

A discrete Fourier kernel and Fraenkel's tiling conjecture

by

RON GRAHAM and KEVIN O'BRYANT (San Diego, CA)

1. Introduction. The result that drives this paper is

$$(1) \quad \sum_{n=1}^p e^{2\pi i \lfloor nq/p \rfloor / q} = \frac{1 - e^{2\pi i / q}}{1 - e^{2\pi i \bar{p} / q}},$$

where p and q are relatively prime positive integers and \bar{p} is the multiplicative inverse of $p \pmod q$. The LHS is complicated by the irregularity arising from the floor function, while the RHS is complicated by the presence of a modular inverse; therein lies the beauty and utility of (1).

Before stating the general result of which (1) is a special case (Theorem 1.1), we need to introduce some notation. We set $\omega := e^{2\pi i / q}$, and whenever the range of a summation is not written explicitly, it is to be taken over all of \mathbb{Z}_q , the integers modulo q :

$$\sum_x = \sum_{x \in \mathbb{Z}_q} = \sum_{x=1}^q = \sum_{x=0}^{q-1}.$$

We use the Fourier transform

$$\widehat{f}(j) := \sum_x f(x) \omega^{-jx}$$

($\widehat{f}(j)$ is called the j th Fourier coefficient), the Fourier inversion formula

$$\widehat{\widehat{f}}(x) = qf(x),$$

convolution

$$f * g(x) := \sum_y f(y)g(x - y)$$

2000 *Mathematics Subject Classification*: 42A16, 11B50, 11L99.

Key words and phrases: Beatty set, discrete Fourier transform, Fraenkel's Conjecture, perfect covering.

Research of the first-name author supported in part by grant CCR-0310991.

The second-name author is a National Science Foundation Mathematical Sciences Postdoctoral Fellow, NSF grant DMS-0202460.

and the interchange-of-summations result

$$\widehat{f * g}(j) = \widehat{f}(j)\widehat{g}(j).$$

Also, let

$$\llbracket P \rrbracket R := \begin{cases} 0 & \text{if } P \text{ is False,} \\ R & \text{if } P \text{ is True.} \end{cases}$$

Note that $\llbracket \text{False} \rrbracket R$ is defined even if R is not. When $R = 1$, we omit it from the notation. We also adopt the common practice of identifying a multiset with its indicator function, i.e., $S(x)$ is the multiplicity of x in the multiset S .

We distinguish the rational Beatty sets (p, q are any integers, and r any real number)

$$\mathcal{B}_{p,r}^q := \left\{ \left\lfloor n \frac{q}{p} + r \right\rfloor : n \in \mathbb{Z} \right\}.$$

Usually, q will be fixed and in this situation we omit it from the notation. We will always assume that r is an integer ⁽¹⁾, and when $r = 0$ we omit it from our notation. Note that the density of the set $\mathcal{B}_{p,r}^q$ is p/q .

Note that $\mathcal{B}_{p,r}^q$ consists of p congruence classes modulo q , and so $\mathcal{B}_{p,r}^q$ is naturally considered as a subset of \mathbb{Z}_q . If the p points were perfectly evenly distributed around \mathbb{Z}_q (as happens if $q/p \in \mathbb{Z}$), then the Fourier transform would be 0 except at multiples of the difference between points. Thus, one naturally expects that $\mathcal{B}_p(j)$ will be small except when jq/p is near an integer. This is confirmed by Figure 1, which shows the Fourier transform of \mathcal{B}_{24}^{121} , and Figures 2 and 3, which show $|\widehat{\mathcal{B}_{p,r}^q}(1)|$ for small relatively prime p, q (r is irrelevant). Theorem 1.1 gives an explicit formula for $\widehat{\mathcal{B}_{p,r}^q}$ which quantifies the validity of this expectation.

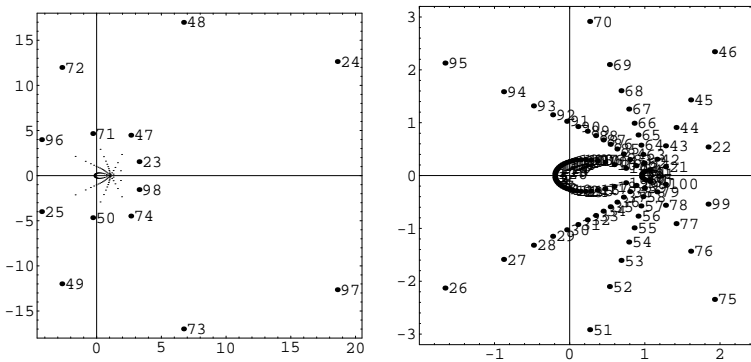


Fig. 1. The points $\widehat{\mathcal{B}_{24}^{121}}(j)$ ($1 \leq j \leq 120$), shown in the complex plane and labeled by j . The left graph shows all 120 points. The right graph, which resembles a spider, shows only those closest to 1.

⁽¹⁾ This is no loss of generality: if n_0 is a value of n for which the fractional part $\{nq/p + r\}$ is minimal, then $\mathcal{B}_{p,r}^q = \mathcal{B}_{p, \lfloor n_0q/p+r \rfloor}^q$.

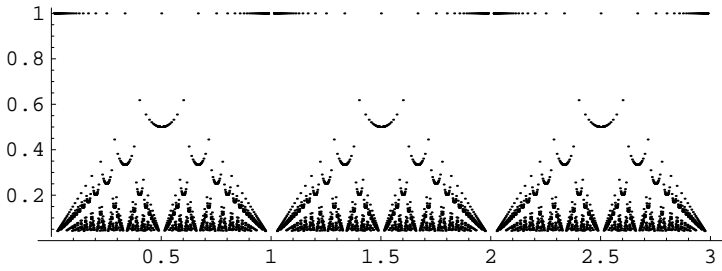


Fig. 2. The points $(p/q, |\widehat{\mathcal{B}}_p^q(1)|)$ for $\gcd(p, q) = 1$, $0 < p < 3q$, and $1 \leq q \leq 75$

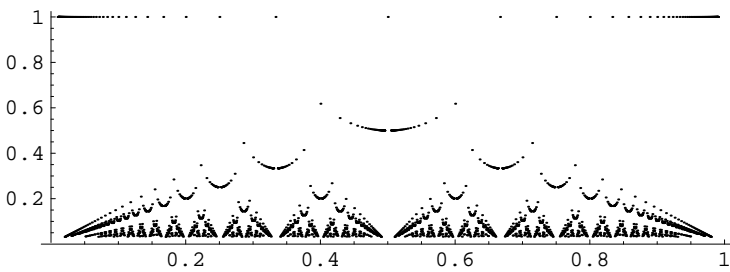


Fig. 3. The points $(p/q, |\widehat{\mathcal{B}}_p^q(1)|)$ for $\gcd(p, q) = 1$, $0 < p < q$, $1 < q \leq 100$

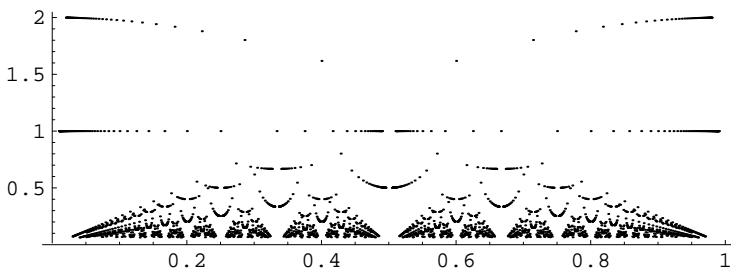


Fig. 4. The points $(p/q, |\widehat{\mathcal{B}}_p^q(2)|)$ for $\gcd(p, q) = 1$, $0 < p < q$, $2 < q \leq 100$

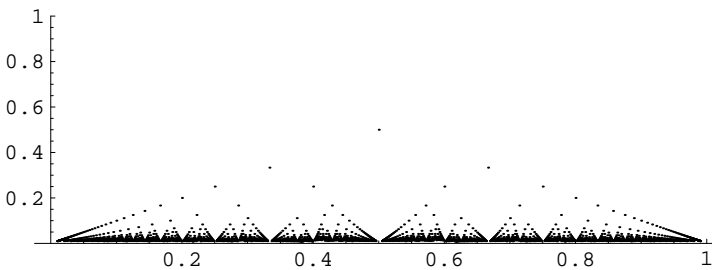


Fig. 5. The points $(p/q, \prod_{i=1}^n |a_i|)$, where $[a_0; a_1, \dots, a_n]$ is the NICF of p/q

THEOREM 1.1. *Let $p \neq 0, q > 1$ be integers with $g := \gcd(p, q)$, let \bar{p} satisfy $p\bar{p} \equiv g \pmod{q}$, and let r be any integer. Then*

$$\widehat{\mathcal{B}}_{p,r}^q(0) = p,$$

and for $j \not\equiv 0 \pmod{q}$,

$$\widehat{\mathcal{B}}_{p,r}^q(j) = \llbracket g \mid j \rrbracket g \frac{1 - \omega^j}{1 - \omega^{j\bar{p}}} \omega^{-jr}, \quad |\widehat{\mathcal{B}}_{p,r}^q(j)| = \llbracket g \mid j \rrbracket g \left| \frac{\sin(\pi j/q)}{\sin(\pi j\bar{p}/q)} \right|.$$

Figure 2 shows $|\widehat{\mathcal{B}}_p^q(1)|$ for relatively prime p and q with $0 < p < 3q$ and $1 < q \leq 75$. Figures 3 and 4 show the first and second coefficients when p and q are relatively prime, $0 < p < q$, and $q \leq 100$. There are three symmetries visible to the naked eye. The first (from Figure 2) is that $|\widehat{\mathcal{B}}_{p+q}^q| = |\widehat{\mathcal{B}}_p^q|$. In other words, the function $|\widehat{\mathcal{B}}_x^q(j)|$ is periodic with period q . This is a consequence of the fact $\mathcal{B}_{p+q}^q(x) = 1 + \mathcal{B}_p^q(x)$, which we prove along the way to proving Theorem 1.1.

The second is that

$$|\widehat{\mathcal{B}}_p^q(j)| = |\widehat{\mathcal{B}}_{q-p}^q(j)|,$$

which is seen in the pictures as a symmetry about $1/2$. This is a consequence of a theorem of Fraenkel (Corollary 1.2 below) which states that the complement of a rational Beatty set is a rational Beatty set. We give a new proof of this in Section 3.

The third symmetry is that the graphs on $[1/4, 1/3]$, on $[1/3, 1/2]$, etc., seem to be quite similar. This is essentially the symmetry of the continued-fraction map $x \mapsto 1/x \pmod{1}$. For each rational p/q , there is a unique finite sequence $[a_0; a_1, \dots, a_n]$ of integers with the properties: for $i > 0$, $|a_i| \geq 2$; for $0 < i < n$, if $a_i = \pm 2$ then $a_i a_{i+1}$ is positive; $a_n \neq -2$; and

$$\frac{p}{q} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_n}}}.$$

This is the nearest-integer continued fraction (commonly abbreviated NICF). Compare Figure 3 with Figure 5, which shows the points $(\frac{p}{q}, \prod_{i=1}^n |a_i|)$: the points in Figure 5 are located precisely at the bottom of the “cups” in Figure 3.

We remark that while (1) connects Beatty sequences with density p/q directly to the inverse of p modulo q , the direct connection between both objects and continued fractions is well studied. We also note that the inverse of p modulo q has arisen independently in the recent work of Simpson [7], in which he uses generating functions to prove necessary and sufficient conditions for two rational Beatty sequences not to intersect.

The main result in the study of Beatty sequences was discovered by Lord Rayleigh: If α is irrational and $1/\alpha + 1/\beta = 1$, then the sets $\{\lfloor n\alpha \rfloor : n \geq 1\}$, $\{\lfloor n\beta \rfloor : n \geq 1\}$ partition \mathbb{Z}^+ . In the 1950s Skolem extended this to non-homogeneous sets, and in 1969 Fraenkel corrected Skolem's work and extended it to include rational α . We direct the reader to [5] for the general rational/irrational statement, an elementary proof, and the history of Fraenkel's Partition Theorem. The rational case (Corollary 1.2) is an easy consequence of Theorem 1.1.

COROLLARY 1.2 (Fraenkel's Partition Theorem, rational case). *The sets \mathcal{B}_{p_1, r_1}^q and \mathcal{B}_{p_2, r_2}^q , where q, p_k, r_k are integers, partition \mathbb{Z} if and only if $p_1 + p_2 = q$ and*

$$p_1 r_1 + p_2 r_2 \equiv -\gcd(p_1, q) \pmod{q}.$$

Attempts to extend this to more than two sequences have had some success, but a general statement remains elusive. In the early 1970s (see [1, 2]), Fraenkel was led to conjecture that there was essentially only one way to partition \mathbb{Z} into Beatty sets with distinct densities.

CONJECTURE 1.3 (Fraenkel's Conjecture). *If the sets*

$$\{\lfloor n\alpha_1 + r_1 \rfloor : n \in \mathbb{Z}\}, \{\lfloor n\alpha_2 + r_2 \rfloor : n \in \mathbb{Z}\}, \dots, \{\lfloor n\alpha_m + r_m \rfloor : n \in \mathbb{Z}\}$$

partition \mathbb{Z} , $m \geq 3$, and $1 < \alpha_1 < \alpha_2 < \dots < \alpha_m$, then $\alpha_k = 2^k - 2^{k-m}$.

The conjecture has been proven in case any α is irrational (see [3]), $\alpha_1 \leq 1.5$ (see [6]), or $m \leq 6$ (see [8]), and in several other less-easily-stated circumstances. The article [9] of R. Tijdeman contains an excellent survey of the progress on Fraenkel's Conjecture.

We offer a stronger conjecture, and will apply Theorem 1.1 to prove some special cases. We say that sets S_1, \dots, S_m are a *perfect c -fold covering of \mathbb{Z}* if $S_1(x) + \dots + S_m(x) = c$ for all $x \in \mathbb{Z}$, and simply that they are a *perfect covering* if we do not wish to specify c .

CONJECTURE 1.4 (Covering Fraenkel Conjecture). *Let $q, m \geq 3$, and let p_1, \dots, p_m be distinct integers with $0 < p_k < q$, $\gcd(q, p_1, \dots, p_m) = 1$, and with no proper subset $I \subsetneq [m]$ having $\sum_{i \in I} p_i \equiv 0 \pmod{q}$. Let r_1, \dots, r_m be arbitrary integers. The sets \mathcal{B}_{p_k, r_k}^q ($1 \leq k \leq m$) are a perfect covering if and only if:*

- (i) q is odd, and m is the order of 2 modulo q ;
- (ii) the sets can be renumbered so that there are integers δ (relatively prime to q with modular inverse $\bar{\delta}$) and γ such that for $1 \leq k \leq m$,

$$p_k \equiv \delta 2^{m-k} \pmod{q} \quad \text{and} \quad r_k \equiv \gamma - \bar{\delta} 2^{k-1} \pmod{q}.$$

This is admittedly not as pithy as Fraenkel’s Conjecture, but we hope that its greater generality will shed new light on an old problem. Since $\mathcal{B}_{p,r}^q(x) = 1 + \mathcal{B}_{p+q,r}^q(x)$, we may assume without loss of generality that $p_k < q$. We use Theorem 1.1 to prove the “if” claim of the CFC, and in fact we show that if the covering (with all $p_k < q$) is a perfect c -fold covering, then c is the number of ones in the binary expansion of $\delta(2^m - 1)/q$. We prove the “only if” part of the CFC under the additional hypothesis that $m \leq 5$, and also under the additional hypotheses that $\gcd(q, p_k) = 1$ for some k and that q is sufficiently large.

We suspect that if $m \geq 3$, sequences $S(\alpha_k, \beta_k) = \{ \lfloor n\alpha_k + \beta_k \rfloor : n \in \mathbb{Z} \}$ are a perfect covering and some α_k is irrational, then two of the α_k ’s are in fact equal. Graham’s proof [3] of this in the 1-covering case does not extend easily to multiple coverings. We have not investigated this further, and at any rate this guess does not fall within the scope of the present article.

We will use the following consequence of Theorem 1.1 several times.

COROLLARY 1.5 (Covering Criterion). *The sequences \mathcal{B}_{p_k,r_k}^q ($1 \leq k \leq m$) are a perfect c -fold covering of \mathbb{Z} if and only if*

$$cq = \sum_{k=1}^m p_k$$

and for $1 \leq j < q$ (with $g_k = \gcd(p_k, q)$),

$$0 = \sum_{k=1}^m \llbracket g_k \mid j \rrbracket g_k \frac{\omega^{-jr_k}}{1 - \omega^{j\overline{p}_k}}.$$

2. Proof of Theorem 1.1. We will give a kernel function $K(x)$, whose transform we can compute, such that

$$(2) \quad \mathcal{B}_{p,r}^q * K(x) = R(x),$$

where $R(x)$ will also have an easily computed transform. Taking the Fourier transform of this equation gives $\widehat{\mathcal{B}_{p,r}^q}(j)\widehat{K}(j) = \widehat{R}(j)$, which is the same as $\widehat{\mathcal{B}_{p,r}^q}(j) = \widehat{R}(j)(\widehat{K}(j))^{-1}$. The zeroth coefficient can be dealt with immediately, and thereafter we demonstrate that we may assume that $r = 0$, that $\gcd(p, q) = 1$, and that $0 < p < q$. Then we define K and R , show that (2) holds, and compute the transforms of R and K to complete the proof.

We have

$$\widehat{\mathcal{B}_{p,r}^q}(j) := \sum_x \mathcal{B}_{p,r}^q(x)\omega^{-jx} = \sum_{n=0}^{p-1} \omega^{-j\lfloor nq/p+r \rfloor}.$$

For $j = 0$, this gives the first claim of Theorem 1.1: $\widehat{\mathcal{B}_{p,r}^q}(0) = p$.

Since we assume that r is an integer, we also have

$$\widehat{\mathcal{B}}_{p,r}^q(j) = \sum_{n=0}^{p-1} \omega^{-j\lfloor nq/p+r \rfloor} = \sum_{n=0}^{p-1} \omega^{-j\lfloor nq/p \rfloor - jr} = \omega^{-jr} \widehat{\mathcal{B}}_{p,0}^q(j).$$

Thus, it is sufficient to work with $r = 0$.

Now we wish to show that we may take p and q to be relatively prime. If $S: \mathbb{Z} \rightarrow \mathbb{C}$ is periodic with period l , and S_l and S_{kl} are the induced functions on \mathbb{Z}_l and \mathbb{Z}_{kl} , then

$$\widehat{S}_{kl}(j) = k\llbracket k \mid j \rrbracket \widehat{S}_l(j/k).$$

Thus, if $ga = p$ and $gb = q$ with $\gcd(a, b) = 1$, then

$$\widehat{\mathcal{B}}_p^q(j) = g\llbracket g \mid j \rrbracket \widehat{\mathcal{B}}_a^b(j/g).$$

If we assume for the moment that we have proved Theorem 1.1 in the relatively prime case, then we have

$$\widehat{\mathcal{B}}_p^q(j) = g\llbracket g \mid j \rrbracket \frac{1 - (e^{2\pi i/b})^{j/g}}{1 - (e^{2\pi i\bar{a}/b})^{j/g}} = g\llbracket g \mid j \rrbracket \frac{1 - (e^{2\pi i/(bg)})^j}{1 - (e^{2\pi i\bar{a}/(bg)})^j} = g\llbracket g \mid j \rrbracket \frac{1 - \omega^j}{1 - \omega^{j\bar{a}}}$$

where $\omega = e^{2\pi i/q}$ and \bar{a} , the inverse of $a = p/g$ modulo $b = q/g$, satisfies $p\bar{a} \equiv g \pmod{q}$. Thus, it is sufficient to work with relatively prime p and q .

We may assume that $0 < p < q$ since

$$(3) \quad \mathcal{B}_{p+q}^q(x) = 1 + \mathcal{B}_p^q(x),$$

and so the Fourier coefficients (except the zeroth) are sensitive only to $p \pmod{q}$. To see (3), observe that the function $\mathcal{B}_p^q(x)$ takes on only the values $\lfloor p/q \rfloor$ and $\lceil p/q \rceil$. Moreover, $\mathcal{B}_p^q(x) = \beta$ (with $\beta = \lceil p/q \rceil$) if and only if there is an integer n with $x \leq nq/p < (n + \beta - 1)q/p < x + 1$, which is equivalent to

$$x \frac{p}{q} \leq n < (x + 1) \frac{p}{q} - (\beta - 1) = x \frac{p}{q} + \frac{p}{q} - \beta + 1.$$

This happens if and only if the fractional part $\{xp/q\}$ is 0 or is strictly larger than $\beta - p/q = 1 - \{p/q\}$. Thus, the property $\mathcal{B}_p^q(x) = \lceil p/q \rceil$ can be described entirely in terms of the fractional part $\{xp/q\}$, which depends only on $p \pmod{q}$.

Now, we take K to be the set $\{1 - \bar{p}, 2 - \bar{p}, \dots, 0\} = (-\bar{p}, 0]$, and set $R(x) := |\mathcal{B}_p \cap [x, x + \bar{p})|$.

We use the following two properties of the Beatty set \mathcal{B}_p (with $0 < p < q$). We call the first property ‘‘duality’’: an integer k is in \mathcal{B}_p if and only if the fractional part of kp/q is 0 or strictly greater than $1 - p/q$. To prove this, simply observe that $k \in \mathcal{B}_p$ if there is an integer n with $k \leq nq/p < k + 1$, which we rearrange as $kp/q \leq n < kp/q + p/q$. This

happens exactly if the fractional part of kp/q is 0 or strictly greater than $1 - p/q$. The second property is called “balance”: for all real numbers $x < y$, the number $|\mathcal{B}_p \cap [x, y)|$ is either $\lfloor (y - x)p/q \rfloor$ or $\lceil (y - x)p/q \rceil$. To prove this, observe that we are counting the integers n with $x \leq nq/p < y$, which is equivalent to $xp/q \leq n < yp/q$. Since we only care about integral n , we can write this as $\lceil xp/q \rceil \leq n < \lceil yp/q \rceil$. Clearly there are $\lceil yp/q \rceil - \lceil xp/q \rceil$ such n , and this is

$$\left\lceil \frac{yp}{q} \right\rceil - \left\lceil \frac{xp}{q} \right\rceil = \left(\frac{yp}{q} + \varepsilon_1 \right) - \left(\frac{xp}{q} + \varepsilon_2 \right) = (y - x) \frac{p}{q} + \varepsilon_1 - \varepsilon_2,$$

where the ε 's are both in $[0, 1)$. It follows that the true value is an integer which is strictly less than 1 away from $(y - x)p/q$, i.e., either $\lfloor (y - x)p/q \rfloor$ or $\lceil (y - x)p/q \rceil$.

We will show that

$$(4) \quad R(x) = \lfloor \bar{p}p/q \rfloor + \llbracket x = 0 \rrbracket,$$

but first we show that $R(0) > R(1)$. Since $R(0)$ counts the number of elements of $\mathcal{B}_p = \{ \lfloor nq/p \rfloor \bmod q : 1 \leq n \leq p \}$ in $[0, \bar{p})$ and $R(1)$ counts those in $[1, \bar{p}]$, we need to show that $0 \in \mathcal{B}_p$ and $\bar{p} \notin \mathcal{B}_p$. Obviously $\lfloor pq/p \rfloor \equiv 0 \pmod{q}$, so the substance here is that $\bar{p} \notin \mathcal{B}_p$. By duality, $\bar{p} \in \mathcal{B}_p$ if and only if the fractional part of $\bar{p}p/q$ is 0 or strictly greater than $1 - p/q$. Since $p\bar{p} \equiv 1 \pmod{q}$, the fractional part of $\bar{p}p/q$ is $1/q$, which is neither 0 nor strictly greater than $1 - p/q$ (because p, q are relatively prime).

We now show (4) by evaluating $\sum_x R(x)$ in two ways. First, every $y \in \mathcal{B}_p$ contributes to $R(y), R(y - 1), \dots, R(y - \bar{p} + 1)$. Thus

$$(5) \quad \sum_x R(x) = |\mathcal{B}_p| \bar{p} = p\bar{p}.$$

Second, by the balance property of Beatty sets, we know that $R(x)$ is either $\lfloor \bar{p}p/q \rfloor$ or $\lceil \bar{p}p/q \rceil = \lfloor \bar{p}p/q \rfloor + 1$, and in particular $|R^{-1}(\lfloor \bar{p}p/q \rfloor)| + |R^{-1}(\lfloor \bar{p}p/q \rfloor + 1)| = q$. Thus

$$(6) \quad \begin{aligned} \sum_x R(x) &= |R^{-1}(\lfloor \bar{p}p/q \rfloor)| \lfloor \bar{p}p/q \rfloor + |R^{-1}(\lfloor \bar{p}p/q \rfloor + 1)| (\lfloor \bar{p}p/q \rfloor + 1) \\ &= q \lfloor \bar{p}p/q \rfloor + |R^{-1}(\lfloor \bar{p}p/q \rfloor + 1)|. \end{aligned}$$

Reducing (5) and (6) modulo q tells us that $|R^{-1}(\lfloor \bar{p}p/q \rfloor + 1)| = 1$. Since $R(0) > R(1)$, we know that $R^{-1}(\lfloor \bar{p}p/q \rfloor + 1) = \{0\}$, whence (4).

Theorem 1.1 now follows from the straightforward calculations (for $j \not\equiv 0 \pmod{q}$)

$$\widehat{K}(j) = \frac{1 - \omega^{j\bar{p}}}{1 - \omega^j}, \quad \widehat{R}(j) = 1$$

and

$$\begin{aligned} \mathcal{B}_p * K(x) &:= \sum_y \mathcal{B}_p(y)K(x - y) = \sum_y \llbracket y \in \mathcal{B}_p \rrbracket \llbracket -\bar{p} < x - y \leq 0 \rrbracket \\ &= \sum_y \llbracket y \in \mathcal{B}_p \rrbracket \llbracket y \in [x, x + \bar{p}] \rrbracket = |\mathcal{B}_p \cap [x, x + \bar{p}]| = R(x). \end{aligned}$$

2.1. An interesting variation. There is another interesting way to finish the proof of Theorem 1.1. It plays on another expression of the “balance” property of Beatty sets: for fixed t , the difference $\lfloor (n + t)q/p \rfloor - \lfloor nq/p \rfloor$ is either $\lfloor tq/p \rfloor$ or $\lceil tq/p \rceil$.

Assume that $j \not\equiv 0 \pmod{q}$, $r = 0$, and $p < q$ are relatively prime and positive.

Let \bar{q} be the inverse of q modulo p , and let \bar{p} be the inverse of p modulo q . We will use the identity

$$\lfloor \bar{q}\bar{q}/p \rfloor = (q\bar{q} - 1)/p \equiv -\bar{p} \pmod{q}.$$

Set $b(n) := \lfloor nq/p \rfloor$, and

$$\Delta(n) := b(n) - b(n - \bar{q}).$$

We compute $\sum_{n=0}^{p-1} \Delta(n)$ in two ways. First, the sum telescopes to

$$\begin{aligned} \sum_{n=0}^{p-1} \Delta(n) &= \sum_{n=p-\bar{q}}^{p-1} b(n) - \sum_{n=-\bar{q}}^{-1} b(n) = \sum_{n=-\bar{q}}^{-1} b(n+p) - \sum_{n=-\bar{q}}^{-1} b(n) \\ &= \sum_{n=-\bar{q}}^{-1} (q + b(n)) - \sum_{n=-\bar{q}}^{-1} b(n) = \bar{q}q. \end{aligned}$$

Second, note that $\Delta(n)$ is either $a := \lfloor \bar{q}q/p \rfloor$ or $a + 1 = \lceil \bar{q}q/p \rceil$, say there are β integers n inclusively between 0 and $p - 1$ with $\Delta(n) = a + 1$, and $p - \beta$ integers n with $\Delta(n) = a$. We have

$$\sum_{n=0}^{p-1} \Delta(n) = \beta(a + 1) + (p - \beta)a = \beta + pa.$$

Equating these two evaluations modulo p (and using $0 \leq \beta \leq p$), we find that $\beta = 1$. By direct arithmetic, $\Delta(0) = \lceil \bar{q}q/p \rceil$, and so for $x \not\equiv 0 \pmod{p}$, $\Delta(x) = \lfloor \bar{q}q/p \rfloor$.

We now use this information directly (set $\gamma = \omega^{-j}$):

$$\begin{aligned} \widehat{\mathcal{B}}_p(j) &= \sum_{n=1}^p \gamma^{\lfloor nq/p \rfloor} = 1 + \sum_{n=1}^{p-1} \gamma^{b(n)} = 1 + \sum_{n=1}^{p-1} \gamma^{b(n)} \gamma^{b(n-\bar{q})-b(n)} \gamma^{\lfloor \bar{q}q/p \rfloor} \\ &= 1 + \gamma^{\lfloor \bar{q}q/p \rfloor} \sum_{n=1}^{p-1} \gamma^{b(n-\bar{q})} = 1 + \gamma^{\lfloor \bar{q}q/p \rfloor} \left(\left(\sum_{n=1}^p \gamma^{b(n-\bar{q})} \right) - \gamma^{b(p-\bar{q})} \right) \\ &= 1 + \gamma^{\lfloor \bar{q}q/p \rfloor} (\widehat{\mathcal{B}}_p(j) - \gamma^{-\lfloor \bar{q}q/p \rfloor}). \end{aligned}$$

Solving this equation yields

$$\widehat{\mathcal{B}}_p(j) = \frac{1 - \gamma^{-1}}{1 - \gamma^{\lfloor \bar{q}q/p \rfloor}} = \frac{1 - \omega^j}{1 - \omega^{-j \lfloor \bar{q}q/p \rfloor}} = \frac{1 - \omega^j}{1 - \omega^{j\bar{p}}}$$

3. Proof of Fraenkel’s Partition Theorem. By Corollary 1.5, we can assume that $p_1 + p_2 = q$; we need only show that

$$(7) \quad 0 = \llbracket g_1 \mid j \rrbracket g_1 \frac{\omega^{-jr_1}}{1 - \omega^{j\bar{p}_1}} + \llbracket g_2 \mid j \rrbracket g_2 \frac{\omega^{-jr_2}}{1 - \omega^{j\bar{p}_2}}$$

is satisfied for $1 \leq j < q$ if and only if $p_1r_1 + p_2r_2 \equiv -g_1 \pmod{q}$.

We first assume that (7) holds for all $j \in [1, q]$. In particular, we set $j = p_1$. Since $p_1 + p_2 = q$, we have $g_1 = g_2$, $g_1 \mid j$, and (7) simplifies to

$$\frac{\omega^{-p_1r_1}}{1 - \omega^{p_1\bar{p}_1}} + \frac{\omega^{-p_1r_2}}{1 - \omega^{p_1\bar{p}_2}} = 0.$$

Rearranging this gives

$$(8) \quad \frac{\omega^{-p_1r_2}}{\omega^{-p_1r_1}} = -\frac{1 - \omega^{p_1\bar{p}_2}}{1 - \omega^{p_1\bar{p}_1}}.$$

Since $-p_1 \equiv p_2 \pmod{q}$, $p_1\bar{p}_1 \equiv g_1 \pmod{q}$, and $p_1\bar{p}_2 \equiv -p_1\bar{p}_1 \pmod{q}$, equality (8) becomes

$$\omega^{p_2r_2 + p_1r_1} = \frac{\omega^{-p_1r_2}}{\omega^{-p_1r_1}} = -\frac{1 - \omega^{-g_1}}{1 - \omega^{g_1}} = \omega^{-g_1},$$

whence $p_2r_2 + p_1r_1 \equiv -g_1 \pmod{q}$. We can read this argument from the bottom up to see the other half of “if and only if”.

4. Fraenkel’s Covering Conjecture

4.1. Constructions

LEMMA 4.1. *If $q \geq 3$, $2^m \equiv 1 \pmod{q}$, $p_k \equiv 2^{m-k} \pmod{q}$, and $r_k \equiv -2^{k-1} \pmod{q}$, then $\mathcal{B}_{p_k, r_k} (1 \leq k \leq m)$ is a perfect covering.*

Proof. We have

$$\sum_{k=1}^m p_k \equiv \sum_{k=1}^m 2^{m-k} = 2^m - 1 \equiv 0 \pmod{q}$$

so the first equation of the Covering Criterion is satisfied for some c . Our hypotheses imply that $\gcd(p_k, q) = 1$ and $\bar{p}_k \equiv 2^k \pmod{q}$, so we need only show that

$$(9) \quad 0 = \sum_{k=1}^m \frac{\omega^{-r_k}}{1 - \omega^{\bar{p}_k}} = -\sum_{k=1}^m \frac{\omega^{2^{k-1}}}{1 - \omega^{2^k}}$$

holds for ω any q th root of unity except 1.

Since $1 - \omega^{2^k} = (1 - \omega) \prod_{s=0}^{k-1} (1 + \omega^{2^s})$, we can bring the summands in (9) over a common denominator:

$$\sum_{k=1}^m \frac{\omega^{2^{k-1}}}{1 - \omega^{2^k}} = \sum_{k=1}^m \frac{\omega^{2^{k-1}} \prod_{s=k}^{m-1} (1 + \omega^{2^s})}{(1 - \omega) \prod_{s=0}^{m-1} (1 + \omega^{2^s})},$$

and we see that it will suffice to show that

$$\sum_{k=1}^m \omega^{2^{k-1}} \prod_{s=k}^{m-1} (1 + \omega^{2^s})$$

is zero. But

$$\omega^{2^{k-1}} \prod_{s=k}^{m-1} (1 + \omega^{2^s}) = \sum_{a \in A_k} \omega^a,$$

where A_k consists of those integers whose binary expansions have the form $(b_{m-1}b_{m-2} \dots b_1b_0)_2$ with $b_0 = b_1 = \dots = b_{k-2} = 0$ and $b_{k-1} = 1$. Thus

$$\sum_{k=1}^m \omega^{2^{k-1}} \prod_{s=k}^{m-1} (1 + \omega^{2^s}) = \sum_{k=1}^m \sum_{a \in A_k} \omega^a = \sum_{x=1}^{2^m-1} \omega^x,$$

and since $2^m - 1$ is a multiple of q , this is zero. ■

THEOREM 4.2. *Suppose that $q, m \geq 3, p_k, r_k, \delta, \gamma$ ($1 \leq k \leq m$) satisfy conditions (i) and (ii) of the CFC, and that $0 < p_k < q$ for $1 \leq k \leq m$. The m sequences \mathcal{B}_{p_k, r_k}^q are a perfect c -fold covering, where c is the number of ones in the binary expansion of $\delta(2^m - 1)/q$.*

Proof. This is equivalent to something by the Covering Criterion: the zeroth coefficient criterion becomes $\sum_{k=1}^m p_k = cq$, and the nonzero coefficient part of the criterion, with an appropriate choice of j and multiplying by $\omega^{-j\gamma}$, becomes equivalent to Lemma 4.1. Thus, what remains to be proved is that $\sum_{k=1}^m p_k = cq$.

We have

$$S := \sum_{k=1}^m p_k \equiv \sum_{k=1}^m \delta 2^{m-k} = \delta(2^m - 1) \equiv 0 \pmod{q}$$

so S is definitely a multiple of q . Note that ζ_k defined by

$$\zeta_k \equiv 2^{m-k} \delta(2^m - 1)/q \pmod{2^m - 1} \quad \text{and} \quad 0 < \zeta_k < 2^m$$

also satisfies $\zeta_k = p_k(2^m - 1)/q$. If the binary expansion of ζ_1 is $(b_{m-1}b_{m-2} \dots b_1b_0)_2$, then the binary expansion of ζ_k is $(b_{k-2}b_{k-3} \dots b_0b_{m-1} \dots b_{k-1})_2$. It follows that $\sum_{k=1}^m \zeta_k = (2^m - 1)w$, where w is the number of 1's in the binary expansion of any of the ζ_k , in particular, in the expansion of $\zeta_m =$

$\delta(2^m - 1)/q$. On the other hand, $\sum_{k=1}^m \zeta_k = \sum_{k=1}^m p_k(2^m - 1)/q = c(2^m - 1)$. Consequently, $c = w$. ■

According to Fraenkel's Conjecture, the values of q for which there is a nontrivial perfect 1-covering by ≥ 3 Beatty sets are of the form $2^m - 1$. As a consequence of the preceding result, we can identify those q which allow for a nontrivial perfect 2-covering.

COROLLARY 4.3. *If q is of the form $2^m - 1$, $m \geq 3$, or $(2^{2uv} - 1)/(2^u + 1)$ for $u, v \geq 1$, then there is a perfect 2-covering by at least three Beatty sets with period q and distinct densities.*

Proof. In this proof, we abbreviate $\gcd(a, b)$ as simply (a, b) . From Theorem 4.2, we know that q has a perfect 2-covering if there is a $\delta < q$ with $(\delta, q) = 1$ such that $\delta(2^m - 1)/q = 2^s + 1$ for some $s < m$, where m is the order of 2 modulo q . Let $d = (2^m - 1, 2^s + 1)$. Since the fractions

$$\frac{(2^m - 1)/d}{(2^s + 1)/d} = \frac{q}{\delta}$$

are both reduced we see that

$$q = \frac{2^m - 1}{(2^m - 1, 2^s + 1)}.$$

Using the elementary identity $2^{(a,b)} - 1 = (2^a - 1, 2^b - 1)$, we now have

$$\begin{aligned} 2^{(m,2s)} - 1 &= (2^m - 1, 2^{2s} - 1) = (2^m - 1, 2^s + 1)(2^m - 1, 2^s - 1) \\ &= (2^m - 1, 2^s + 1)(2^{(m,s)} - 1). \end{aligned}$$

There are two possibilities: $(m, 2s) = (m, s)$ or $(m, 2s) = 2(m, s)$. In the first case, we find that $(2^m - 1, 2^s + 1) = 1$ and so $q = 2^m - 1$. It is clear that any value of $m \geq 3$ will work here. In the second case, we must have $m = 2M$. Thus, in this case $(m, 2s) = (2M, 2s) = 2(M, s) = 2(m, s)$ by hypothesis, i.e., $(M, s) = (2M, s)$. Hence, if we let $u = (M, s)$ then $M = uv$ for some v . This implies that

$$q = \frac{2^{2uv} - 1}{2^u + 1}$$

for some $u, v \geq 1$. This completes the proof. ■

If our Covering Fraenkel Conjecture is correct, then these are all the values of q for which there exist nontrivial perfect 2-coverings. Besides the values of the form $2^m - 1$, the other values less than 10^6 given by these expressions are: 5, 21, 51, 85, 341, 455, 819, 1365, 3855, 5461, 13107, 21845, 29127, 31775, 87381, 209715, 258111, 349525, and 986895.

4.1.1. Wacky trigonometric identities. The computer algebra systems *Mathematica 5.0* and *Maple 7.0* will not automatically simplify the two

expressions ⁽²⁾

$$\frac{1}{\sin(\pi/7)} - \frac{1}{\sin(2\pi/7)} - \frac{1}{\sin(3\pi/7)}$$

and

$$\begin{aligned} &\frac{1}{\sin(\pi/21)} - \frac{1}{\sin(2\pi/21)} - \frac{1}{\sin(4\pi/21)} - \frac{1}{\sin(5\pi/21)} \\ &\qquad\qquad\qquad - \frac{1}{\sin(8\pi/21)} + \frac{1}{\sin(10\pi/21)} \end{aligned}$$

to 0, although they can be coaxed into verifying these identities by first replacing $\sin x$ with $\frac{1}{2i}(e^{ix} - e^{-ix})$. But even this algebraification does not enable the CA systems to verify

$$-2 = \sum_{k=1}^{11} \frac{\sin(2^{k+4}\pi/89)}{\sin(2^k\pi/89)}.$$

We will use the construction of perfect covers and Theorem 1.1 (with some further manipulation) to generate these and other trigonometric identities.

If $q \geq 3$ and $2^m \equiv 1 \pmod{q}$, then (from the proof of Lemma 4.1)

$$0 = \sum_{k=1}^m \frac{\omega^{2^{k-1}}}{1 - \omega^{2^k}} = \sum_{k=0}^{m-1} \frac{1}{\omega^{2^k} - \omega^{-2^k}} = \sum_{k=0}^{m-1} \frac{1}{2i \sin(2^k \pi/q)}.$$

Thus,

$$0 = \sum_{k=1}^m \frac{1}{\sin(2^k \pi/q)} = \sum_{k=1}^m \csc(2^k \pi/q).$$

The two expressions given at the beginning of this subsection are this with $(q, m) = (7, 3)$ and $(q, m) = (21, 6)$ (using $\sin(x) = \sin(\pi - x) = \sin(x + 2\pi)$). We note that Jager & Lenstra [4] showed that all linear dependencies over \mathbb{Q} of $\csc(\pi/q), \csc(2\pi/q), \dots, \csc(\frac{q-1}{2}\pi/q)$ have this form when q is a prime.

Let us take a closer look at our basic identity, which we can expand as follows:

$$\begin{aligned} 0 &= \sum_{k=0}^{m-1} \frac{1}{\omega^{2^k} - \omega^{2^{-k}}} \\ &= - \sum_{k=0}^{m-1} \left(\omega^{2^k} + \omega^{3 \cdot 2^k} + \omega^{5 \cdot 2^k} + \dots + \omega^{(2^t-1) \cdot 2^k} - \frac{\omega^{2^t \cdot 2^k}}{\omega^{2^k} - \omega^{-2^k}} \right), \end{aligned}$$

⁽²⁾ The CASs remain sadly unreliable. For example, *Mathematica 5.0* computes the limit

$$\lim_{n \rightarrow \infty} \frac{\pi n/3^n}{\sin(\pi n/3^n)} \left(1 + \frac{n-1}{n} \right)$$

to be 0. The authors are unaware of any source which documents the mathematical failures of these often-used rarely-cited closed-source programs.

for any t with $0 < t \leq m - 1$. Thus,

$$\sum_{k=0}^{m-1} \frac{\omega^{2t \cdot 2^k}}{\omega^{2^k} - \omega^{2^{-k}}} = \sum_{k=0}^{m-1} \sum_{u=1}^t \omega^{(2u-1)2^k}.$$

Let $C_q(x)$ denote the (multi-)set $\{x \cdot 2^j \bmod q : 0 \leq j < m\}$. Thus, interchanging the order of summation, we have

$$\sum_{k=0}^{m-1} \frac{\omega^{2t \cdot 2^k}}{\omega^{2^k} - \omega^{2^{-k}}} = \sum_{u=1}^t \sum_{a \in C_q(2u-1)} \omega^a.$$

We can rewrite the LHS summand as

$$\frac{\omega^{2t \cdot 2^k}}{\omega^{2^k} - \omega^{2^{-k}}} = \frac{\cos(2\pi 2t \cdot 2^k/q) + i \sin(2\pi 2t \cdot 2^k/q)}{2i \sin(2\pi 2^k/q)}$$

where we have taken $\omega = e^{2\pi i/q}$. Thus,

$$\begin{aligned} \sum_{k=0}^{m-1} \frac{\cos(2\pi 2t \cdot 2^k/q)}{\sin(2\pi \cdot 2^k/q)} &= -2\Im\left(\sum_{u=1}^t \sum_{a \in C_q(2u-1)} \omega^a\right), \\ \sum_{k=0}^{m-1} \frac{\sin(2\pi 2t \cdot 2^k/q)}{\sin(2\pi \cdot 2^k/q)} &= 2\Re\left(\sum_{u=1}^t \sum_{a \in C_q(2u-1)} \omega^a\right). \end{aligned}$$

Hence, we need to understand the sums

$$S(q, t) := \sum_{u=1}^t \sum_{a \in C_q(2u-1)} \omega^a.$$

To begin with, if $-1 \in C_q(1)$ then every term ω^a in S will also have its conjugate ω^{-a} in S as well. This happens exactly when the order of 2 modulo q is even, and in this case we have

$$\sum_{k=0}^{m-1} \frac{\cos(2\pi 2t \cdot 2^k/q)}{\sin(2\pi \cdot 2^k/q)} = 0,$$

but for the trivial reason that every term in the sum occurs with its negative!

In general, each $C_q(2u - 1)$ contains r terms, so that $S(q, t)$ is the sum of t blocks of r powers of ω . If the union of these blocks is a perfect c -covering of $\{\omega, \omega^2, \omega^3, \dots, \omega^{q-1}\}$ then $S(q, t)$ is just equal to $-c$. For example, for $q = 7$, we have $C_7(1) = \{1, 2, 4\}$, $C_7(3) = \{3, 5, 6\}$. Thus,

$$S(7, 2) = \sum_{u=1}^2 \sum_{a \in C_7(2u-1)} \omega^a = (\omega + \omega^2 + \omega^4) + (\omega^3 + \omega^5 + \omega^6) = -1,$$

so that

$$\sum_{k=0}^2 \frac{\sin(8\pi \cdot 2^k/7)}{\sin(2\pi \cdot 2^k/7)} = -2.$$

Another simple case where this happens is when $q \equiv 1 \pmod{6}$ is prime, 2 has order $(q - 1)/3$ modulo q , and 1, 3 and 5 are in distinct $C_q(i)$. In this case, $C_q(1)$, $C_q(3)$ and $C_q(5)$ are disjoint, so that their union is $\mathbb{Z}_q \setminus \{0\}$, which implies that $S_q(3) = -1$. Examples of this occur for $q = 229, 277, 283$, etc. Note that the real part of ω^a is equal to the real part of ω^{-a} . Hence, if the $C_q(b_i), 1 \leq i \leq (q - 1)/m$, form a complete set of disjoint C 's, then in forming a perfect covering of $\mathbb{Z}_q \setminus \{0\}$, we can use either $C_q(b_i)$ or $C_q(-b_i)$ interchangeably, if we only want to control the real part of $S(q, t)$. For example, for $q = 89$, 2 has order 11 modulo 89, and the complete set of disjoint C 's is $C_{89}(1), C_{89}(3), C_{89}(5), C_{89}(9), C_{89}(11), C_{89}(13), C_{89}(19)$, and $C_{89}(33)$. However, one can check that $-1 \in C_{89}(11), -3 \in C_{89}(33), -5 \in C_{89}(9)$ and $-13 \in C_{89}(19)$. Thus,

$$\Re\left(\sum_{u=1}^8 \sum_{a \in C_{89}(2u-1)} \omega^a\right) = \Re\left(\sum_{j=1}^{88} \omega^j\right) = -1.$$

This implies (as usual) the unlikely identity

$$\sum_{k=0}^{10} \frac{\sin(32\pi \cdot 2^k/89)}{\sin(2\pi \cdot 2^k/89)} = -2.$$

Using these ideas (and other extensions thereof), many other results of this type can be derived but we will not pursue these here.

4.2. Bounding q . We assume in this section that the p_k are distinct, $0 < p_k < q$, define $g_k := \gcd(p_k, q)$, assume that $\gcd(q, p_1, \dots, p_m) = \gcd(g_1, \dots, g_m) = 1, r_k \in \mathbb{Z}$, that the m sequences \mathcal{B}_{p_k, r_k} are a perfect c -fold covering, and that there is no pair $i < j$ with $p_i + p_j = q$ (this is weaker than the hypotheses of the CFC). Let $g := \min\{g_1, \dots, g_m\}$, and let n be the multiplicity of g in $\{g_1, \dots, g_m\}$.

LEMMA 4.4. *If $j \not\equiv 0 \pmod{q}$ is a multiple of one of g_1, \dots, g_m , then it is a multiple of at least three of them.*

Proof. Using this j in the second displayed equation in Corollary 1.5, we have

$$0 = \sum_k g_k \llbracket g_k \mid j \rrbracket \frac{\omega^{-jr_k}}{1 - \omega^{j\bar{p}_k}}.$$

Clearly this sum cannot have only one nonzero term. Suppose that it has exactly two, say $g_1 \mid j$ and $g_2 \mid j$. If $g_1 < g_2$, then g_1 is a multiple of only

one of g_1, \dots, g_m , which cannot happen (set $j = g_1$). Thus without loss of generality we may assume that $j = g_1 = g_2$. We have

$$0 = \frac{\omega^{-jr_1}}{1 - \omega^{j\bar{p}_1}} + \frac{\omega^{-jr_2}}{1 - \omega^{j\bar{p}_2}}.$$

Multiply by ω^{jr_2} and clear denominators to get (setting $d = r_2 - r_1$)

$$1 - \omega^{j\bar{p}_1} + \omega^{jd} - \omega^{j(\bar{p}_2+d)} = 0.$$

If four complex numbers with the same modulus sum to 0, then we can split the four into two pairs, each of which sums to 0.

Our first case is $1 = \omega^{j\bar{p}_1}, \omega^{j(\bar{p}_2+d)} = \omega^{jd}$, which is the same as $j\bar{p}_1 \equiv 0 \pmod{q}, j\bar{p}_2 + jd \equiv jd \pmod{q}$. It follows that $j\bar{p}_1 \equiv j\bar{p}_2 \pmod{q}$, and we multiply this congruence by p_1p_2 (a multiple of j^2) to get

$$j^2p_2 \equiv j^2p_1 \pmod{j^2q}.$$

Thus $p_1 \equiv p_2 \pmod{q}$, and since $0 < p_k < q$, we actually have $p_1 = p_2$. This contradicts our hypothesis that the p_k are distinct.

Our second case is $1 = -\omega^{jd}, \omega^{j\bar{p}_1} = -\omega^{j(\bar{p}_2+d)}$, which forces q to be even and which is the equivalent to $jd \equiv q/2 \pmod{q}, j\bar{p}_1 \equiv q/2 + j\bar{p}_2 + jd \pmod{q}$. It follows that $j\bar{p}_1 \equiv j\bar{p}_2 \pmod{q}$, which we handled above.

Our third case is $1 = \omega^{j(\bar{p}_2+d)}, \omega^{j\bar{p}_1} = \omega^{jd}$, and this is the same as $j\bar{p}_2 + jd \equiv 0 \pmod{q}, j\bar{p}_1 \equiv jd \pmod{q}$. Combining these gives $j\bar{p}_1 + j\bar{p}_2 \equiv 0 \pmod{q}$. Multiply this equation by p_1p_2 (a multiple of j^2) to get

$$0 \equiv p_1p_2(j\bar{p}_1 + j\bar{p}_2) \equiv j^2p_2 + j^2p_1 \pmod{j^2q},$$

whence $p_1 + p_2 \equiv 0 \pmod{q}$. Since $0 < p_k < q$, we actually have $p_1 + p_2 = q$. This contradicts our hypothesis that there is no pair of p ’s which sum to q . ■

LEMMA 4.5. *If $n = 3$, then $q \leq 7g$; if $n = 4$, then $q \leq 17g$; if $n = 5$ then $q \leq 33g$; if $n = 6$ then $q \leq 730g$; and in general*

$$q \leq \left(\left(\frac{n}{e-1} + 1 \right)^n + 1 \right) g.$$

Proof. Set $j = p_k$ in Corollary 1.5, and subtract $2g_k\omega^{-p_k r_k}(1 - \omega^{p_k \bar{p}_k})^{-1}$ from both sides, to get

$$-2g_k \frac{\omega^{-p_k r_k}}{1 - \omega^{p_k \bar{p}_k}} = \sum_{i=1}^m (1 - 2\llbracket k = i \rrbracket) \llbracket g_i \mid p_k \rrbracket g_i \frac{\omega^{-p_k r_i}}{1 - \omega^{p_k \bar{p}_i}}.$$

Taking the absolute value of each side, and using the triangle inequality and the identity

$$1 - e^{is} = -2ie^{is/2} \sin(s/2),$$

we get

$$\frac{2g_k}{\sin(\pi g_k/q)} \leq \sum_{i=1}^m \frac{\llbracket g_i \mid p_k \rrbracket g_i}{|\sin(\pi p_k \bar{p}_i/q)|}$$

for all $k \in [m]$.

Suppose that our numbering has $g = g_k$ for $k \in [n]$. For $k \in [n]$ we have the inequalities

$$\frac{2}{\sin(\pi g/q)} \leq \sum_{i=1}^n \frac{1}{|\sin(\pi p_k \bar{p}_i/q)|}.$$

By replacing q with q/g , we can assume without loss of generality that $g = 1$ (the bound we find for q will in truth be a bound for q/g). We wish to show that if q is large enough, then the RHS must be small for some choice of k .

Let $\|x\|$ be the distance from x to the nearest multiple of q , and let z satisfy $\sum_{i=z+1}^{z+n-1} i^{-1} < 1$. Consider the directed graph with vertices p_1, \dots, p_n , with an edge from p_i to p_j if $\|p_j \bar{p}_i\| \leq z$. Every finite directed graph contains either a sink (a point with no out-edges) or a cycle. If $p_{v_1}, p_{v_2}, \dots, p_{v_\beta}$ is a cycle, then

$$\begin{aligned} \|p_{v_2} \bar{p}_{v_1}\| \cdot \|p_{v_3} \bar{p}_{v_2}\| \cdots \|p_{v_1} \bar{p}_{v_\beta}\| &\equiv (\pm p_{v_1} \bar{p}_{v_2})(\pm p_{v_2} \bar{p}_{v_3}) \cdots (\pm p_{v_\beta} \bar{p}_{v_1}) \\ &\equiv \pm 1 \pmod{q} \end{aligned}$$

and

$$1 < \|p_{v_1} \bar{p}_{v_2}\| \cdot \|p_{v_2} \bar{p}_{v_3}\| \cdots \|p_{v_\beta} \bar{p}_{v_1}\| \leq z^\beta \leq z^n.$$

Therefore, $z^n \geq q - 1$. If p_k is a sink, then all $(1 \leq i \leq n, i \neq k)$ of $\|p_k \bar{p}_i\|$ are strictly greater than z . Since p_1, \dots, p_n are distinct and there is no solution to $p_i + p_j = q$, the n values $\|p_k \bar{p}_i\|$ are also distinct. Thus,

$$(10) \quad \frac{2}{\sin(\pi/q)} \leq \sum_{i=1}^n \frac{1}{|\sin(\pi p_k \bar{p}_i/q)|} \leq \frac{1}{\sin(\pi/q)} + \sum_{i=1}^{n-1} \frac{1}{\sin(\pi(z+i)/q)}.$$

Using the approximation $\sin x \approx x$ for small x , one sees that (10) bounds q above. More precisely, if the graph has a cycle, then $q \leq z^n + 1$, and otherwise q is bounded by (10). For $n = 3, 4, 5, 6$, we calculate that $z = 1, 2, 2, 3$, and consequently q is at most $\max\{2, 7\}$, $\max\{17, 10\}$, $\max\{33, 24\}$, $\max\{730, 3\}$, respectively.

To prove the ‘‘in general’’ statement, we need only work with $n \geq 7$. Let $z = \lfloor n/(e - 1) + 1 \rfloor$. We define the graph as above, and handle a cycle in the same way. If p_k is a sink, then (10) becomes

$$\frac{1}{\pi/q} \leq \frac{1}{\sin(\pi/q)} \leq \sum_{i=1}^{n-1} \frac{1}{\sin(\pi(z+i)/q)} \leq \frac{z+n-1}{\sin(\pi(z+n-1)/q)} \sum_{i=1}^{n-1} \frac{1}{z+i},$$

where we have used the inequalities

$$x \geq \sin x \geq \frac{\sin(\pi(z+n-1)/q)}{\pi(z+n-1)/q} x$$

for $0 < x < \pi(z+n-1)/q$. We note that

$$\sum_{i=1}^{n-1} \frac{1}{z+i} \leq \int_z^{z+n-1} \frac{dx}{x} = \ln\left(\frac{z+n-1}{z}\right),$$

so that our inequality can be weakened to read

$$1 \leq \frac{\pi(z+n-1)/q}{\sin(\pi(z+n-1)/q)} \ln\left(\frac{z+n-1}{z}\right).$$

This is inconsistent for any $z > n/(e-1)$, $q > z^n$ and $n \geq 4$. ■

LEMMA 4.6. *If $m \leq 5$, then $g = 1$.*

Proof. Renumber so that $g = g_1 \leq g_2 \leq \dots \leq g_m$. If all the g_i are equal, then $g = 1$ since $\gcd\{g_1, \dots, g_m\} = 1$. Thus we may assume that $n < m$.

By Lemma 4.4 with $j = g$, we have $n \geq 3$. Since $n < m$, we may assume that $4 \leq m \leq 6$, so that $g = g_1 = g_2 = g_3 < g_4$. Clearly g divides g_1, g_2, g_3 by definition, and g_4, g_5 by Lemma 4.4 (with $j = g_4$ and $j = g_5$, respectively). Since $\gcd\{g_1, \dots, g_m\} = 1$, we have shown that $g = 1$. ■

THEOREM 4.7. *The CFC is true for $m \leq 5$.*

Proof. First, observe that by Lemma 4.6 we may restrict our attention to sequences \mathcal{B}_{p_k, r_k} with p_1 relatively prime to q . Moreover, as a consequence of Corollary 1.5, the sequences $\mathcal{B}_{p_1, r_1}, \mathcal{B}_{p_2, r_2}, \dots, \mathcal{B}_{p_m, r_m}$ are a perfect covering if and only if the sequences

$$\mathcal{B}_{1,0}, \mathcal{B}_{\bar{p}_1 p_2, p_1 r_2}, \dots, \mathcal{B}_{\bar{p}_1 p_m, p_1 r_m}$$

are a perfect covering ⁽³⁾. Thus, we may assume that $p_1 = 1$ and $r_1 = 0$. Corollary 1.5 also tells us that $p_m \equiv -\sum_{k=1}^{m-1} p_k \pmod{q}$, and with $j = 1$ that

$$(11) \quad 0 = \sum_{k=1}^m \llbracket g_k = 1 \rrbracket \frac{\omega^{-r_k}}{1 - \omega^{\bar{p}_k}}.$$

This implies that

$$(12) \quad 1 \leq \sum_{k=2}^m \left| \frac{1 - \omega}{1 - \omega^{\bar{p}_k}} \right| = \sum_{k=2}^m \frac{\sin(\pi/q)}{\sin(\pi \bar{p}_k/q)}.$$

In this expression there are $m - 1$ degrees of freedom: $q, p_2, p_3, \dots, p_{m-1}$.

⁽³⁾ This will typically affect the *multiplicity* of the covering.

Without loss of generality $1 = p_1 < p_2 < p_3 < \dots < p_m < q$. Also, the hypotheses of the CFC imply that there is no solution to $p_i + p_j = q$, and Lemma 4.5 (with Lemma 4.6) implies $q \leq 33$.

There are only 346 m -tuples (p_1, \dots, p_m) with $m \leq 5$,

$$1 = p_1 < p_2 < \dots < p_m < q \leq 33,$$

$\sum_{k=1}^m p_k \equiv 0 \pmod{q}$, no solution to $p_i + p_j = q$, and satisfying (12). We refine our search by noting that if $(p_k, q) = 1$, then $(\bar{p}_k p_1, \bar{p}_k p_2, \dots, \bar{p}_k p_m)$ must also be on our list of 346 (this is equivalent to taking values of j other than 1 in deriving the inequality (12)). This pares the list down to a single tuple for $m = 3$, a single tuple for $m = 4$, and 10 tuples for $m = 5$. The tuples predicted by the CFC are on these lists, and the remaining 9 tuples are eliminated by an exhaustive search for r_2, \dots, r_5 such that

$$0 = \frac{1}{1 - \omega} + \sum_{k=2}^5 \frac{\omega^{-r_k}}{1 - \omega^{\bar{p}_k}}.$$

The only perfect coverings with 5 or fewer Beatty sequences are those predicted by the Covering Fraenkel Conjecture. ■

We remark that we may similarly reduce the $m = 6$ case of Fraenkel’s Conjecture (but not the CFC) to a finite computation. For example, if $m = 6, n = 4$, then we may argue as in the $m = 5$ case of Lemma 4.6 that $g = 1$, and so by Lemma 4.5 we get the bound $q \leq 730$. If $m = 6, n = 3$ (so that $q \leq 7g$), then we may (using Lemma 4.4) renumber so that $g = g_1 = g_2 = g_3$ and $h = g_4 = g_5 = g_6$, with $\gcd(g, h) = 1$. Since the p_k are distinct, we have $p_1 + p_2 + p_3 \geq g + 2g + 3g = 6g$ and $p_4 + p_5 + p_6 \geq 6h > 6g$. Thus $q = \sum p_k > 12g$, a contradiction. In contrast, for $m = 7$, we arrive at the consistent inequalities $q \leq 17g$ and $q = \sum p_k > 16g$.

5. Proving Fraenkel’s Conjecture. We envision a noncomputational proof of Fraenkel’s Conjecture along the following lines. Suppose that \mathcal{B}_{p_k, r_k}^q ($1 \leq k \leq m$) partition \mathbb{Z} , with $p_1 < p_2 < \dots < p_m < q$, and suppose that m is minimal. Let $g_k := \gcd(p_k, q)$.

Now, suppose that $g := \min_k \{g_k\}$ is larger than 1. The Covering Criterion with $j = g$ yields

$$0 = \sum_{\substack{k=1 \\ g_k=g}}^m \frac{\omega^{-g v_k}}{1 - \omega^{g \bar{p}_k}}.$$

Let u_1, \dots, u_n be those \bar{p}_k for which $g_k = g$ (there are $n \geq 3$ of them by Lemma 4.4, and $n < m$ since $\gcd\{g_1, \dots, g_m\} = 1$), and let v_1, \dots, v_n be the negatives of the r_k for which $g_k = g$. Also replace $\omega = e^{2\pi i/q}$ with $x = e^{2\pi i g/q}$

to get

$$0 = \sum_{k=1}^n \frac{x^{v_k}}{1 - x^{u_k}}.$$

This seems to imply that the sum vanishes for x any (q/g) th root of unity, which would imply that these sequences alone form a perfect covering, whence $\sum_{k=1}^m p_k \llbracket g_k = g \rrbracket \geq q$. This is impossible since $n < m$. Thus, the following conjecture implies that, in the present setting, $g = 1$.

CONJECTURE 5.1. *Suppose that $1 \leq u_1 < u_2 < \dots < u_n < q$, with $\gcd(u_k, q) = 1$ for all k , and let v_1, \dots, v_n be arbitrary integers. If the function*

$$f(x) := \sum_{k=1}^n \frac{x^{v_k}}{1 - x^{u_k}}$$

vanishes at $x = e^{2\pi i/q}$, then $\sum_{k=1}^n u_k \geq q$.

This in turn simplifies the Covering Criterion substantially. Considering the absolute value of the Covering Criterion as in the proof of Lemma 4.5 ⁽⁴⁾ the following conjecture becomes relevant.

CONJECTURE 5.2. *Suppose that p_1, \dots, p_n are distinct and relatively prime to $q > (7/4)^n$, with $\sum p_k \leq q$, and for each $k \in [n]$,*

$$\frac{2}{\sin(\pi/q)} \leq \sum_{i=1}^n \frac{1}{|\sin(\pi p_k \bar{p}_i/q)|}.$$

Then $q = 2^n - 1$ and $\{p_1, \dots, p_n\} \equiv \{1, 2, \dots, 2^{n-1}\} \pmod{q}$.

At this point, we would have shown that a counterexample to Fraenkel's Conjecture (with m sequences) must have $q < (7/4)^m$. We envision handling this situation combinatorially, probably in conjunction with Tijdeman's combinatorial restrictions. He notes [8, Lemma 4] that if \mathcal{B}_{p_k, r_k} and \mathcal{B}_{p_j, r_j} are disjoint, then either $p_k = p_j$ or $\lfloor q/p_k \rfloor \neq \lfloor q/p_j \rfloor$, and so

$$\lfloor q/p_m \rfloor < \dots < \lfloor q/p_2 \rfloor < \lfloor q/p_1 \rfloor.$$

Also, his main lemma [8, Lemma 3] can be strengthened (using the same proof, but in terms of Beatty sequences instead of balanced sequences) to provide the powerful restriction on the p_k 's in a counterexample with minimal m : $p_k \leq (q - 2g_k)/3$. Tijdeman used these two lemmas (and some casework) to show that $m \geq 7$. Thus, the remaining situation has many sequences with small (but spread out) p_k 's and quite small q .

⁽⁴⁾ In Lemma 4.5 we found that for $q > n^n$ (roughly), k could be chosen to make a particular inequality invalid. Conjecture 5.2 posits that the n^n bound can be improved to 2^n , and barring the single exception of $q = 2^n - 1$, it can be improved to $(7/4)^n$. This is supported by computational investigations.

6. Refining the conjectures. Ideally, one would like arithmetic conditions on α_k, r_k for the sequences $\{[n\alpha_k + r_k] : n \in \mathbb{Z}\}$ to be a perfect covering, without assuming that the α are distinct. Morikawa has given such conditions for a small number of sequences to be a perfect 1-cover; see [9] for a brief description of Morikawa's work and citations for his many papers on the topic.

The Covering Fraenkel Conjecture that we have advanced is another step in this direction. A more ambitious step would be to replace the condition "with no proper subset $I \subsetneq [m]$ having $\sum_{i \in I} p_i \equiv 0 \pmod{q}$ " with the weaker condition "with no proper subset of the sequences being a perfect covering."

We note that Conjecture 5.1 can likely be strengthened:

CONJECTURE 6.1. *Suppose that $1 \leq u_1 < u_2 < \dots < u_n < q$, with $\gcd(u_k, q) = 1$ for all k , and with no subset of the u_k 's summing to a multiple of q , and let v_1, \dots, v_n be arbitrary integers. If the function*

$$f(x) := \sum_{k=1}^n \frac{x^{v_k}}{1 - x^{u_k}}$$

vanishes at $x = e^{2\pi i/q}$, then it vanishes at all q th roots of unity except $x = 1$.

Joe Buhler notes that

$$\frac{1}{1-x} + \frac{x^5}{1-x^2} + \frac{x^{10}}{1-x^4} + \frac{x^{10}}{1-x^{11}} + \frac{x^5}{1-x^{13}} + \frac{1}{1-x^{14}}$$

vanishes at primitive 15th roots of unity, but not at the primitive 5th roots of unity, and thus the condition on sums of subsets of the u_k 's is necessary.

Acknowledgements. The authors wish to thank the National Science Foundation for supporting mathematics in general and the authors in particular. We thank Professor Greg Martin of the University of British Columbia for supplying the main idea underlying Lemma 4.5.

References

- [1] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monogr. Enseign. Math. 28, L'Enseignement Mathématique, Univ. Genève, Genève, 1980.
- [2] A. S. Fraenkel, *Complementing and exactly covering sequences*, J. Combin. Theory Ser. A 14 (1973), 8–20.
- [3] R. L. Graham, *Covering the positive integers by disjoint sets of the form $\{[n\alpha + \beta] : n = 1, 2, \dots\}$* , *ibid.* 15 (1973), 354–358.
- [4] H. Jager and H. W. Lenstra Jr., *Linear independence of cosecant values*, Nieuw Arch. Wisk. (3) 23 (1975), 131–144.

- [5] K. O'Bryant, *Fraenkel's partition and Brown's decomposition*, *Integers* 3 (2003), A11, 17 pp. (electronic).
- [6] R. J. Simpson, *Disjoint covering systems of rational Beatty sequences*, *Discrete Math.* 92 (1991), 361–369.
- [7] —, *Disjoint Beatty sequences*, *Integers* 4 (2004), A12, 10 pp. (electronic).
- [8] R. Tijdeman, *Fraenkel's conjecture for six sequences*, *Discrete Math.* 222 (2000), 223–234.
- [9] —, *Exact covers of balanced sequences and Fraenkel's conjecture*, in: *Algebraic Number Theory and Diophantine Analysis* (Graz, 1998), de Gruyter, Berlin, 2000, 467–483.

Department of Computer Science & Engineering
University of California at San Diego
San Diego, CA 92093, U.S.A.
E-mail: rgraham@ucsd.edu

Department of Mathematics
University of California at San Diego
San Diego, CA 92093, U.S.A.
E-mail: kevin@member.ams.org

Received on 16.7.2004
and in revised form on 18.3.2005

(4805)