Modular Restrictions on Circulant Weighing Matrices

Vassil Yorgov
Department of Mathematics and Computer Science, Fayetteville State University
Fayetteville, NC 28301
vyorgov@uncfsu.edu

An $n \times n$ matrix W with entries $(1, -1, 0)$ satisfying $W \cdot W^T = kI$, where I is the identity matrix of order n, is called a weighing matrix of order n and weight k.

A circulant matrix is a square matrix in which each row (except for the first) is a right cyclic shift of its predecessor. The set of all circulant weighing matrices of order n and weight k is denoted by $CW(n, k)$. The ring of all circulant matrices of order n over the integers, $\mathbb{Z}$, is isomorphic to the quotient ring $R_n = \mathbb{Z}[x]/(x^n - 1)$. A natural isomorphism takes the circulant matrix W with first row $(w_0, w_1, \ldots, w_{n-1})$ into the polynomial $w(x) = w_0 + w_1 x + \ldots + w_{n-1}x^{n-1}$. A polynomial $w(x)$ determines a circulant weighing matrix of weight k if and only if $w(x)w(x_{n-1}) = k$ in R_n. In that case $k = s^2$ where $s = w(1)$.

An integer t in Z_n^* is a multiplier of $w(x)$ from $CW(n, s^2)$ if $w(x) = w(x^t)$. It is known that if $CW(n, s^2) \neq \varnothing$ and $s = p^m$ for some prime p relatively prime to n, then there exist a $w(x)$ in $CW(n, s^2)$ having p as a multiplier.

We use reduction modulo p and the ring structure of $\mathbb{Z}_p[x]/(x^n - 1)$ to obtain certain restrictions on circulant weighing matrices with a multiplier p. We apply this restrictions to derive several new $CW(121, 81)$ with 3-rank 10, 15, 20, and 25 and to prove nonexistence of $CW(273, 121)$, $CW(273, 64)$, and $CW(273, 25)$.