EQUALITIES AMONG CAPACITIES OF (D, K)-CONSTRAINED SYSTEMS*

NAVIN KASHYAP† AND PAUL H. SIEGEL†

Abstract. In this paper, we consider the problem of determining when the capacities of distinct (d, k)-constrained systems can be equal. A (d, k)-constrained system consists of binary sequences which have at least d zeros and at most k zeros between any two successive ones. If we let $C(d, k)$ denote the capacity of a (d, k)-constrained system, then it is known that $C(d, 2d) = C(d+1, 3d+1)$, and $C(d, 2d+1) = C(d+1, \infty)$. Repeated application of these two identities also yields the chain of equalities $C(1, 2) = C(2, 4) = C(3, 7) = C(4, \infty)$. We show that these are the only equalities possible among the capacities of (d, k)-constrained systems. In the process, we also provide useful factorizations of the characteristic polynomials for these constraints.

Key words. Shannon capacity, constrained systems, (d, k)-constraints, polynomial factorization

AMS subject classifications. 94A55, 11R09

1. Introduction. Given non-negative integers d, k, with $d < k$, we say that a binary sequence is (d, k)-constrained if every run of zeros has length at most k and any two successive ones are separated by a run of zeros of length at least d. A (d, k)-*constrained system* is defined to be the set of all finite-length (d, k)-constrained binary sequences. The above definition can be extended to the case $k = \infty$ by not imposing an upper bound on the lengths of zero-runs. In other words, a binary sequence is said to be (d, ∞)-constrained if any two successive ones are separated by at least d zeros, and a (d, ∞)-*constrained system* is defined to be the set of all finite-length (d, ∞)-constrained binary sequences. From now on, when we refer to (d, k)-constrained systems, we shall also allow k to be ∞.

Let $\mathcal{S}(d, k)$ be a (d, k)-constrained system, and let $q_{d,k}(n)$ be the number of length-n sequences in $\mathcal{S}(d, k)$. The *Shannon capacity*, or simply *capacity*, of $\mathcal{S}(d, k)$ is defined as

$$C(d, k) = \lim_{n \to \infty} \frac{1}{n} \log_2 q_{d,k}(n) \tag{1}$$

It is well-known (see *e.g.*, [2]) that $C(d, k) = \log_2 \rho_{d,k}$, where $\rho_{d,k}$ is the unique largest-magnitude root of a certain polynomial, $\chi_{d,k}(z)$, called the *characteristic polynomial* of the constraint. When k is finite, $\chi_{d,k}(z)$ takes the form

$$\chi_{d,k}(z) = z^{k+1} - \sum_{j=0}^{k-d} z^j \tag{2}$$

and when $k = \infty$,

$$\chi_{d,\infty}(z) = z^{d+1} - z^d - 1 \tag{3}$$

$\rho_{d,k}$ is always real and lies in the interval $(1, 2]$, so that $0 < C(d, k) \leq 1$. In fact, $C(d, k) = 1$ if and only if $(d, k) = (0, \infty)$.

*This work was supported by a research grant from Applied Micro Circuits Corporation, San Diego, CA

†Dept. of Electrical and Computer Engineering, University of California – San Diego, 9500 Gilman Drive, MC 0407, La Jolla, CA 92093-0407. Email: {nkashyap,psiegel}@ece.ucsd.edu.

Interest in constrained systems and their capacities dates back to the work of Shannon [8]. In the mathematical literature, constrained systems are the subject of study of symbolic dynamics (*cf.* [3]), where the capacity of a constrained system is referred to as its entropy. (d,k)-constrained systems in particular have applications in magnetic and optical recording systems [5].

It is easily verified that certain pairs of (d,k)-constrained systems have the same capacity. For example, we have the identities

$$C(d,2d) = C(d+1,3d+1) \tag{4}$$

$$C(d,2d+1) = C(d+1,\infty) \tag{5}$$

true for all $d \geq 0$. The first equality is a consequence of the fact that $\chi_{d+1,3d+1}(z) = (z^{d+1}+1)\,\chi_{d,2d}(z)$, since all the roots of $z^{d+1}+1$ lie on the unit circle, so that $\rho_{d,2d} = \rho_{d+1,3d+1}$. Similarly, the factorization $\chi_{d,2d+1}(z) = \chi_{d+1,\infty}(z)\,\sum_{i=0}^{d} z^i$ yields (5), since $\sum_{i=0}^{d} z^i = (z^{d+1}-1)/(z-1)$ has all its roots on the unit circle as well.

Repeatedly applying the two identities above also yields the chain of equalities

$$C(1,2) = C(2,4) = C(3,7) = C(4,\infty) \tag{6}$$

It is the aim of this paper to show that (4), (5) and (6) capture all the equalities possible among the capacities of (d,k)-constrained systems. More precisely, we shall prove the following theorem:

THEOREM 1. *If $C(d,k) = C(\hat{d},\hat{k})$ for $(d,k) \neq (\hat{d},\hat{k})$, then one of the following holds:*
(i) $\{(d,k),(\hat{d},\hat{k})\} = \{(\ell,2\ell),\,(\ell+1,3\ell+1)\}$ for some integer $\ell \geq 0$,
(ii) $\{(d,k),(\hat{d},\hat{k})\} = \{(\ell,2\ell+1),\,(\ell+1,\infty)\}$ for some integer $\ell \geq 0$,
(iii) $(d,k),(\hat{d},\hat{k})$ are among the pairs listed in (6).

The key to our proof of this result is an explicit factorization we obtain for the characteristic polynomials of the (d,k)-constraints. We show that $\chi_{d,k}(z)$ can be factored as

$$\chi_{d,k}(z) = \Phi_{d,k}(z)\,\Psi_{d,k}(z)$$

where $\Phi_{d,k}(z), \Psi_{d,k}(z) \in \mathbb{Z}[z]$, $\Psi_{d,k}(z)$ is irreducible (over $\mathbb{Z}$), and $\Phi_{d,k}(z)$ either is 1 or has all its roots on the unit circle. We can, in fact, determine an explicit form for the polynomials $\Phi_{d,k}(z)$, from which we can deduce an expression for $\Psi_{d,k}(z)$ for certain (d,k) pairs. An immediate consequence of this result is that $C(d,k) = C(\hat{d},\hat{k})$ if and only if $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$. Theorem 1 is then obtained by identifying all the cases where we can have $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$. This last step relies heavily on the explicit form we derive for the Φ and Ψ polynomials.

The rest of the paper is organized as follows. In Section 2, we present the factorization of $\chi_{d,k}(z)$, which we use in Section 3 to prove Theorem 1.

2. Factorization of $\chi_{d,k}(z)$. We shall first consider the factorization of $\chi_{d,\infty}(z)$, as it follows directly from existing results. Throughout this paper, we shall only be concerned with polynomials with integer coefficients. Any such polynomial is called reducible if it can be factored over the integers, and irreducible otherwise.

If $F(z) \in \mathbb{Z}[z]$ is a polynomial of degree n, then $F^*(z) = z^n F(1/z)$ is called the *reciprocal polynomial* of $F(z)$. Thus, for example, if $F(z) = z^5 - 4z^4 + 6z^3 - 4z^2 - 1$, then $F^*(z) = 1 - 4z + 6z^2 - 4z^3 - z^5$ is its reciprocal polynomial.

Observe that $\chi^*_{d,\infty}(z) = 1 - z - z^{d+1}$, so that when d is odd, $-\chi^*_{d,\infty}(-z) = z^{d+1} - z - 1$, and when d is even, $\chi^*_{d,\infty}(-z) = z^{d+1} + z + 1$. The following result deals with the irreducibility of the polynomials $z^n - z - 1$ and $z^n + z + 1$.

THEOREM 2 ([7, Theorem 1]). *(i) $z^n - z - 1$ is irreducible for all n.*
(ii) For $n > 2$, $z^n + z + 1$ is irreducible iff $n \not\equiv 2 \pmod 3$. If $n \equiv 2 \pmod 3$, then $z^2 + z + 1$ is a factor and the other factor is irreducible.

Thus, by part (i) of the above theorem, for odd d, $-\chi^*_{d,\infty}(-z)$ is irreducible, and hence, so is $\chi_{d,\infty}(z)$. When d is even, it is either 0, 2 or 4 (mod 6). In the first two cases, $d + 1 \not\equiv 2 \pmod 3$, and so by part (ii) of the above result, $\chi^*_{d,\infty}(-z)$ is irreducible, and therefore, so is $\chi_{d,\infty}(z)$. When $d \equiv 4 \pmod 6$, we have $d + 1 \equiv 2 \pmod 3$, and applying part (ii) of the theorem again, we see that $\chi^*_{d,\infty}(-z) = (z^2 + z + 1)p(z)$ for some irreducible $p(z)$. Therefore, in this case, we have $\chi_{d,\infty}(z) = (z^2 - z + 1)\Psi_{d,\infty}(z)$, with $\Psi_{d,\infty}(z) = p^*(-z)$ being irreducible. In fact, one can easily verify by means of an inductive argument that when $d \equiv 4 \pmod 6$, then

$$\Psi_{d,\infty}(z) = z^3 - z - 1 + \sum_{l=2}^{(d+2)/6} (z^{6l-3} - z^{6l-5} - z^{6l-6} + z^{6l-8}) \tag{7}$$

We summarize these results in the following theorem.

THEOREM 3. *For $d \not\equiv 4 \pmod 6$, $\chi_{d,\infty}(z)$ is irreducible. For $d \equiv 4 \pmod 6$, $\chi_{d,\infty}(z) = (z^2 - z + 1)\Psi_{d,\infty}(z)$, with $\Psi_{d,\infty}(z)$ irreducible and of the form given by (7).*

When k is finite, the factorization we obtain for $\chi_{d,k}(z)$ is based on a technique originally due to Ljunggren [4], which was further developed by Filaseta [1]. We briefly describe this technique here. .

We define $F(z) \in \mathbb{Z}[z]$ to be *self-reciprocal* if $F(z) = \pm F^*(z)$. Note that $F(z)$ is self-reciprocal if and only if λ being a root of $F(z)$ implies that λ^{-1} is also a root. An example of a polynomial that is self-reciprocal is $z^5 - 10z^3 + 10z^2 - 1$.

Now, any $F(z) \in \mathbb{Z}[z]$ can always be written as $F(z) = \Phi(z)\Psi(z)$, where $\Phi(z)$ is the product of all the irreducible self-reciprocal factors of $F(z)$ that have positive leading coefficients. If $F(z)$ has no irreducible self-reciprocal factors, then we take $\Phi(z) = 1$ and $\Psi(z) = F(z)$. We call $\Phi(z)$ the *reciprocal part* of $F(z)$, while $\Psi(z)$ is called the *non-reciprocal part* of $F(z)$. It is worth pointing out that this definition does not preclude $\Psi(z)$ from being self-reciprocal itself. For example, $F(z) = z^6 + z^5 + z^4 + 3z^3 + z^2 + z + 1 = (z^3 + z^2 + 1)(z^3 + z + 1)$, and both the factors are irreducible, but not self-reciprocal. Thus, the non-reciprocal part of $F(z)$ is $F(z)$ itself, which is a self-reciprocal polynomial. On the other hand, the reciprocal part of any polynomial is always self-reciprocal.

Note that if we take $F(z) = \chi_{d,\infty}(z)$, then Theorem 3 shows that the reciprocal part of $F(z)$ is 1 when $d \not\equiv 4 \pmod 6$, and is $z^2 - z + 1$ when $d \equiv 4 \pmod 6$. Thus, the non-reciprocal part of $F(z)$ is $F(z)$ itself in the former case, and is $\Psi_{d,\infty}(z)$ as given by (7) in the latter case. Observe that in either case, the non-reciprocal part of $F(z)$ is irreducible.

The following result [1, Lemma 1] tells us precisely when the non-reciprocal part of a polynomial is reducible.

LEMMA 4 (Ljunggren-Filaseta Lemma). *The non-reciprocal part of $F(z) \in \mathbb{Z}[z]$ is reducible if and only if there exists $G(z)$ different from $\pm F(z)$ and $\pm F^*(z)$ such*

that $G(z)G^*(z) = F(z)F^*(z)$.

The "only if" part of this lemma is sufficient for our purposes. To verify this part, note that if the non-reciprocal part, $\Psi(z)$, is reducible, then $\Psi(z) = A(z)B(z)$ for some non-self-reciprocal polynomials $A(z)$ and $B(z)$. Setting $G(z) = A(z)B^*(z)\Phi(z)$, where $\Phi(z)$ is the reciprocal part of $F(z)$, we see that $G(z)$ has the properties stated in the lemma.

We shall use the Ljunggren-Filaseta lemma to prove the irreducibility of the non-reciprocal part of $\chi_{d,k}(z)$ $(k < \infty)$. Once this is done, we shall study the reciprocal part of the polynomial. Recall that $\chi_{d,k}(z)$ is a polynomial of the form $f(z) = z^n - z^m - z^{m-1} - \ldots - z - 1$ for some $n > m > 0$. It is well-known (see *e.g.* [9]) that when $n = m + 1$, the polynomial $f(z)$ is itself irreducible. So, we need only consider the case when $n \geq m + 2$. We shall show that if $g(z) \in \mathbb{Z}[z]$ is a polynomial such that $g(z)g^*(z) = f(z)f^*(z)$, then $g(z) = \pm f(z)$ or $\pm f^*(z)$. The "only if" part of the Ljunggren-Filaseta lemma then shows that the non-reciprocal part of $f(z)$ is irreducible.

So, let $g(z) = \sum_{i=0}^{n} g_i z^i$ be a polynomial in $\mathbb{Z}[z]$ such that $g(z)g^*(z) = f(z)f^*(z)$. Note that $g(z)$ must itself be a polynomial of degree n. Without loss of generality, we may assume that $g_n > 0$ (else, replace $g(z)$ by $-g(z)$).

LEMMA 5. *The coefficients* g_i *of* $g(z)$ *must satisfy the following equations:*

$$g_n = 1\ ,\ g_0 = -1 \tag{8}$$

$$g_1 - g_{n-1} = -1 \tag{9}$$

$$\sum_{i=1}^{n-2} g_i g_{i+1} = m - 1 \tag{10}$$

$$\sum_{i=1}^{n-1} g_i^2 = m \tag{11}$$

Proof: Let $f(z) = \sum_{i=0}^{n} f_i z^i$, so that $f_n = 1$, $f_i = 0$ for $m + 1 \leq i \leq n - 1$, and $f_i = -1$ for $0 \leq i \leq m$.

Equating the constant coefficients of $f(z)f^*(z)$ and $g(z)g^*(z)$, we see that $g_0 g_n = -1$. Since $g_0, g_n \in \mathbb{Z}$ and $g_n > 0$, we must have $g_n = 1, g_0 = -1$.

(9) is obtained by equating the coefficients of z in $f(z)f^*(z)$ and $g(z)g^*(z)$. The coefficient of z in $g(z)g^*(z)$ is $g_0 g_{n-1} + g_1 g_n = g_1 - g_{n-1}$. Now, note that since $n \geq m+2$, we have $f_{n-1} = 0$. Hence, the coefficient of z in $f(z)f^*(z)$ is $f_0 f_{n-1} + f_1 f_n = -1$.

To get (10), we equate the coefficients of z^{n-1}. In $g(z)g^*(z)$, this coefficient is $\sum_{i=0}^{n-1} g_i g_{i+1}$, while in $f(z)f^*(z)$, it is $\sum_{i=0}^{n-1} f_i f_{i+1} = \sum_{i=0}^{m-1} f_i f_{i+1}$, since $f_{i+1} = 0$ for $m \leq i \leq n-2$, and $f_i = 0$ for $i = n-1$. But in the range $0 \leq i \leq m-1$, $f_i = f_{i+1} = -1$, which shows that $\sum_{i=0}^{m-1} f_i f_{i+1} = m$. Thus, we have $\sum_{i=0}^{n-1} g_i g_{i+1} = m$, which reduces to (10) upon using (8) and (9).

Finally, the coefficient of z^n in $g(z)g^*(z)$ is $\sum_{i=0}^{n} g_i^2$, and correspondingly, in $f(z)f^*(z)$ is $\sum_{i=0}^{n} f_i^2 = m + 2$. Hence, $\sum_{i=0}^{n} g_i^2 = m + 2$, and since $g_0^2 = g_n^2 = 1$, we see that $\sum_{i=1}^{n-1} g_i^2 = m$, which proves (11). ■

We use this lemma to prove the following proposition.

PROPOSITION 6. *The non-reciprocal part of* $f(z) = z^n - z^m - z^{m-1} - \ldots - z - 1$, $n > m > 0$, *is irreducible.*

Proof: As noted above, we need only prove the result for $n \geq m+2$. Lemma 5 (which applies for $n \geq m+2$) shows that any $g(z) = \sum_{i=0}^{n} g_i z^i$ such that $g(z)g^*(z) = f(z)f^*(z)$ and $g_n > 0$ must satisfy (8)–(11). Now, observe that

$$\begin{aligned}\sum_{i=1}^{n-2}(g_i - g_{i+1})^2 &= \sum_{i=1}^{n-2} g_i^2 + \sum_{i=1}^{n-2} g_{i+1}^2 - 2\sum_{i=1}^{n-2} g_i g_{i+1} \\ &= 2\sum_{i=1}^{n-1} g_i^2 - g_1^2 - g_{n-1}^2 - 2\sum_{i=1}^{n-2} g_i g_{i+1} \\ &= 2m - g_1^2 - g_{n-1}^2 - 2(m-1)\end{aligned}$$

with the last equality using (10) and (11). Thus, we see that

$$g_1^2 + g_{n-1}^2 + \sum_{i=1}^{n-2}(g_i - g_{i+1})^2 = 2 \tag{12}$$

Since all the g_i's are integers, this equation is satisified if and only if exactly $n-2$ of the quantities g_1, g_{n-1}, $g_i - g_{i+1}$ $(i = 1, 2, \ldots, n-2)$ are 0, and the remaining two non-zero quantities take values from the set $\{-1, 1\}$. In particular, $g_1 \in \{-1, 0, 1\}$. We consider each of the three choices for g_1 in turn.

If $g_1 = -1$, then (9) shows that $g_{n-1} = 0$. Hence, there exists a $k \in \{1, 2, \ldots, n-2\}$ such that $g_k - g_{k+1} = \pm 1$ and $g_i - g_{i+1} = 0$ for $i = 1, 2, \ldots, n-2$, $i \neq k$. Now, if $g_k - g_{k+1} = 1$, then we must have $g_i = -1$ for $1 \leq i \leq k$, and $g_i = -2$ for $k+1 \leq i \leq n-1$, which contradicts $g_{n-1} = 0$. Hence, $g_k - g_{k+1}$ must be -1, in which case $g_i = -1$ for $1 \leq i \leq k$, and $g_i = 0$ for $k+1 \leq i \leq n-1$. Using (11), we see that $k = m$, which forces $g(z)$ to be $z^n - z^m - z^{m-1} - \ldots - z - 1 = f(z)$.

If $g_1 = 0$, then (9) yields $g_{n-1} = 1$. As above, we must have $g_k - g_{k+1} = \pm 1$ for some $k \in \{1, 2, \ldots, n-2\}$, and $g_i - g_{i+1} = 0$ for $i = 1, 2, \ldots, n-2$, $i \neq k$. This time, choosing $g_k - g_{k+1}$ to be 1 leads to $g_{n-1} = -1$, which contradicts $g_{n-1} = 1$. Thus, $g_k - g_{k+1} = -1$, so that $g_i = 0$ for $1 \leq i \leq k$, and $g_i = 1$ for $k+1 \leq i \leq n-1$. From (11), we now get $k+1 = n-m$. Hence, $g(z)$ must be $z^n + z^{n-1} + \ldots + z^{n-m} - 1 = -f^*(z)$.

If $g_1 = 1$, then (9) implies that $g_{n-1} = 2$, which means that (12) cannot be satisfied. So, g_1 cannot be 1.

Thus, we have shown that if $g(z)$ is such that $g(z)g^*(z) = f(z)f^*(z)$ and $g_n > 0$, then $g(z) = f(z)$ or $g(z) = -f^*(z)$. For any $g(z)$ with $g_n < 0$, we can apply the above reasoning to $-g(z)$. This proves that if $g(z) \in \mathbb{Z}[z]$ is such that $g(z)g^*(z) = f(z)f^*(z)$, then $g(z) = \pm f(z)$ or $\pm f^*(z)$. The proposition now follows from the Ljunggren-Filaseta lemma. ■

Having shown the irreducibility of the non-reciprocal part of $f(z) = z^n - z^m - z^{m-1} - \ldots - z - 1$, we move on to analyzing the reciprocal part, $\phi(z)$, of $f(z)$. Our first goal is to show that all the roots of $\phi(z)$ are in fact certain roots of unity, which will help us in determining the exact form of $\phi(z)$.

LEMMA 7. *If* λ *is a root of* $\phi(z)$, *then* λ *is a root of either* $\sum_{i=0}^{m-1} z^i$ *or* $\sum_{i=0}^{m+1} z^i$. *In other words,* λ *is either an* m*th or an* $(m+2)$*th root of unity, distinct from 1.*

Proof: Let λ be a root of $\phi(z)$. Note that $\lambda \neq 0$ because 0 cannot be a root of $f(z)$, as $f(0) = -1$. Since $\phi(z)$ is a self-reciprocal polynomial, λ^{-1} is also a root of $\phi(z)$. Since $\phi(z)$ is a factor of $f(z)$, we have $f(\lambda) = f(\lambda^{-1}) = 0$. This implies that

$$\lambda^n - \lambda^m - \lambda^{m-1} - \ldots - \lambda - 1 = 0 \tag{13}$$

$$\lambda^n + \lambda^{n-1} + \ldots + \lambda^{n-m+1} + \lambda^{n-m} - 1 = 0 \tag{14}$$

Equating the left-hand sides of these two equations, cancelling out the common terms and re-arranging, we obtain

$$(\lambda^{n-1} + \lambda^{n-2} + \ldots + \lambda^{n-m}) + (\lambda^m + \lambda^{m-1} + \ldots + \lambda) = 0$$

Dividing through by $\lambda \neq 0$, we see that the above equation simplifies to

$$(\lambda^{n-m-1} + 1)(\lambda^{m-1} + \lambda^{m-2} + \ldots + 1) = 0$$

Hence, λ is a root of either $z^{n-m-1} + 1$ or $\sum_{i=0}^{m-1} z^i$. However, if λ is a root of $z^{n-m-1} + 1$, then $\lambda^{n-m-1} = -1$. Now, note that (14) can be re-written as $\lambda^{n-m-1}(\lambda^{m+1} + \lambda^m + \ldots + \lambda) - 1 = 0$, which reduces to $-\lambda^{m+1} - \lambda^m - \ldots - \lambda - 1 = 0$, since $\lambda^{n-m-1} = -1$. Hence if λ is a root of $z^{n-m-1} + 1$, then it is also a root of $\sum_{i=0}^{m+1} z^i$, which proves the lemma. ■

We can actually say something more about the roots of $\phi(z)$, as we shall see in the next few lemmas.

LEMMA 8. *If λ is a root of $\phi(z)$ that is also a root of $\sum_{i=0}^{m-1} z^i$, then λ is in fact a root of $\sum_{i=0}^{q-1} z^i$, where $q = \gcd(m, n)$.*

Proof: Suppose that λ is as in the hypothesis of the lemma. Since $\phi(\lambda) = 0$, we also have $f(\lambda) = 0$, which means that

$$\lambda^n - \sum_{i=0}^{m} \lambda^i = 0 \tag{15}$$

But since λ is a root of $\sum_{i=0}^{m-1} z^i$, we have $\sum_{i=0}^{m-1} \lambda^i = 0$ and moreover, $\lambda^m = 1$. Hence, (15) reduces to $\lambda^n = 1$. Hence, λ is also an nth root of unity distinct from 1, *i.e.*, λ is a root of $\sum_{i=0}^{n-1} z^i$. Therefore, λ is a root of $\gcd\left(\sum_{i=0}^{m-1} z^i, \sum_{i=0}^{n-1} z^i\right) = \sum_{i=0}^{q-1} z^i$, where $q = \gcd(m, n)$. ■

When λ is an $(m+2)$th root of unity, things get a little more complicated.

LEMMA 9. *If λ is a root of $\phi(z)$ that is also a root of $\sum_{i=0}^{m+1} z^i$, then*
(i) m is even,
(ii) λ is a root of $z^r + 1$, where $r = \gcd(\frac{m}{2} + 1, n + 1)$, and
(iii) $(n+1)/r$ is odd.

Proof: Let λ be as in the hypothesis of the lemma. Again, the fact that $f(\lambda) = 0$ leads to (15). This time, since $\lambda \neq 1$ is an $(m+2)$th root of unity, we have $\sum_{i=0}^{m+1} \lambda^i = 0$ which implies that $-\sum_{i=0}^{m} \lambda^i = \lambda^{m+1} = 1/\lambda$, using $\lambda^{m+2} = 1$. Therefore, (15) reduces to $\lambda^n + 1/\lambda = 0$ or equivalently, $\lambda^{n+1} = -1$.

Now, since λ is a root of $\sum_{i=0}^{m+1} z^i$, it is of the form $\lambda = e^{2\pi i \frac{k}{m+2}}$ for some $k \in \{1, 2, \ldots, m+1\}$. Therefore, $-1 = \lambda^{n+1} = e^{2\pi i \frac{k}{m+2}(n+1)}$. Hence, $\frac{2k}{m+2}(n+1) = 2j+1$ for some integer j, which upon re-arrangement becomes

$$(2k)(n+1) = (2j+1)(m+2) \tag{16}$$

Since the left-hand side of the above equation is even, so is the right-hand side. This means that m must be even, since $2j+1$ is odd. This proves (i).

Re-arranging (16), we get $k\frac{n+1}{m/2+1} = 2j+1$. Defining r to be $\gcd(\frac{m}{2}+1, n+1)$, we let $m' = (\frac{m}{2}+1)/r$ and $n' = (n+1)/r$. Thus, m', n' are integers such that $\gcd(m', n') = 1$, and $\frac{n+1}{m/2+1} = \frac{n'}{m'}$. Therefore, we have

$$k\frac{n'}{m'} = 2j+1 \tag{17}$$

Since $\gcd(m', n') = 1$, the fact that $k\frac{n'}{m'}$ is an integer implies that $m'|k$. Writing $k = lm'$ and plugging into (17), we get $ln' = 2j+1$. Therefore, $n'|(2j+1)$ which shows that n' is odd, thus proving (iii). Note that as $l|(2j+1)$, l is also odd.

Finally, $\lambda = e^{2\pi i \frac{k}{m+2}} = e^{\pi i \frac{k}{m/2+1}} = e^{\pi i \frac{lm'}{rm'}} = e^{\pi i \frac{l}{r}}$. Since l is odd, $\lambda^r = -1$, which shows that λ is a root of $z^r + 1$, thus completing the proof of the lemma. ■

Now, from Lemmas 7, 8 and 9, we see that every root of $\phi(z)$ is also a root of $(\sum_{i=0}^{q-1} z^i)(z^r+1)$. In fact, for odd m, Lemma 9 (i) shows that no root of $\phi(z)$ can be a root of z^r+1, so that every root of $\phi(z)$ is actually a root of $\sum_{i=0}^{q-1} z^i$. Now, if we can show that $\phi(z)$ has no repeated roots, it immediately follows that $\phi(z)$ is a factor of $\sum_{i=0}^{q-1} z^i$ for odd m, and of $(\sum_{i=0}^{q-1} z^i)(z^r+1)$ for even m. We proceed to show this next.

LEMMA 10. *$\phi(z)$ has no repeated roots.*

Proof: Suppose that λ is a repeated root of $\phi(z)$. Note that $|\lambda| = 1$ since any root of $\phi(z)$ is some root of unity. Define $g(z) = (z-1)f(z) = z^{n+1} - z^n - z^{m+1} + 1$. If λ is a repeated root of $\phi(z)$, then it must be a repeated root of $g(z)$ as well. Hence, $g(\lambda) = g'(\lambda) = 0$, which implies that

$$\lambda^{n+1} - \lambda^n - \lambda^{m+1} + 1 = 0 \tag{18}$$

$$(n+1)\lambda^n - n\lambda^{n-1} - (m+1)\lambda^m = 0 \tag{19}$$

Multiplying (18) by $(n+1)$ and subtracting the result from λ times (19), we get

$$\lambda^n + (n-m)\lambda^{m+1} = n+1 \tag{20}$$

But, this leads to a contradiction because

$$n+1 = |\lambda^n + (n-m)\lambda^{m+1}| \leq |\lambda|^n + (n-m)|\lambda|^{m+1} = 1 + n - m \leq n,$$

with the last inequality arising from the fact that $m > 0$. This contradiction proves the lemma. ■

As observed prior to the statement of Lemma 10, we can now conclude that $\phi(z)$ is a factor of $\sum_{i=0}^{q-1} z^i$ for odd m, and of $(\sum_{i=0}^{q-1} z^i)(z^r+1)$ for even m.

In fact, for odd m, we can show that $\phi(z) = \sum_{i=0}^{q-1} z^i$. Since we already know that $\phi(z)|(\sum_{i=0}^{q-1} z^i)$ in this case, we only need to show that $(\sum_{i=0}^{q-1} z^i)|\phi(z)$. It actually suffices to show that $(\sum_{i=0}^{q-1} z^i)|f(z)$. This is because any factor, irreducible or otherwise, of $\sum_{i=0}^{q-1} z^i$ is always self-reciprocal (recall that $\phi(z)$ is the product of all irreducible self-reciprocal factors of $f(z)$): if $\pi(z)$ is a factor of $\sum_{i=0}^{q-1} z^i$ and λ is a root of $\pi(z)$, then so is its complex conjugate, $\overline{\lambda} = \lambda^{-1}$.

So, to show that $(\sum_{i=0}^{q-1} z^i)|f(z)$, we write $n = n'q$, $m = m'q$, so that

$$\begin{aligned}
f(z) &= z^{n'q} - \sum_{i=0}^{m'q} z^i \\
&= z^{n'q} - z^{m'q} - \sum_{i=0}^{m'q-1} z^i \\
&= z^{m'q}(z^{(n'-m')q} - 1) - \left(\sum_{i=0}^{q-1} z^i\right)\left(\sum_{l=0}^{m'-1} z^{lq}\right) \\
&= z^{m'q}(z^q - 1)\left(\sum_{l=0}^{n'-m'-1} z^{lq}\right) - \left(\sum_{i=0}^{q-1} z^i\right)\left(\sum_{l=0}^{m'-1} z^{lq}\right) \\
&= z^{m'q}(z-1)\left(\sum_{i=0}^{q-1} z^i\right)\left(\sum_{l=0}^{n'-m'-1} z^{lq}\right) - \left(\sum_{i=0}^{q-1} z^i\right)\left(\sum_{l=0}^{m'-1} z^{lq}\right) \\
&= \left(\sum_{i=0}^{q-1} z^i\right)\left(z^{m'q}(z-1)\sum_{l=0}^{n'-m'-1} z^{lq} - \sum_{l=0}^{m'-1} z^{lq}\right) \\
&= \left(\sum_{i=0}^{q-1} z^i\right)\left(\sum_{l=m'}^{n'-1} z^{lq+1} - \sum_{l=0}^{n'-1} z^{lq}\right) \qquad (21)
\end{aligned}$$

Thus, we have proved that $(\sum_{i=0}^{q-1} z^i)|f(z)$, which implies that $\phi(z) = \sum_{i=0}^{q-1} z^i$. Note that the factorization in (21) is true for any m and n, not just for odd m. However, odd m ensures that $\sum_{i=0}^{q-1} z^i$ is the reciprocal part of $f(z)$ and the other factor is the non-reciprocal part.

The above argument, in conjunction with Proposition 6, proves the following theorem.

THEOREM 11. *Let $f(z) = z^n - \sum_{i=0}^{m} z^i$, $n > m > 0$, m odd, and let $q = \gcd(m,n)$. Then, $f(z) = \left(\sum_{i=0}^{q-1} z^i\right)\psi(z)$, with $\psi(z) = \sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}$ irreducible. In particular, for odd m, $f(z)$ is irreducible if and only if $\gcd(m,n) = 1$.*

We next tackle the case when m is even, which is a little less clean. The first observation to be made here is that when $(n+1)/r$ is also even, where $r = \gcd(\frac{m}{2} + 1, n+1)$, then it follows from Lemma 9 (iii) that $\phi(z)$ cannot share any roots with $\sum_{i=0}^{m+1} z^i$. So, it must share all its roots with $\sum_{i=0}^{q-1} z^i$, q being $\gcd(m,n)$ as above, implying that $\phi(z)|\sum_{i=0}^{q-1} z^i$. So, applying the argument given prior to the statement of Theorem 11, we see that in this case as well, we have $f(z) = \left(\sum_{i=0}^{q-1} z^i\right)\psi(z)$, with $\psi(z)$ irreducible and of the form stated in the theorem. This situation holds,

for example, when n is odd and $4|m$, since then $\frac{m}{2}+1$ is odd, and so is r because $r|(\frac{m}{2}+1)$, leading to the conclusion that $(n+1)/r$ is even.

So, we are left with the case when m is even, but $(n+1)/r$ is odd. This is dealt with in the following proposition.

PROPOSITION 12. *When m is even and $(n+1)/r$ is odd, then $\phi(z)$ is the least common multiple (lcm) of $\sum_{i=0}^{q-1} z^i$ and z^r+1.*

Proof: From Lemmas 7, 8 and 9, we know that $\phi(z)$ is a factor of $\phi_1(z)\phi_2(z)$, where we have defined $\phi_1(z) = z^r+1$ and $\phi_2(z) = \sum_{i=0}^{q-1} z^i$. In fact, as $\phi(z)$ has no repeated roots, it must be a factor of $\frac{\phi_1(z)\phi_2(z)}{\gcd(\phi_1(z),\phi_2(z))} = \mathrm{lcm}(\phi_1(z),\phi_2(z))$, since dividing by $\gcd(\phi_1(z),\phi_2(z))$ takes out some roots common to $\phi_1(z)$ and $\phi_2(z)$.

So, we need to show the converse, *i.e.*, that $\mathrm{lcm}(\phi_1(z),\phi_2(z))$ is a factor of $\phi(z)$. Equivalently, we need to show that $\phi_1(z)|\phi(z)$ and $\phi_2(z)|\phi(z)$. Recalling that $\phi(z)$ is the product of all the irreducible self-reciprocal factors of $f(z)$, it suffices to show that $\phi_1(z)|f(z)$ and $\phi_2(z)|f(z)$. This is because any factor, irreducible or otherwise, of either $\phi_1(z)$ or $\phi_2(z)$ is self-reciprocal. Indeed, if $\pi(z)$ is a factor of either polynomial and λ is a root of $\pi(z)$, then so is its complex conjugate $\overline{\lambda}$. But as λ, being a root of $\phi_1(z)$ or $\phi_2(z)$, lies on the unit circle, we have $\overline{\lambda} = \lambda^{-1}$, implying that $\pi(z)$ is self-reciprocal.

We have already seen (equation (21)) that $\phi_2(z)|f(z)$. To prove that $\phi_1(z)|f(z)$, we shall show that $f(\lambda)=0$ for any root λ of $\phi_1(z)$, which is sufficient because $\phi_1(z)$ has no repeated roots. Since $\lambda \notin \{0,1\}$, it is enough to show that $\lambda(\lambda-1)f(\lambda)=0$, *i.e.*, $\lambda^{n+2}-\lambda^{n+1}-\lambda^{m+2}+\lambda = 0$. Now, $\lambda^{n+1} = (\lambda^r)^{(n+1)/r} = (-1)^{(n+1)/r} = -1$ as $(n+1)/r$ is odd. Moreover, defining $m' = (\frac{m}{2}+1)/r$, we have $\lambda^{m+2} = (\lambda^r)^{2m'} = (-1)^{2m'} = 1$. Hence, $\lambda^{n+2}-\lambda^{n+1}-\lambda^{m+2}+\lambda = -\lambda-(-1)-1+\lambda = 0$, as desired. ■

The next lemma explicitly determines the lcm of $\sum_{i=0}^{q-1} z^i$ and z^r+1.

LEMMA 13. *If q is even, then*

$$\mathrm{lcm}\Big(\sum_{i=0}^{q-1} z^i, z^r+1\Big) = \frac{z^r+1}{z+1}\sum_{i=0}^{q-1} z^i = \left(\sum_{i=0}^{r-1}(-z)^i\right)\left(\sum_{i=0}^{q-1} z^i\right)$$

Otherwise,

$$\mathrm{lcm}\Big(\sum_{i=0}^{q-1} z^i, z^r+1\Big) = (z^r+1)\sum_{i=0}^{q-1} z^i$$

Proof: Let $\phi_1(z) = z^r+1$ and $\phi_2(z) = \sum_{i=0}^{q-1} z^i$. Since $\gcd(\phi_1,\phi_2)\cdot\mathrm{lcm}(\phi_1,\phi_2) = \phi_1(z)\phi_2(z)$, the lemma is proved once we show that $\gcd(\phi_1,\phi_2)$ is $z+1$ if q is even, and 1 otherwise.

We first show that if $\gcd(\phi_1,\phi_2) \neq 1$, then q is even, and $\gcd(\phi_1,\phi_2) = z+1$. Suppose that $\pi(z)$ is a non-trivial factor of both $\phi(z)$ and $\phi_2(z)$, so that there exists a λ such that $\phi_1(\lambda) = \phi_2(\lambda) = 0$. Such a λ must be of the form $\lambda = e^{2\pi i\frac{k}{q}}$ for some $k \in \{1,2,\ldots,q-1\}$, and must satisfy $\lambda^r = -1$. Hence, $e^{2\pi i\frac{kr}{q}} = -1$, which means that $2k\frac{r}{q}$ must be an odd integer.

Now, as $q|n$ and $r|(n+1)$, $\gcd(q,r)=1$. So, for $2k\frac{r}{q}$ to be an integer, $2k$ must be a multiple of q. Let $2k=ql$, so that $2k\frac{r}{q}=lr$. Thus, lr is an odd integer, which shows that r and l are both odd. Furthermore, since $2k=ql$, the fact that l is odd implies that q is even. In fact, this also forces λ to be -1, because $\lambda=e^{2\pi i\frac{k}{q}}=e^{\pi il}=-1$, since l is odd.

Thus, if $\pi(z)$ is a non-trivial factor of both $\phi_1(z)$ and $\phi_2(z)$, then $\lambda=-1$ is the only root that $\pi(z)$ can have. Since neither $\phi_1(z)$ nor $\phi_2(z)$ has repeated roots, -1 must be a simple root of $\pi(z)$, which shows that $\pi(z)=z+1$. We have thus shown that if $\gcd(\phi_1,\phi_2)$ is non-trivial, then q is even and $\gcd(\phi_1,\phi_2)=z+1$.

It only remains to show that if q is even, then $\gcd(\phi_1,\phi_2)=z+1$. Note that if $q=\gcd(m,n)$ is even, then so is n. Therefore, $n+1$ is odd, and since $r|(n+1)$, so is r. But, for even q and odd r, it is clear that $\phi_1(-1)=\phi_2(-1)=0$. Hence, $(z+1)|\gcd(\phi_1,\phi_2)$, meaning that $\gcd(\phi_1,\phi_2)$ is non-trivial. But as we have already shown, this implies that $\gcd(\phi_1,\phi_2)=z+1$. ■

We compile all the results proved above for the case when m is even in the following theorem.

THEOREM 14. *Let $f(z)=z^n-\sum_{i=0}^{m}z^i$, $n>m>0$, m even, and let $q=\gcd(m,n)$, $r=\gcd(\frac{m}{2}+1,n+1)$, $n'=(n+1)/r$. Then, $f(z)=\phi(z)\psi(z)$, where $\psi(z)$ is irreducible and*

$$\phi(z)=\begin{cases}\sum_{i=0}^{q-1}z^i & \text{if } n' \text{ is even}\\ \left(\sum_{i=0}^{r-1}(-z)^i\right)\left(\sum_{i=0}^{q-1}z^i\right) & \text{if } q \text{ is even}\\ (z^r+1)\sum_{i=0}^{q-1}z^i & \text{otherwise.}\end{cases}$$

We would like to remark that when q is even, $n'=(n+1)/r$ is odd, so that the statement of the theorem is indeed consistent.

At this stage, it is worth pointing out that the results of Theorems 11 and 14 can be partially obtained from results in the existing literature, specifically [4] and [6]. Observe that, as noted in the proof of Lemma 10, we may define $g(z)=(z-1)f(z)=z^{n+1}-z^n-z^{m+1}+1$. Now, Ljunggren [4] considered the factorization of polynomials of the form $q(x)=x^n\pm x^m\pm x^p\pm 1$ with $n>m>p>0$, and claimed to show that all such polynomials can be factored as $q(x)=\phi(x)\psi(x)$, where $\phi(x)$ is self-reciprocal and has all its zeros on the unit circle, and $\psi(x)$ is either 1 or a non self-reciprocal irreducible polynomial. However, there was a minor error in Ljunggren's work, which was subsequently corrected by Mills [6]. Mills' work shows that Ljunggren's claim is in fact true for any polynomial $g(z)$ as above. Since $m+1\geq 2$, $g(z)$ is not self-reciprocal and hence, must have a non-trivial non-reciprocal part $\psi(z)$. Thus, these results show that $g(z)$, and hence $f(z)$, can be written as the product of a self-reciprocal polynomial having all its roots on the unit circle and a non-trivial, irreducible, non self-reciprocal polynomial. Of course, these results do not go so far as to provide the specific forms of the reciprocal and non-reciprocal parts of $f(z)$ that we have derived above. So, in the interest of keeping our paper self-contained, we have chosen to include complete proofs of the aforementioned theorems.

3. Identifying Equalities Among (d,k) Capacities. We shall use the factorization obtained in the previous section for the characteristic polynomials of (d,k) constraints to determine all possible equalities among the capacities of such constraints.

We begin by showing that this problem is equivalent to the one of determining when the non-reciprocal parts of the characteristic polynomials of two such constraints can be equal. Throughout this section, we consider (d,k) pairs such that $0 < d < k \leq \infty$, and $\Phi_{d,k}(z)$ and $\Psi_{d,k}(z)$ will be used to denote the reciprocal and non-reciprocal parts, respectively, of the characteristic polynomial $\chi_{d,k}(z)$. Also, given polynomials $f(z), g(z)$ we shall use $f(z) = g(z)$ to denote that the two polynomials are identical.

THEOREM 15. *$C(d,k) = C(\hat{d},\hat{k})$ if and only if $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$.*

Proof: We shall show that $\rho_{d,k} = \rho_{\hat{d},\hat{k}}$ if and only if $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$, the ρ's being the largest roots of their respective characteristic polynomials.

Observe first that since the reciprocal parts of the characteristic polynomials have all their roots on the unit circle, and the ρ's are strictly greater than 1, the ρ's must be roots of the non-reciprocal parts. So, if $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$, then their largest roots must be identical, *i.e.*, $\rho_{d,k} = \rho_{\hat{d},\hat{k}}$.

Conversely, suppose that $\rho_{d,k} = \rho_{\hat{d},\hat{k}}$. Since $\Psi_{d,k}(z)$ is irreducible and has $\rho_{d,k}$ as a root, it must be the minimal polynomial (over $\mathbb{Z}$) of $\rho_{d,k}$. Similarly, $\Psi_{\hat{d},\hat{k}}(z)$ is the minimal polynomial of $\rho_{\hat{d},\hat{k}}$. Hence, by the uniqueness of the minimal polynomial of an algebraic integer, $\rho_{d,k} = \rho_{\hat{d},\hat{k}}$ implies that $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$. ■

With this theorem in hand, we can begin our investigation of equalities among the capacities of (d,k)-constrained systems. We shall first consider the case when at least one of the (d,k) constraints has $k = \infty$. Observe that since $\Psi_{d,\infty}(z)$ is either $\chi_{d,\infty}(z)$ itself or of the form given in (7), we can have $C(d,\infty) = C(\hat{d},\infty)$, or equivalently, $\Psi_{d,\infty}(z) = \Psi_{\hat{d},\infty}(z)$, if and only if $d = \hat{d}$. So, we need only concern ourselves with the situation when $C(d,\infty) = C(\hat{d},\hat{k})$ with $\hat{k}$ finite.

At this point, we shall find it convenient to introduce some definitions.

DEFINITION 16. *A polynomial $f(z) = z^n - \sum_{i=0}^{m} z^i$, $n > m > 0$, is defined as being of*

- Type I *if its reciprocal part, $\phi(z)$, is of the form $\sum_{i=0}^{q-1} z^i$, with $q \geq 1$ odd;*
- Type II *if $\phi(z)$ is of the form $(z^r+1)\sum_{i=0}^{q-1} z^i$, with $q \geq 1$ odd, $r \geq 1$; and*
- Type III *if $\phi(z)$ is of the form $\left(\sum_{i=0}^{r-1}(-z)^i\right)\left(\sum_{i=0}^{q-1} z^i\right)$, with $q \geq 2$ even, and $r \geq 3$ odd.*

Theorems 11 and 14 show that any such $f(z)$ is always of Type I, II or III, with $q = \gcd(m,n)$ and $r = \gcd(\frac{m}{2}+1, n+1)$. These theorems can be used to determine exactly when $f(z)$ is of a particular type. For example, $f(z)$ is of Type I precisely when one of the following three conditions holds: (i) m is odd, (ii) m and $(n+1)/r$ are even, and (iii) m and n are even, and $r = 1$. Note that when $f(z)$ is of Type I, its non-reciprocal part, $\psi(z)$ is of the form $\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}$, as shown by (21).

The following simple fact about $f(z)$'s of Type II or III will be used often.

LEMMA 17. *Let m be even and let $f(z)$ be of Type II or III. If $q = \gcd(m,n)$ and $r = \gcd(\frac{m}{2}+1, n+1)$, then $q \neq r$.*

Proof: If $q = r$, then $f(z)$ cannot be of Type III, since the definition requires q to be even and r to be odd. So, suppose that $f(z)$ is of Type II, with $q = r$. Note

that since $q|n$ and $r|(n+1)$, we must have $\gcd(q,r)=1$, and hence, $q=r=1$. As $z^r+1=z+1$ is a factor of $f(z)$, we must have $f(-1)=0$. Now, it is easily verified that since $f(z)$ has the form $z^n-\sum_{i=0}^{m} z^i$, $f(-1)$ can be 0 only if m and n are both even. So, $q=\gcd(m,n)$ is even, which is impossible since $q=1$. ■

We will also find the following set of definitions to be useful.

DEFINITION 18. *Given a polynomial $g(z)=\sum_{k=0}^{n} c_k z^k$, we define*

- *$\epsilon_i(g)$, $i\geq 1$, to be the ith smallest $k>0$ such that $c_k\neq 0$.*
- *$\xi_i(g)$, $i\geq 1$, to be the ith largest $k>0$ such that $c_k\neq 0$.*

Thus, for example, with $g(z)=z^6-z^3-z^2-z-1$, we have $\epsilon_i(g)=i$ for $i=1,2,3$, $\epsilon_4(g)=6$, $\xi_1(g)=6$ and $\xi_i(g)=5-i$ for $i=2,3,4$. Note that if $g(z),h(z)$ are polynomials such that $g(z)=h(z)$, then $\epsilon_i(g)=\epsilon_i(h)$ and $\xi_i(g)=\xi_i(h)$ for all $i\geq 1$.

We tackle the equality $C(d,\infty)=C(\hat{d},\hat{k})$ through a series of lemmas, each of which considers a special case in which $\chi_{d,\infty}(z)$ is either irreducible ($d\not\equiv 4 \pmod 6$) or reducible ($d\equiv 4 \pmod 6$), and $\chi_{\hat{d},\hat{k}}(z)$ is of one of the three types defined above.

LEMMA 19. *Let $d\not\equiv 4 \pmod 6$ and $\hat{d},\hat{k}$ be such that $\chi_{\hat{d},\hat{k}}(z)$ is of Type I. Then, $C(d,\infty)=C(\hat{d},\hat{k})$ only if $(\hat{d},\hat{k})=(d-1,2d-1)$.*

Proof: Let $\hat{n}=\hat{k}+1$, $\hat{m}=\hat{k}-\hat{d}$, so that $\chi_{\hat{d},\hat{k}}(z)=z^{\hat{n}}-\sum_{i=0}^{\hat{m}} z^i$, and let $\hat{q}=\gcd(\hat{m},\hat{n})$. Under the assumptions of the lemma, $\Psi_{d,\infty}(z)=\chi_{d,\infty}(z)=z^{d+1}-z^d-1$, and $\Psi_{\hat{d},\hat{k}}(z)=\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1}-\sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}$.

If $C(d,\infty)=C(\hat{d},\hat{k})$, then by Theorem 15, $\Psi_{d,\infty}(z)=\Psi_{\hat{d},\hat{k}}(z)$, *i.e.*

$$z^{d+1}-z^d-1=\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1}-\sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}} \tag{22}$$

Now, note that $\xi_1(\Psi_{d,\infty})=d+1$, while $\xi_1(\Psi_{\hat{d},\hat{k}})=\hat{n}-\hat{q}+1$. Equating these, we get

$$d=\hat{n}-\hat{q} \tag{23}$$

Next, observe that $\epsilon_1(\Psi_{d,\infty})=d$. Additionally, we claim that $\epsilon_1(\Psi_{\hat{d},\hat{k}})=\hat{q}$. This is because the smallest $k>0$ such that the coefficient of z^k in $-\sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}$ is non-zero is precisely $\hat{q}$, and the term $-z^{\hat{q}}$ cannot be cancelled out by any term in $\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1}$. The reason that $-z^{\hat{q}}$ cannot get cancelled out is that the smallest exponent of z in $\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1}$ is $\hat{m}+1$, which is larger than $\hat{q}$, since $\hat{q}=\gcd(\hat{m},\hat{n})$. Therefore, equating $\epsilon_1(\Psi_{d,\infty})$ and $\epsilon_1(\Psi_{\hat{d},\hat{k}})$, we get

$$d=\hat{q} \tag{24}$$

From (23) and (24), we see that $\hat{n}=2d$. Plugging this and $\hat{q}=d$ into (22), we get $z^{d+1}-z^d-1=\sum_{l=\frac{\hat{m}}{d}}^{1} z^{ld+1}-z^d-1$. It follows that $\hat{m}=d$, and since $(\hat{m},\hat{n})=(\hat{k}-\hat{d},\hat{k}+1)$ by definition, the fact that $(\hat{m},\hat{n})=(d,2d)$ implies that $(\hat{d},\hat{k})=(d-1,2d-1)$. ■

The proof of the above lemma involves arguments typical of those used in the proofs to follow. One especially important fact used in the above proof that should be kept in mind is that the function ϵ_1, when applied to the polynomial $\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}$, yields $\hat{q}$. Also, in all that is to follow, we shall continue to take $(\hat{m},\hat{n})$ to be $(\hat{k}-\hat{d},\hat{k}+1)$, and $\hat{q}$ to be $\gcd(\hat{m},\hat{n})$.

LEMMA 20. *If $d \not\equiv 4 \pmod 6$ and $\hat{d},\hat{k}$ are such that $\chi_{\hat{d},\hat{k}}(z)$ is of Type II, then $C(d,\infty) \neq C(\hat{d},\hat{k})$.*

Proof: With $d,\hat{d},\hat{k}$ as in the statement of the lemma, we have $\Psi_{d,\infty}(z) = z^{d+1} - z^d - 1$, and

$$\Psi_{\hat{d},\hat{k}}(z) = \frac{\chi_{\hat{d},\hat{k}}(z)}{\Phi_{\hat{d},\hat{k}}(z)} = \frac{z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i}{(z^{\hat{r}}+1)\sum_{i=0}^{\hat{q}-1} z^i} = \frac{\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}}{z^{\hat{r}}+1}$$

where $\hat{r} = \gcd(\frac{\hat{n}}{2}+1, \hat{n}+1)$, and the last equality above comes from (21).

Suppose that $C(d,\infty) = C(\hat{d},\hat{k})$, so that $\Psi_{d,\infty}(z) = \Psi_{\hat{d},\hat{k}}(z)$. Since the Ψ's are as given above, we have $(z^{\hat{r}}+1)(z^{d+1}-z^d-1) = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}$, which upon expanding out the left-hand side (LHS) becomes

$$z^{d+\hat{r}+1} + z^{d+1} - z^{d+\hat{r}} - z^{\hat{r}} - z^d - 1 = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}} \tag{25}$$

Our goal is to show that such an equality cannot arise for any $d,\hat{d},\hat{k}$ satisfying the hypothesis of the lemma, leading to a contradiction that proves the lemma.

Applying ξ_1 to both sides of (25), we get $d+\hat{r}+1 = \hat{n}-\hat{q}+1$, implying

$$d + \hat{r} = \hat{n} - \hat{q} \tag{26}$$

Next, note that the function ϵ_1, when applied to the RHS of (25), yields $\hat{q}$, and when applied to the LHS, yields either d or $\hat{r}$, depending on whether $d \leq \hat{r}$ or $d > \hat{r}$. So, if $d \leq \hat{r}$, then $d = \hat{q}$, and if $d > \hat{r}$, then $\hat{q} = \hat{r}$. However, we cannot have $d > \hat{r}$, since $\hat{q} = \hat{r}$ is ruled out by Lemma 17.

Thus, we see that $d \leq \hat{r}$, so that $d = \hat{q}$. Plugging this into (26), we get $\frac{\hat{n}}{\hat{q}} = 2 + \frac{\hat{r}}{d}$. Using this and $d = \hat{q}$, the RHS of (25) becomes

$$\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{r}}{d}+1} z^{ld+1} - \sum_{l=0}^{\frac{\hat{r}}{d}+1} z^{ld} = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{r}}{d}} z^{ld+1} - \sum_{l=0}^{\frac{\hat{r}}{d}} z^{ld} + z^{d+\hat{r}+1} - z^{d+\hat{r}}$$

Therefore, upon cancelling out some terms common to both sides, (25) simplifies to $z^{d+1} - z^{\hat{r}} - z^d - 1 = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{r}}{d}} z^{ld+1} - \sum_{l=0}^{\frac{\hat{r}}{d}} z^{ld}$. Applying ξ_1 to both sides of this equality, we get $d+1 = \hat{r}+1$, *i.e.*, $d = \hat{r}$. We thus have $\hat{q} = d = \hat{r}$, which is impossible by Lemma 17. ■

LEMMA 21. *If $d \not\equiv 4 \pmod 6$ and $\hat{d}, \hat{k}$ are such that $\chi_{\hat{d},\hat{k}}(z)$ is of Type III, then $C(d,\infty) \neq C(\hat{d},\hat{k})$.*

Proof: An argument similar to that at the beginning of the proof of Lemma 20 shows that if $C(d,\infty) = C(\hat{d},\hat{k})$, with $d, \hat{d}, \hat{k}$ as above, then

$$\left(\sum_{i=0}^{\hat{r}-1}(-z)^i\right)(z^{d+1} - z^d - 1) = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}$$

Equivalently, multiplying both sides by $z+1$, we have

$$(z^{\hat{r}}+1)(z^{d+1} - z^d - 1) = (z+1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right)$$

Expanding out both sides of the above equation, we get

$$z^{d+\hat{r}+1} + z^{d+1} - z^{d+\hat{r}} - z^{\hat{r}} - z^d - 1 = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+2} - \sum_{l=0}^{\frac{\hat{m}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}} \qquad (27)$$

Now, by definition of Type III, $\hat{r} \geq 3$, so that the term $-z^{d+\hat{r}}$ on the LHS of the above equation cannot get cancelled out by another term on the LHS. Therefore, the RHS must also have a $-z^{d+\hat{r}}$ term, and due to the negative sign, it must be one of the terms in $-\sum_{l=0}^{\frac{\hat{m}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}$. In other words, $d+\hat{r}$ must be one of the exponents of z in these two summations. Observe that the maximum exponent of z in these summations is $\max(\hat{m}-\hat{q}+1, \hat{n}-\hat{q}) = \max(\hat{m}+1,\hat{n}) - \hat{q} = \hat{n}-\hat{q}$, since $\hat{n} > \hat{m}$. Therefore, $d+\hat{r} \leq \hat{n}-\hat{q}$.

However, if we apply ξ_1 to both sides of (27), we find that $d+\hat{r}+1 = \hat{n}-\hat{q}+2$, so that $d+\hat{r} = \hat{n}-\hat{q}+1$, which contradicts $d+\hat{r} \leq \hat{n}-\hat{q}$. So, (27) cannot hold under the assumptions of the lemma, implying that $C(d,\infty)$ cannot be equal to $C(\hat{d},\hat{k})$. ■

The last three lemmas show that when $d \not\equiv 4 \pmod 6$, then $C(d,\infty) = C(\hat{d},\hat{k})$ only if $(\hat{d},\hat{k}) = (d-1, 2d-1)$. The next three lemmas consider the case when $d \equiv 4 \pmod 6$. Recall that for any such d, $\Psi_{d,\infty}(z)$ is as given in (7).

LEMMA 22. *Let $d \equiv 4 \pmod 6$ and $\hat{d}, \hat{k}$ be such that $\chi_{\hat{d},\hat{k}}(z)$ is of Type I. Then, $C(d,\infty) = C(\hat{d},\hat{k})$ only if $d = 4$ and $(\hat{d},\hat{k}) = (1,2)$.*

Proof: If $C(d,\infty) = C(\hat{d},\hat{k})$ with $d, \hat{d}, \hat{k}$ as above, then we have

$$z^3 - z - 1 + \sum_{l=2}^{(d+2)/6} (z^{6l-3} - z^{6l-5} - z^{6l-6} + z^{6l-8}) = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}} \qquad (28)$$

Applying ϵ_1 to both sides of this equation, we get $1 = \hat{q}$. Therefore, $\Phi_{\hat{d},\hat{k}}(z) = \sum_{i=0}^{\hat{q}-1} z^i = 1$, and hence $\Psi_{\hat{d},\hat{k}}(z) = \chi_{\hat{d},\hat{k}}(z)$. Thus, we must have $\Psi_{d,\infty}(z) = \chi_{\hat{d},\hat{k}}(z)$.

Now, the polynomial on the LHS of (28) can be of the form $z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i$ only if $d = 4$, since in this case it has no terms of the form $z^{6l-3} - z^{6l-5} - z^{6l-6} + z^{6l-8}$. So, $\Psi_{d,\infty}(z) = \chi_{\hat{d},\hat{k}}(z)$ implies that $d = 4$, in which case $\Psi_{d,\infty} = z^3 - z - 1 = \chi_{1,2}(z)$. Hence, $(\hat{d}, \hat{k}) = (1, 2)$, which proves the lemma. ■

For the proofs of the next couple of lemmas, it is convenient to introduce the following notation: we shall use $\Omega(z^k)$ to denote an arbitrary polynomial of the form $\sum_{i=k}^{l} c_i z^i$, with $l \geq k$.

LEMMA 23. *Let $d \equiv 4 \pmod 6$ and $\hat{d}, \hat{k}$ be such that $\chi_{\hat{d},\hat{k}}(z)$ is of Type II. Then, $C(d, \infty) = C(\hat{d}, \hat{k})$ only if $d = 4$ and $(\hat{d}, \hat{k}) = (2, 4)$.*

Proof: Arguing as in the proof of Lemma 20, we find that for the above choice of $d, \hat{d}, \hat{k}$, $C(d, \infty) = C(\hat{d}, \hat{k})$ implies

$$(z^{\hat{r}} + 1)\left(z^3 - z - 1 + \sum_{l=2}^{(d+2)/6} (z^{6l-3} - z^{6l-5} - z^{6l-6} + z^{6l-8})\right) = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}$$

As usual, we now apply ϵ_1 to both sides of this equation, which yields $1 = \hat{q}$. Hence, $\Phi_{\hat{d},\hat{k}}(z) = (z^{\hat{r}} + 1)\sum_{i=0}^{\hat{q}-1} z^i = z^{\hat{r}} + 1$. Therefore, $\chi_{\hat{d},\hat{k}}(z) = \Phi_{\hat{d},\hat{k}}(z)\Psi_{\hat{d},\hat{k}}(z) = \Phi_{\hat{d},\hat{k}}(z)\Psi_{d,\infty}(z)$, which shows that

$$\chi_{\hat{d},\hat{k}}(z) = (z^{\hat{r}} + 1)\left(z^3 - z - 1 + \sum_{l=2}^{(d+2)/6} (z^{6l-3} - z^{6l-5} - z^{6l-6} + z^{6l-8})\right) \tag{29}$$

Note that since $\hat{q} = 1$, by Lemma 17, $\hat{r} \geq 2$.

Suppose first that $d = 4$, so that $\Psi_{d,\infty}(z) = z^3 - z - 1$. Then, (29) becomes $\chi_{\hat{d},\hat{k}}(z) = (z^{\hat{r}} + 1)(z^3 - z - 1)$, which is the same as

$$\chi_{\hat{d},\hat{k}}(z) = z^{\hat{r}+3} + z^3 - z^{\hat{r}+1} - z^{\hat{r}} - z - 1 \tag{30}$$

Since only the leading coefficient of the polynomial $\chi_{\hat{d},\hat{k}}(z)$ is positive, either $z^{\hat{r}+3}$ or z^3 must be eliminated by one of the other terms on the RHS of (30). As $\hat{r} + 3$ is strictly larger than any other exponent of z on the RHS, z^3 is the term that must get eliminated, and this can happen only if either $\hat{r} = 3$ or $\hat{r} + 1 = 3$, *i.e.*, $\hat{r} = 2$. If $\hat{r} = 3$, then the RHS of (30) turns out to be $z^6 - z^4 - z - 1$, which is not of the form $z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i$. So, we must have $\hat{r} = 2$, in which case the RHS of (30) becomes $z^5 - z^2 - z - 1 = \chi_{2,4}(z)$. So, one possible solution for $C(d, \infty) = C(\hat{d}, \hat{k})$ is $(d, \hat{d}, \hat{k}) = (4, 2, 4)$.

Now, suppose that $d > 4$, so that $d \geq 10$, as 10 is the next largest integer that is equivalent to 4 (mod 6). Then, $\Psi_{d,\infty}(z) = -1 - z + z^3 + z^4 + \Omega(z^5)$, and (29) becomes

$$\chi_{\hat{d},\hat{k}}(z) = z^{\hat{r}+4} + z^{\hat{r}+3} + z^4 + z^3 - z^{\hat{r}+1} - z^{\hat{r}} - z - 1 + \Omega(z^5) \tag{31}$$

Note that if $\hat{r} \geq 5$, then the RHS above becomes $z^4 + z^3 - z - 1 + \Omega(z^5)$, which cannot be of the form $z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i$. So, we must have $\hat{r} = 2$, 3 or 4.

If $\hat{r}=2$, then the RHS of (29) is of the form $z^{d+\hat{r}-1}+\sum_{i=5}^{d+\hat{r}-2}c_iz^i+z^4-z^2-z-1$, which cannot be $\chi_{\hat{d},\hat{k}}(z)$ for any $\hat{d},\hat{k}$. Similarly, if $\hat{r}=4$, then the RHS of (29) is of the form $z^{d+\hat{r}-1}+\sum_{i=5}^{d+\hat{r}-2}c_iz^i+z^3-z-1$, which cannot be any $\chi_{\hat{d},\hat{k}}(z)$.

Finally, if $\hat{r}=3$, then the RHS of (29) becomes $z^{d+\hat{r}-1}+\sum_{i=5}^{d+\hat{r}-2}c_iz^i-z-1$, which can at best be $z^{d+\hat{r}-1}-z-1=z^{d+2}-z-1=\chi_{d,d+1}(z)$. But this too does not yield a solution to $C(d,\infty)=C(\hat{d},\hat{k})$, since it is clear that $C(d,\infty)\neq C(d,d+1)$ for any d. This completes the analysis of the $d>4$ case, and hence the proof of the lemma. ■

LEMMA 24. *Let $d\equiv 4 \pmod 6$ and $\hat{d},\hat{k}$ be such that $\chi_{\hat{d},\hat{k}}(z)$ is of Type III. Then, $C(d,\infty)=C(\hat{d},\hat{k})$ only if $(\hat{d},\hat{k})=(d-1,2d-1)$.*

Proof: With $d,\hat{d},\hat{k}$ as in the above statement, if $C(d,\infty)=C(\hat{d},\hat{k})$, then the usual argument shows that we must have

$$\left(\sum_{i=0}^{\hat{r}-1}(-z)^i\right)\Psi_{d,\infty}(z)=\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1}z^{l\hat{q}+1}-\sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1}z^{l\hat{q}} \tag{32}$$

with $\Psi_{d,\infty}(z)$ having the form given in (7).

Note that as $\chi_{\hat{d},\hat{k}}(z)$ is of Type III, we must have $\hat{r}\geq 3$ odd. Suppose first that $\hat{r}=3$. Then the LHS of the above equation is $(z^2-z+1)\Psi_{d,\infty}(z)=\chi_{d,\infty}(z)=z^{d+1}-z^d-1$ by Theorem 3. Therefore, (32) in this case is identical to (22) in the proof of Lemma 19. As analyzed there, this equation implies $(\hat{d},\hat{k})=(d-1,2d-1)$.

So, we are left with the case $\hat{r}\geq 5$. Note that the LHS of (32) may be written as

$$\begin{aligned}\left(z^2-z+1+\sum_{i=3}^{\hat{r}-1}(-z)^i\right)\Psi_{d,\infty}(z)&=(z^2-z+1)\Psi_{d,\infty}(z)-z^3\left(\sum_{i=0}^{\hat{r}-4}(-z)^i\right)\Psi_{d,\infty}(z)\\&=z^{d+1}-z^d-1-z^3\left(\sum_{i=0}^{\hat{r}-4}(-z)^i\right)\Psi_{d,\infty}(z)\end{aligned}$$

Therefore, if we multiply both sides of (32) by $\sum_{i=0}^{\hat{q}-1}z^i$, and use (21), then the resulting equation can be written as

$$\begin{aligned}\chi_{\hat{d},\hat{k}}(z)&=(z^{d+1}-z^d-1)\sum_{i=0}^{\hat{q}-1}z^i-z^3\left(\sum_{i=0}^{\hat{r}-4}(-z)^i\right)\Psi_{d,\infty}(z)\sum_{i=0}^{\hat{q}-1}z^i\\&=z^{d+\hat{q}}-z^d-\sum_{i=0}^{\hat{q}-1}z^i+z^3+\Omega(z^4)\end{aligned} \tag{33}$$

where we have used the fact that $(z^{d+1}-z^d-1)\sum_{i=0}^{\hat{q}-1}z^i=z^{d+\hat{q}}-z^d-\sum_{i=0}^{\hat{q}-1}z^i$.

Now, the fact that $\hat{r}=\gcd(\frac{\hat{m}}{2}+1,\hat{n}+1)\geq 5$ implies that $\frac{\hat{m}}{2}+1\geq 5$ which means that $\hat{m}\geq 8$. Therefore, $\chi_{\hat{d},\hat{k}}(z)=z^{\hat{n}}-\sum_{i=0}^{\hat{m}}z^i$ must contain the sequence $-z^8-z^7-\ldots-z-1$. In particular, the coefficient of z^3 in $\chi_{\hat{d},\hat{k}}(z)$ is -1. However, on the RHS of (33), there are at most two z^3 terms, one of which is $+z^3$, and the other is $-z^3$ from the summation $-\sum_{i=0}^{\hat{q}-1}z^i$ if $\hat{q}-1\geq 3$. So, the coefficient of z^3 on

the RHS of (33) can either be 0 or +1, which implies that the RHS cannot be of the form required by $\chi_{\hat{d},\hat{k}}(z)$. Therefore, we cannot have $C(d,\infty) = C(\hat{d},\hat{k})$ when $\hat{r} \geq 5$. ■

Lemmas 19 – 24 together prove the following result, which is the part of Theorem 1 dealing with the case when one of the (d,k) constraints involved is a (d,∞) constraint.

THEOREM 25. *If $d, \hat{d}, \hat{k}$ are non-negative integers such that $C(d,\infty) = C(\hat{d},\hat{k})$, then one of the following holds:*
(i) $(\hat{d},\hat{k}) = (d-1, 2d-1)$,
(ii) $d = 4$ *and* $(\hat{d},\hat{k})$ *is either* $(1,2)$ *or* $(2,4)$.

We now move on to analyze the equality $C(d,k) = C(\hat{d},\hat{k})$ when $k, \hat{k}$ are both finite. Once again, we perform a case-by-case analysis of the various situations that arise when each of the characteristic polynomials involved is of one of the three types defined earlier. Because of symmetry, there are only six cases to be considered — three when $\chi_{d,k}(z)$ and $\chi_{\hat{d},\hat{k}}(z)$ are of the same type, and three more as follows: (a) $\chi_{d,k}(z)$ of Type I, $\chi_{\hat{d},\hat{k}}(z)$ of Type II, (b) $\chi_{d,k}(z)$ of Type I, $\chi_{\hat{d},\hat{k}}(z)$ of Type III, and (c) $\chi_{d,k}(z)$ of Type II, $\chi_{\hat{d},\hat{k}}(z)$ of Type III.

The situation when $\chi_{d,k}(z)$ and $\chi_{\hat{d},\hat{k}}(z)$ are both of Type I is the easiest to deal with, and we dispose of this first. As usual, we define $(m,n) = (k-d, k+1)$, $(\hat{m},\hat{n}) = (\hat{k}-\hat{d}, \hat{k}+1)$, $q = \gcd(m,n)$ and $\hat{q} = \gcd(\hat{m},\hat{n})$.

LEMMA 26. *Let $d, k, \hat{d}, \hat{k}$ be such that $\chi_{d,k}(z)$ and $\chi_{\hat{d},\hat{k}}(z)$ are both of Type I. Then, $C(d,k) = C(\hat{d},\hat{k})$ only if $(d,k) = (\hat{d},\hat{k})$.*

Proof: By Theorem 15, $C(d,k) = C(\hat{d},\hat{k})$ implies $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$. Since $\chi_{d,k}(z)$ and $\chi_{\hat{d},\hat{k}}(z)$ are both of Type I, we have an explicit form for their non-reciprocal parts, using which we get

$$\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq} = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}} \tag{34}$$

Applying ϵ_1 to both sides of the above equation, we get $q = \hat{q}$. But this means that $\Phi_{d,k}(z) = \sum_{i=0}^{q-1} z^i = \sum_{i=0}^{\hat{q}-1} z^i = \Phi_{\hat{d},\hat{k}}(z)$. Thus, the polynomials $\chi_{d,k}(z)$ and $\chi_{\hat{d},\hat{k}}(z)$ have identical reciprocal parts and identical non-reciprocal parts, which shows that $\chi_{d,k}(z) = \chi_{\hat{d},\hat{k}}(z)$, *i.e.*, $(d,k) = (\hat{d},\hat{k})$. ■

When $\chi_{d,k}(z)$ and $\chi_{\hat{d},\hat{k}}(z)$ are both of Type II or Type III, the analysis involves the use of the following technical lemma, whose proof we defer to the end of this paper.

LEMMA 27. *Let $m, n, r, \hat{m}, \hat{n}, \hat{r}$ be positive integers such that $n > m$, and $\hat{n} > \hat{m}$. If $(z^r+1)\left(z^n - \sum_{i=0}^{m} z^i\right) = (z^{\hat{r}}+1)\left(z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i\right)$, then $(m,n,r) = (\hat{m},\hat{n},\hat{r})$.*

In all that is to follow, we shall take $r = \gcd(\frac{m}{2}+1, n+1)$ and $\hat{r} = \gcd(\frac{\hat{m}}{2}+1, \hat{n}+1)$, whenever $m, \hat{m}$ are even.

LEMMA 28. *Let $d, k, \hat{d}, \hat{k}$ be such that $\chi_{d,k}(z)$ and $\chi_{\hat{d},\hat{k}}(z)$ are either both of Type II*

or both of Type III. Then, $C(d,k) = C(\hat{d},\hat{k})$ only if $(d,k) = (\hat{d},\hat{k})$.

Proof: Suppose first that $\chi_{d,k}(z)$ and $\chi_{\hat{d},\hat{k}}(z)$ are both of Type II. As shown in the proof of Lemma 20, we have

$$\Psi_{d,k}(z) = \frac{\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}}{z^r+1}, \quad \Psi_{\hat{d},\hat{k}}(z) = \frac{\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}}{z^{\hat{r}}+1}$$

Therefore, if $C(d,k) = C(\hat{d},\hat{k})$, then we have $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$, from which it follows that

$$(z^{\hat{r}}+1)\left(\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}\right) = (z^r+1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right) \tag{35}$$

We shall consider the following four cases individually: (i) $r \leq \hat{q}$ and $q < \hat{r}$, (ii) $r \leq \hat{q}$ and $q \geq \hat{r}$, (iii) $r > \hat{q}$ and $q < \hat{r}$, and (iv) $r > \hat{q}$ and $q \geq \hat{r}$. Observe, however, that (iv) is the same as (i), with the roles of (d,k) and $(\hat{d},\hat{k})$ reversed. So, it suffices to consider the first three cases only.

We consider case (i) first. In this case, applying ϵ_1 to both sides of (35), we find that $q = r$, which is impossible by Lemma 17.

In case (ii), applying ϵ_1 to both sides of (35) yields $r = \hat{r}$. Hence, (35) reduces to (34) in the proof of Lemma 26, which as shown in that proof, leads to the conclusion that $(d,k) = (\hat{d},\hat{k})$.

Moving on to case (iii), applying ϵ_1 to (35) here yields $q = \hat{q}$. Hence, multiplying both sides of (35) by $\sum_{i=0}^{q-1} z^i$, we get via (21), $(z^{\hat{r}}+1)\left(z^n - \sum_{i=0}^{m} z^i\right) = (z^r+1)\left(z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i\right)$. But now, Lemma 27 shows that $(m,n) = (\hat{m},\hat{n})$, which implies that $(d,k) = (\hat{d},\hat{k})$ in this case as well. Thus, we have shown that when $\chi_{d,k}(z)$ and $\chi_{\hat{d},\hat{k}}(z)$ are both of Type II, then $C(d,k) = C(\hat{d},\hat{k})$ is possible only if $(d,k) = (\hat{d},\hat{k})$.

If $\chi_{d,k}(z), \chi_{\hat{d},\hat{k}}(z)$ are both of Type III, then using (21), we find that

$$\Psi_{d,k}(z) = \frac{\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}}{\sum_{i=0}^{r-1}(-z)^i}, \quad \Psi_{\hat{d},\hat{k}}(z) = \frac{\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}}{\sum_{i=0}^{\hat{r}-1}(-z)^i}$$

So, from $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$, we obtain

$$\left(\sum_{i=0}^{\hat{r}-1}(-z)^i\right)\left(\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}\right) = \left(\sum_{i=0}^{r-1}(-z)^i\right)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right)$$

Multiplying both sides of the above equation by $z+1$, we obtain (35), which as shown above, leads to $(d,k) = (\hat{d},\hat{k})$. ■

At this point, we would like to remark that Lemmas 26 and 28 actually prove the following interesting fact: if two polynomials of the same type (I, II or III) have identical non-reciprocal parts, then the polynomials themselves are identical. In other words, within each of the three type classes, a polynomial is uniquely determined by its non-reciprocal part.

We are now only left to deal with the three cases where the characteristic polynomials are of different types. The next three lemmas consider each case in turn.

LEMMA 29. *Let $d, k, \hat{d}, \hat{k}$ be such that $\chi_{d,k}(z)$ is of Type I and $\chi_{\hat{d},\hat{k}}(z)$ is of Type II. Then, $C(d,k) = C(\hat{d},\hat{k})$ only if $(d,k) = (d, 2d)$ and $(\hat{d},\hat{k}) = (d+1, 3d+1)$.*

Proof: With $d, k, \hat{d}, \hat{k}$ as above, we have

$$\Psi_{d,k}(z) = \sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}, \quad \Psi_{\hat{d},\hat{k}}(z) = \frac{\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}}{z^{\hat{r}}+1}$$

So, if $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$, then it follows that

$$(z^{\hat{r}}+1)\left(\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}\right) = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}} \tag{36}$$

Note that if $\hat{r} \leq q$, then applying ϵ_1 to both sides of (36), we get $\hat{r} = \hat{q}$, which is impossible by Lemma 17. Hence, we must have $\hat{r} > q$.

So, applying ϵ_1 to (36) yields $q = \hat{q}$. Therefore, multiplying both sides of (36) by $\sum_{i=0}^{q-1} z^i$, we obtain on account of (21), $(z^{\hat{r}}+1)\left(z^n - \sum_{i=0}^{m} z^i\right) = z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i$, or equivalently,

$$z^{n+\hat{r}} + z^n - \sum_{i=0}^{m} z^{\hat{r}+i} - \sum_{i=0}^{m} z^i = z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i \tag{37}$$

We claim that the equality in (37) is possible only if $\hat{r} = m+1$ and $n = 2m+1$, in which case the LHS of the equation is $\chi_{m+1,3m+1}(z)$. To prove this claim, we observe first that if $\hat{r} \leq m$, then on the LHS of (37), the coefficient of $z^{\hat{r}}$ is -2. This is because we have one $-z^{\hat{r}}$ term coming from the summation $-\sum_{i=0}^{m} z^{\hat{r}+i}$, and another from the summation $-\sum_{i=0}^{m} z^i$, and neither of these terms can be cancelled out by z^n or $z^{n+\hat{r}}$, since $n > m \geq \hat{r}$. However, since there cannot be any term with coefficient -2 on the RHS, we must have $\hat{r} > m$.

Also, $\hat{r} > m+1$ is impossible, since if this were the case, $z^n - \sum_{i=0}^{m} z^{\hat{r}+i} - \sum_{i=0}^{m} z^i$ cannot be of the form $-\sum_{i=0}^{\hat{m}} z^i$, as can easily be verified. Thus, we are forced to conclude that for (37) to hold, $\hat{r}$ must be equal to $m+1$.

With $\hat{r} = m+1$, the LHS of (37) becomes $z^{n+m+1} + z^n - \sum_{i=0}^{2m+1} z^i$, which can be of the form $z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i$ only if $n = 2m+1$, so that z^n cancels out with $-z^{2m+1}$. With this choice of $\hat{r}$ and m, the LHS of (37) reduces to $z^{3m+2} - \sum_{i=0}^{2m} z^i = \chi_{m+1,3m+1}(z)$. Hence, we see that $(\hat{d},\hat{k}) = (m+1, 3m+1)$, and as $(m,n) = (m, 2m+1)$, we also have $(d,k) = (m, 2m)$, which proves the lemma. ■

LEMMA 30. *Let $d, k, \hat{d}, \hat{k}$ be such that $\chi_{d,k}(z)$ is of Type I and $\chi_{\hat{d},\hat{k}}(z)$ is of Type III. Then, $C(d,k) = C(\hat{d},\hat{k})$ only if $(d,k) = (d, 2d)$ and $(\hat{d},\hat{k}) = (d+1, 3d+1)$, or $(d,k) = (1,2)$ and $(\hat{d},\hat{k}) = (3,7)$.*

Proof: For the above choice of $d, k, \hat{d}, \hat{k}$, it follows from $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$ that $\left(\sum_{i=0}^{\hat{r}-1}(-z)^i\right)\left(\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}\right) = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}$, which upon multiplying by $z+1$ becomes

$$(z^{\hat{r}}+1)\left(\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}\right) = (z+1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right) \tag{38}$$

Now, the RHS above can be written as $(z+1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=1}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right) - z - 1$. Note that the $-z$ term cannot get cancelled out by any other term, since the smallest exponent of z in $(z+1)\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1}$ is $\hat{m}+1 \geq 2$. Therefore, ϵ_1 applied to the RHS of (38) yields 1.

When ϵ_1 is applied to the LHS of (38), we either get $\hat{r}$, if $\hat{r} \leq q$, or we get q, if $\hat{r} > q$. Therefore, either $\hat{r} = 1$ or $q = 1$. However, $\hat{r} = 1$ is impossible because $\hat{r} \geq 3$ by definition of Type III polynomials. Hence, we must have $q = 1$.

Therefore, (38) reduces to

$$(z^{\hat{r}}+1)\left(z^n - \sum_{i=0}^{m} z^i\right) = (z+1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right) \tag{39}$$

We will show that if $m \geq 2$, then the above equality is possible only if $(d,k) = (d,2d)$ and $(\hat{d},\hat{k}) = (d+1, 3d+1)$, and if $m = 1$, then the equality above implies that $(d,k) = (1,2)$ and $(\hat{d},\hat{k}) = (3,7)$.

So, suppose first that $m \geq 2$. The LHS of (39) can be written as $z^{n+\hat{r}} + z^n - \sum_{i=0}^{m} z^{\hat{r}+i} - \sum_{i=0}^{m} z^i$. Since $\hat{r} \geq 3$ and $m \geq 2$, the coefficient of z^2 in this polynomial is -1. Now, since $\hat{q} \geq 2$ by definition of Type III polynomials, there can be a $-z^2$ term on the RHS of (39) only if $\hat{q} = 2$. Therefore, it follows from (21) that the RHS of (39) is

$$(z+1)\,\frac{z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i}{\sum_{i=0}^{\hat{q}-1} z^i} = (z+1)\,\frac{z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i}{z+1} = z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i$$

Thus, we see that when $m \geq 2$, we must have $\hat{q} = 2$, and furthermore, (39) reduces to (37). But, as shown in the proof of Lemma 29, (37) holds only if $(d,k) = (d,2d)$ and $(\hat{d},\hat{k}) = (d+1, 3d+1)$.

It only remains to consider the case when $m = 1$. In this case, the LHS of (39) is $(z^{\hat{r}}+1)(z^n - z - 1) = z^{n+\hat{r}} + z^n - z^{\hat{r}+1} - z^{\hat{r}} - z - 1$. Cancelling out $-z-1$ from both sides of (39), we get

$$z^{n+\hat{r}} + z^n - z^{\hat{r}+1} - z^{\hat{r}} = (z+1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=1}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right) \tag{40}$$

Now, ϵ_1 applied to the RHS above yields $\hat{q}$, and the coefficient of $z^{\hat{q}}$ is -1. The $-z^{\hat{q}}$ term on the RHS must correspond to either $-z^{\hat{r}}$ or $-z^{\hat{r}+1}$ on the LHS. Since $\hat{q} \neq \hat{r}$

by Lemma 17, the $-z^{\hat{q}}$ term on the RHS must correspond to the $-z^{\hat{r}+1}$ term on the LHS, showing that $\hat{q} = \hat{r} + 1$. Therefore, ϵ_1 when applied to the LHS of (40) must yield $\hat{r} + 1$, which means that $-z^{\hat{r}}$ must get cancelled by z^n, so that we must have $n = \hat{r}$. Finally, applying ξ_1 to (40), we also obtain $n + \hat{r} = \hat{n} - \hat{q} + 2$. Using $\hat{q} = \hat{r} + 1$ and $n = \hat{r}$ to eliminate $\hat{q}$ and $\hat{r}$ from this last equation, we get $\hat{n} = 3n - 1$.

Since $\hat{q} = \hat{r} + 1 = n + 1$, and $\hat{q}|\hat{n}$, we find that $n + 1$ must divide $3n - 1$. Writing $3n - 1$ as $3(n + 1) - 4$, we see that $n + 1$ must be a factor of 4. Hence, $n = 0, 1$ or 3. But as $n > m \geq 1$, n must in fact be 3. Hence, $\hat{n} = 3n - 1 = 8$. Furthermore, $\hat{q} = n + 1 = 4$, and so the facts that $\hat{q}|\hat{m}$ and $\hat{m} < \hat{n}$ now imply that $\hat{m} = 4$. Thus, we have shown that when $m = 1$, equality in (38) is possible only if $n = 3$ and $(\hat{m}, \hat{n}) = (4, 8)$. As these values of (m, n) and $(\hat{m}, \hat{n})$ are equivalent to $(d, k) = (1, 2)$ and $(\hat{d}, \hat{k}) = (3, 7)$, the proof of the lemma is complete. ■

LEMMA 31. *Let $d, k, \hat{d}, \hat{k}$ be such that $\chi_{d,k}(z)$ is of Type II and $\chi_{\hat{d},\hat{k}}(z)$ is of Type III. Then, $C(d, k) = C(\hat{d}, \hat{k})$ only if $(d, k) = (d, 2d)$ and $(\hat{d}, \hat{k}) = (d + 1, 3d + 1)$.*

Proof: When $\chi_{d,k}(z)$ is of Type II and $\chi_{\hat{d},\hat{k}}(z)$ is of Type III, from the equality $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$, we get via (21),

$$\left(\sum_{i=0}^{\hat{r}-1}(-z)^i\right)\left(\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}\right) = (z^r + 1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right)$$

Upon multiplying both sides of this equation by $z + 1$, we obtain

$$(z^{\hat{r}} + 1)\left(\sum_{l=\frac{m}{q}}^{\frac{n}{q}-1} z^{lq+1} - \sum_{l=0}^{\frac{n}{q}-1} z^{lq}\right) = (z + 1)(z^r + 1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right) \tag{41}$$

Using $(z^r + 1)(z + 1) = z^{r+1} + z^r + z + 1$, we can write the RHS above as

$$(z + 1)(z^r + 1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=1}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right) - (z^{r+1} + z^r + z + 1) \tag{42}$$

Recall that the definition of Type III requires $\hat{q} \geq 2$ even and $\hat{r} \geq 3$ odd. Since $\hat{m} \geq \hat{q} \geq 2$, the smallest exponent of z in $(z + 1)(z^r + 1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1}\right)$ is $\hat{m} + 1 \geq 3$. Hence, the $-z$ term in (42) cannot be cancelled out by any other term. It follows that the coefficient of z on the RHS of (41) is non-zero, and so this must be true on the LHS as well. But, the only way for the coefficient of z to be non-zero on the LHS is if $\hat{r} = 1$ or $q = 1$. The former is impossible since $\hat{r} \geq 3$. So, we must have $q = 1$, and consequently, the LHS of (41) simplifies to $(z^{\hat{r}} + 1)\left(z^n - \sum_{i=0}^{m} z^i\right)$. Expanding out the product $(z + 1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right)$ on the RHS of (41), we can re-write (41) as

$$(z^{\hat{r}} + 1)\left(z^n - \sum_{i=0}^{m} z^i\right) = (z^r + 1)\left(\sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+2} - \sum_{l=0}^{\frac{\hat{m}}{\hat{q}}-1} z^{l\hat{q}+1} - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}}\right) \tag{43}$$

We have thus far shown that for $\Psi_{d,k}(z) = \Psi_{\hat{d},\hat{k}}(z)$ to be true for $d, k, \hat{d}, \hat{k}$ as in the statement of the lemma, then we must have $q = 1$ and (43) must hold. Our aim now is to show that for $q = 1$ and (43) to be true, we must also have $r = 2$ and $\hat{q} = 4$, from which it will follow that $(d, k) = (d, 2d)$ and $(\hat{d}, \hat{k}) = (d+1, 3d+1)$.

The first step in this process is to show that $\hat{q} \neq 2$, so that (since $\hat{q}$ is even) $\hat{q} \geq 4$. If we assume that $\hat{q} = 2$, then it is easily seen that the RHS of (43) simplifies to $(z^r + 1)\left(z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i\right)$. Therefore, by Lemma 27, (43) holds only if $(m, n) = (\hat{m}, \hat{n})$, or equivalently, $(d, k) = (\hat{d}, \hat{k})$, which cannot happen since $\chi_{d,k}(z)$ and $\chi_{\hat{d},\hat{k}}(z)$ are of different types. Hence, $\hat{q} = 2$ is impossible, and so $\hat{q} \geq 4$. We next show that this, along with the fact that $q = 1$, implies that $r = 2$.

Note that m is even, for if it were odd, then by Theorem 11, $\chi_{d,k}(z)$ would be of Type I. Hence $m \geq 2$, from which it follows that the LHS of (43) contains a $-z^2$ term, *i.e.*, the coefficient of z^2 on the LHS is -1. Therefore, the RHS of (43) must also contain a $-z^2$ term, which since $\hat{q} \geq 4$, can happen only if $r = 1$ or 2. But since $q = 1$, Lemma 17 forces r to be 2.

Setting $r = 2$, it can be verified that (43), upon multiplying out the product on its RHS, becomes

$$(z^{\hat{r}} + 1)\left(z^n - \sum_{i=0}^{m} z^i\right) = \sum_{l=\frac{\hat{m}}{\hat{q}}}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}+4} - \sum_{l=0}^{\frac{\hat{m}}{\hat{q}}-1} (z^{l\hat{q}+3} + z^{l\hat{q}+2} + z^{l\hat{q}+1}) - \sum_{l=0}^{\frac{\hat{n}}{\hat{q}}-1} z^{l\hat{q}} \qquad (44)$$

We now show that the above equality can hold only if $\hat{q} = 4$. Suppose, to the contrary, that $\hat{q} \neq 4$, so that $\hat{q} \geq 6$. Observe that since $\hat{q} \geq 6$, no cancellation of terms is possible among the various summations on the RHS of (44), as the exponents in different summations leave different remainders modulo $\hat{q}$. It follows that the RHS of (44) is of the form $-1 - z - z^2 - z^3 + \Omega(z^6)$, where $\Omega(z^6)$ denotes some polynomial of the form $\sum_{k\geq 6} c_k z^k$. In particular, the RHS cannot contain any z^4 or z^5 terms.

On the other hand, the LHS of (44) is $z^{n+\hat{r}} + z^n - \sum_{i=0}^{m} z^{\hat{r}+i} - \sum_{i=0}^{m} z^i$. Note that neither $z^{n+\hat{r}}$ nor z^n can cancel out any term in the summation $-\sum_{i=0}^{m} z^i$, so that all the terms in this summation remain intact on the LHS. But as the LHS cannot contain any z^4 or z^5 terms (because the RHS does not contain such terms), we find that $m \leq 3$. However, as observed earlier, m is even, so that we must in fact have $m = 2$. But now, in order for the LHS to contain a $-z^3$ term, we must either have $\hat{r} = 3$, or $n = \hat{r}$ and $\hat{r} + 1 = 3$. The latter is impossible, as it implies that $n = 2 = m$, which cannot happen. But $\hat{r} = 3$ is also impossible, since with $\hat{r} = 3$ and $m = 2$, the LHS reduces to $z^{n+\hat{r}} + z^n - \sum_{i=0}^{5} z^i$, which will always contain a z^4 or z^5 term. Thus, if we assume that $\hat{q} \neq 4$, we are forced to conclude that (44) cannot hold.

Therefore, for (44) to hold, we must have $\hat{q} = 4$. But with $\hat{q} = 4$, it is readily verified that the RHS of (44) simplifies to $z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i$. As a result, (44) becomes identical to (37) in the proof of Lemma 29, and as shown there, equality in (37) is possible only if $(d, k) = (d, 2d)$ and $(\hat{d}, \hat{k}) = (d+1, 3d+1)$. This completes the proof of the lemma. ■

Lemmas 26 and 28–31 together prove the following theorem, which in conjunction with Theorem 25, forms Theorem 1.

THEOREM 32. *If $d, k, \hat{d}, \hat{k}$ are non-negative integers such that $C(d, k) = C(\hat{d}, \hat{k})$, but $(d, k) \neq (\hat{d}, \hat{k})$, then one of the following holds:*
(i) $\{(d, k), (\hat{d}, \hat{k})\} = \{(\ell, 2\ell), (\ell + 1, 3\ell + 1)\}$ for some integer $\ell \geq 0$.

(ii) $\{(d,k),(\hat{d},\hat{k})\} = \{(1,2),(3,7)\}$.

There still remains a loose end that needs to be tied up, namely, a proof of Lemma 27. We provide such a proof now.

Proof of Lemma 27: Suppose that $m, n, r, \hat{m}, \hat{n}, \hat{r}$ are as in the statement of the lemma, and that

$$(z^r + 1)\left(z^n - \sum_{i=0}^{m} z^i\right) = (z^{\hat{r}} + 1)\left(z^{\hat{n}} - \sum_{i=0}^{\hat{m}} z^i\right). \tag{45}$$

It suffices to show that $r = \hat{r}$.

Multiplying both sides of (45) by $z - 1$, we obtain

$$(z^r + 1)(z^{n+1} - z^n - z^{m+1} + 1) = (z^{\hat{r}} + 1)(z^{\hat{n}+1} - z^{\hat{n}} - z^{\hat{m}+1} + 1). \tag{46}$$

Observe first that upon comparing the degrees of both sides of the above equation, we get

$$n + r = \hat{n} + \hat{r} \tag{47}$$

Taking the derivative of both sides of (46) and setting $z = 1$ yields $-2m = -2\hat{m}$, so that $m = \hat{m}$. Next, taking the second derivative of both sides of (46) and setting $z = 1$, we get

$$4n - 2m^2 - 2mr - 2m = 4\hat{n} - 2\hat{m}^2 - 2\hat{m}\hat{r} - 2\hat{m}.$$

Using the fact that $m = \hat{m}$, the above equation reduces to

$$4n - 2mr = 4\hat{n} - 2m\hat{r}. \tag{48}$$

But now, using (47) and (48), we have

$$(2m + 4)r = 4(r + n) - (4n - 2mr) = 4(\hat{r} + \hat{n}) - (4\hat{n} - 2m\hat{r}) = (2m + 4)\hat{r}.$$

Since $m \neq -2$, as $m > 0$, we must have $r = \hat{r}$, as desired. ■

Acknowledgment. The authors would like to thank the anonymous reviewer for a thorough review of the paper and for simplifying a few of the proofs in the paper, and especially for the clever proof of Lemma 27.

REFERENCES

[1] M. Filaseta, *On the factorization of polynomials with small Euclidean norm*, in *Number Theory in Progress Vol. 1*, de Gruyter, Berlin, 1999, pp. 143–163.

[2] K.A.S. Immink, P.H. Siegel and J.K. Wolf, *Codes for digital recorders*, IEEE Trans. Inform. Theory, 44 (1998), pp. 2260–2299.

[3] D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics and Coding*, Cambridge Univ. Press, Cambridge, UK, 1995.

[4] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand., 8 (1960), pp. 65–70.

[5] B.H. Marcus, R.M. Roth and P.H. Siegel, *Constrained systems and coding for recording channels*, in *Handbook of Coding Theory*, R. Brualdi, C. Huffman and V. Pless, eds., Elsevier, Amsterdam, The Netherlands, 1998.

[6] W.H. Mills, *The factorization of certain quadrinomials*, Math. Scand., 57 (1985), pp. 44–50.
[7] E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand., 4 (1956), pp. 287–302.
[8] C.E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J., 27 (1948), pp. 379–423.
[9] D.A. Wolfram, *Solving generalized Fibonacci recurrences*, Fibonacci Quart., 36.2 (1998), pp. 129–145.