transform," *Comput. Cardiol.*, vol. 35, pp. 605–608, 2008.

[9] A. V. Oppenheim and R. W. Schafer, *Discrete-Time Signal Processing*. Englewood Cliffs, NJ, USA: Prentice-Hall, 2010.

[10] S.-C. Pei and K.-W. Chang, "Odd Ramanujan sums of complex roots of unity," *IEEE Signal Process. Lett.*, vol. 14, pp. 20–23, Jan. 2007.

[11] M. Planat, "Ramanujan sums for signal processing of low frequency noise," in *Proc. IEEE Int. Freq. Contr. Symp. PDA Exhib.*, 2002, pp. 715–720.

[12] M. Planat, M. Minarovjech, and M. Saniga, "Ramanujan sums analysis of long-periodic sequenes and $1/f$ noise," *EPL J.*, vol. 85, pp. 40005: 1–5, 2009.

[13] S. Ramanujan, "On certain trigonometrical sums and their applications in the theory of numbers," *Trans. Cambridge Philosoph. Soc.*, vol. XXII, no. 13, pp. 259–276, 1918.

[14] S. Samadi, M. Omair Ahmad, and M. N. S. Swamy, "Ramanujan sums and discrete Fourier transforms," *IEEE Signal Process. Lett.*, vol. 12, pp. 293–296, Apr. 2005.

[15] W. A. Sethares and T. W. Staley, "Periodicity transforms," *IEEE Trans. Signal Process.*, vol. 47, pp. 2953–2964, Nov. 1999.

[16] M. R. Schroeder, "The unreasonable effectiveness of number theory in science and communication," *IEEE ASSP Mag.*, pp. 5–12, Jan. 1988.

[17] L. Sugavaneswaran, S. Xie, K. Umapathy, and S. Krishnan, "Time-frequency analysis via Ramanujan sums," *IEEE Signal Process. Lett.*, vol. 19, pp. 352–355, Jun. 2012.

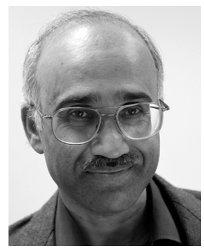
[18] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1993.

[19] P. P. Vaidyanathan, S.-M. Phoong, and Y.-P. Lin, *Signal Processing and Optimization for Transceiver Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[20] P. P. Vaidyanathan, "Ramanujan-sum expansions for finite duration (FIR) sequences," presented at the IEEE Int. Conf. on Acoust., Speech, Signal Process., Florence, Italy, 2014.

[21] P. P. Vaidyanathan, "Ramanujan sums in the context of signal processing—Part II: FIR representations and applications," *IEEE Trans. Signal Process.*, vol. 62, no. 16, pp. 4158–4172, 2014.

[22] Y. Zhang, "Bounded gap between primes," *Ann. Math.*, vol. 179, pp. 1121–1174, 2014.



P. P. Vaidyanathan (S'80–M'83–SM'88–F'91) was born in Calcutta, India, on October 16, 1954. He received the B.Sc. (Hons.) degree in physics and the B.Tech. and M.Tech. degrees in radiophysics and electronics, all from the University of Calcutta, in 1974, 1977, and 1979, respectively, and the Ph.D. degree in electrical and computer engineering from the University of California at Santa Barbara in 1982.

He was a postdoctoral fellow at the University of California, Santa Barbara, from September 1982 to March 1983. In March 1983, he joined the Electrical Engineering Department of the California Institute of Technology as an Assistant Professor, and since 1993, has been Professor of electrical engineering there. His main research interests are in digital signal processing, multirate systems, wavelet transforms, signal processing for digital communications, genomic signal processing, radar signal processing, and sparse array signal processing. He has authored more than 460 papers in journals and conferences, and is the author/coauthor of the four books *Multirate Systems and Filter Banks* (Englewood Cliffs, NJ: Prentice-Hall, 1993), *Linear Prediction Theory* (New York: Morgan and Claypool, 2008), and (with Phoong and Lin) *Signal Processing and Optimization for Transceiver Systems*, (Cambridge, U.K.: Cambridge University Press, 2010), and *Filter Bank Transceivers for OFDM and DMT Systems*(Cambridge, U.K.: Cambridge University Press, 2010). He has written several chapters for various signal processing handbooks.

Dr. Vaidyanathan served as Vice-Chairman of the Technical Program Committee for the 1983 IEEE International Symposium on Circuits and Systems, and as the Technical Program Chairman for the 1992 IEEE International Symposium on Circuits and Systems. He was an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS during 1985–1987, and is currently an Associate Editor for the IEEE SIGNAL PROCESSING LETTERS, and a Consulting Editor for the journal *Applied and Computational Harmonic Analysis*. He has been a Guest Editor in 1998 for Special Issues of the IEEE TRANSACTIONS ON SIGNAL PROCESSING and the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS II, on the topics of filter banks, wavelets and subband coders. He was a recipient of the Award for Excellence In Teaching at the California Institute of Technology for 1983–1984, 1992–1993, and 1993–1994. He also received the NSF's Presidential Young Investigator award in 1986. In 1989, he received the IEEE ASSP Senior Award for his paper on multirate perfect-reconstruction filter banks. In 1990, he was recipient of the S. K. Mitra Memorial Award from the Institute of Electronics and Telecommuncations Engineers, India, for his joint paper in the IETE journal. In 2009 he was chosen to receive the IETE students' journal award for his tutorial paper in the IETE *Journal of Education*. He was also the coauthor of a paper on linear-phase perfect reconstruction filter banks in the IEEE SP TRANSACTIONS, for which the first author (Truong Nguyen) received the Young Outstanding Author award in 1993. He received the 1995 F. E. Terman Award of the American Society for Engineering Education, sponsored by Hewlett Packard Co., for his contributions to engineering education. He has given several plenary talks including at the IEEE ISCAS-04, Sampta-01, Eusipco-98, SPCOM-95, and Asilomar-88 conferences on signal processing. He has been chosen a distinguished lecturer for the IEEE Signal Processing Society for 1996–1997. In 1999 he was chosen to receive the IEEE CAS Society's Golden Jubilee Medal. He is a recipient of the IEEE Signal Processing Society's Technical Achievement Award for 2002, and the IEEE Signal Processing Society's Education Award for 2012.