A Combinatorial Generalization of a Putnam Problem

Ömer Eğecioğlu
Department of Computer Science
University of California
Santa Barbara, CA 93106

As a part of the thirty-fourth William Lowell Putnam Mathematical Competition, the following problem appeared in the Monthly [2]:

> *Let $a_1, a_2, \ldots, a_{2n+1}$ be a sequence of integers such that, if any of them is removed, the remaining ones can be divided into two sets of n integers with equal sums. Prove $a_1 = a_2 = \cdots = a_{2n+1}$.*

Here we give a combinatorial proof of a generalization of this problem. The arguments rely on a matrix theoretic formulation of the original problem and elementary properties of cyclotomic polynomials.

Theorem 1 *Let ξ be a primitive q-th root of unity where $q = p^r$, p prime. Suppose we are given a sequence S of $qn+1$ complex numbers $z_1, z_2, \ldots, z_{qn+1}$ with the property that for every i, $1 \leq i \leq qn+1$, $S \setminus \{z_i\}$ can be partitioned into q equal size subsets $S_{i,0}, S_{i,1}, \ldots, S_{i,q-1}$ with*

$$\sum_{k=0}^{q-1} \xi^k \sum_{z_j \in S_{i,k}} z_j = 0. \tag{1}$$

Then $z_1 = z_2 = \cdots = z_{qn+1}$.

Note that the original problem is a special case of Theorem 1 in which $p = 2$, $r = 1$ and each z_i is an integer.

Proof For each i fix a partition $S_{i,0}, S_{i,1}, \ldots, S_{i,q-1}$ of $S \setminus \{z_i\}$ satisfying (1). Let $N = qn$ and consider the $(N+1) \times (N+1)$ zero diagonal matrix $\mathbf{A} = \|a_{ij}\|$ where for $i \neq j$, $a_{ij} = \xi^k$ if and only if $z_j \in S_{i,k}$. If we put $\overline{\mathbf{z}} = [z_1, z_2, ..., z_{N+1}]^T$, then $\overline{\mathbf{z}}$ is a solution of the linear system $\mathbf{A}\mathbf{z} = \mathbf{0}$.

Since $\sum_{k=0}^{q-1} \xi^k = 0$, $\mathbf{A}$ is singular with zero row sums and $[1, 1, \ldots, 1]^T$ is in the kernel of $\mathbf{A}$. Thus to prove the theorem, it suffices to show that $rank(\mathbf{A}) = N$.

Let $f(x)\,|_{x^k}$ denote the coefficient of the term x^k in a polynomial $f(x)$. Then up to sign, $\det(x\mathbf{I} - \mathbf{A})\,|_{x^r}$ is the sum of the $(N + 1 - r) \times (N + 1 - r)$ principal minors of $\mathbf{A}$. We will show that $\det(x\mathbf{I} - \mathbf{A})\,|_x$ must be nonzero, and hence $rank(\mathbf{A}) = N$. We argue as follows.

Let M_j be the $N \times N$ principal minor of $\mathbf{A}$ corresponding to the j-th diagonal entry. In the expansion of M_j from first principles, we have

$$M_j = \sum_{\sigma} (-1)^{i(\sigma)} \prod_{\substack{i = 1 \\ i \neq j}}^{N+1} a_{i\sigma_i} \tag{2}$$

in which the summation is over all permutations (in fact derangements) σ of the index set $\{1, \ldots, j-1, j+1, \ldots, N+1\}$, and $(-1)^{i(\sigma)}$ is the sign of σ. Clearly the nonzero terms in the sum in (2) are of the form $\pm\xi^e$, for various $e \in \{0, 1, \ldots, q-1\}$. Since $\mathbf{A}$ has zero diagonal and nonzero off-diagonal entries, the sum $\sum(-1)^{i(\sigma)}$ over such terms in M_j is given by

$$\det(\mathbf{J} - \mathbf{I}) = (-1)^{N-1}(N-1)$$

where $\mathbf{J}$ is the $N \times N$ matrix of 1's and $\mathbf{I}$ is the $N \times N$ identity matrix. Since this is true for every M_j, we conclude that

$$\det(x\mathbf{I} - \mathbf{A})\,|_x \;=\; \sum_{j=1}^{N+1} M_j \;=\; c_{q-1}\xi^{q-1} + \cdots + c_1\xi + c_0 \;,$$

with

$$c_{q-1} + \cdots + c_1 + c_0 = (-1)^{N-1}(N-1)(N+1) \quad . \tag{3}$$

Now by way of contradiction, assume that

$$c_{q-1}\xi^{q-1} + \cdots + c_1\xi + c_0 = 0 \ .$$

Setting

$$f(t) = c_{q-1}t^{q-1} + \cdots + c_1 t + c_0 \quad ,$$

we then have $f(\xi) = 0$. Furthermore, $f(t)$ has integral coefficients. Therefore, the q-th cyclotomic polynomial $\Phi_q(t)$ must divide $f(t)$. Note also from (3) that $f(1) \equiv (-1)^N \pmod{p}$. Writing

$f(t) = \Phi_q(t)h(t)$, we must have that $\Phi_q(1)h(1) \equiv (-1)^N \pmod{p}$. In particular, $\Phi_q(1) \not\equiv 0 \pmod{p}$. But we can easily show that for $m = p^r$ with $r > 0$ and p prime, we must have $\Phi_m(1) = p$. To see this, recall that

$$t^m - 1 = \prod_{d \mid m} \Phi_d(t)$$

(see, for example, [3]), and thus, by Möbius inversion,

$$\Phi_m(t) = \prod_{d \mid m} (t^d - 1)^{\mu(\frac{m}{d})}. \tag{4}$$

In (4), μ is the Möbius function defined by

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1 \\ (-1)^\nu & \text{if } m \text{ is a product of } \nu \text{ distinct primes ,} \\ 0 & \text{otherwise .} \end{cases}$$

It immediately follows that for for $m = p^r$, $r > 0$,

$$\Phi_m(t) = \frac{t^{p^r} - 1}{t^{p^{r-1}} - 1} = 1 + t^{p^{r-1}} + t^{2p^{r-1}} + \cdots + t^{(p-1)p^{r-1}} \quad ,$$

and so $\Phi_m(1) = 1$. This gives us the desired contradiction.

We note that the property of $\Phi_m(1)$ for $m = p^r$ that we have made use of is a special case of the following more general result

$$\Phi_m(1) = \begin{cases} 0 & \text{iff } m = 1 \\ p & \text{iff } m = p^r,\ p \text{ prime, } r > 0 \\ 1 & \text{iff } m \text{ has two or more prime factors,} \end{cases}$$

which can be found in [1]. □

In proving Theorem 1 we used the fact that the row sums of the matrix $\mathbf{A}$ vanish only to show that $rank(\mathbf{A}) < N + 1$. The same argument used in the proof also provides a combinatorial proof of the following linear algebra result:

Theorem 2 *Suppose* $\mathbf{A}$ *is an* $N \times N$ *zero diagonal matrix whose off-diagonal entries are* q*-th roots of unity for some* $q = p^r$*,* p *prime,* $r > 0$*. If* $N \not\equiv 1 \pmod{p}$*, then* $\mathbf{A}$ *is nonsingular.*

Remarks: Note that Theorem 2 and its proof apply more generally to a matrix whose diagonal entries are algebraic integers which are merely divisible by the prime p.

Furthermore, if q is not a prime power, then we can show that the conclusion of Theorem 1 is false. In this case $q = uv$ with $\gcd(u, v) = 1$. Using the Chinese remainder theorem, pick $t < q$ with $t \equiv 0 \pmod{u}$ and $t \equiv 1 \pmod{v}$. Take $z_1 = \cdots = z_t = 1$ and $z_{t+1} = \cdots = z_{qn+1} = 0$. Then the twin identities

$$1 + \xi^v + \cdots + \xi^{v(t-1)} = 0 \ , \quad 1 + \xi^u + \cdots + \xi^{u(t-2)} = 0$$

show that no matter which z_i is discarded, the remaining ones can be multiplied by $q-$th roots of 1 using n copies of each root in such a way that they sum to 0.

Finally, we can consider the variant of the problem in which the classes $S_{i,0}, S_{i,1}, \ldots, S_{i,q-1}$ are not required to have the same cardinality. In this case Theorem 2 implies that the solution, if it exists, must be unique up to scalar multiples. It is easy to see that the sequence 1, 1, 1, 3, 3 for example, admits a solution in this general sense.

Acknowledgements: I would like to thank Professors A. Gerasoulis, A. Konheim, and the anonymous referees for helpful hints and suggestions.

References

[1] E.R. Berlekamp, *Algebraic Coding Theory*, revised 1984 edition, Aegean Park Press, p. 92.

[2] A.P. Hillman, "The William Lowell Putnam Mathematical Competition," Problem B-1, *The Mathematical Monthly*, Vol. 81, No. 10, pp. 1086-1094.

[3] K. Ireland and M.I. Rosen, *Elements of Number Theory*, Bogden & Quigley, Inc., Publishers, New York, 1972, Ch. 2.