Condensed Matter Physics 2008, Vol. 11, No 4(56), pp. 723–747

CONDENSED MATTER PHYSICS

On matrices associated to prime factorization of odd integers

T.Bier[1,2]*

[1] DOMAS, Faculty of Science, Sultan Qaboos University, Muscat 123, Al–Khod PO Box, Oman
[2] Twiskenweg 43 B, D 26129 Oldenburg, Germany

Received January 31, 2008

In this paper we introduce in section 5 integral matrices $M(n)$ for any factorization of an odd integer n into r distinct odd primes. The matrices appear in several versions according to a parameter $\rho \in [0,1]$, they have size $2^r \times 2^r$ and their rank satisfies e.g. for $\rho = 1/2$ the inequalities of theorem 4: $r+1 \leqslant \operatorname{rank}(M(n)) \leqslant 2^{r-1}+1$, which are obtained using theorem 1 discussed separately in the first few sections. The cases $\rho = 0, 1, 1/2$ are analyzed in some detail, and various counterexamples for $\rho \neq 0, 1, 1/2$ are included. There are several main results, theorem 5 is a duality between the cases $\rho = 0$ and $\rho = 1$, and theorem 6 is a periodicity theorem. The most important result perhaps is theorem 8 (valid for $\rho = 1/2$ only) on the existence of odd squarefree integers n with r odd prime factors such that $\operatorname{rank}(M(n)) = r+1$ attains the lower bound shown previously.

Key words: *factorization, matrices, floor, ceiling, square roots of unity*

PACS: *02.10.Yn*

1. Determinantal identities for multipliers of square roots of unity

We assume that n is an odd integer that is divisible by precisely $r = \omega(n)$ distinct prime divisors.

Let us denote these prime divisors by $p_1, p_2, \ldots, p_r$. Hence we may assume that the integer n is representable in the form

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_r^{e_r}. \tag{1}$$

Here $e_j > 0$ are positive integer exponents. Then we see that there are precisely r solutions $c_i,\ 1 \leqslant i \leqslant r$ of the congruence $x^2 \equiv 1 \mod n$ which have the following properties:

(1) for all $i = 1, 2, \ldots, r$ we have $1 \leqslant c_i \leqslant n-1$;

(2) for all $i, j = 1, 2, \ldots r$, there are congruences

$$c_i \equiv \epsilon_{ij} \mod p_j^{e_j}, \quad \text{where } \epsilon_{ij} = \begin{cases} -1, & \text{if} \quad i = j, \\ +1, & \text{if} \quad i \neq j. \end{cases} \tag{2}$$

We will refer to this system of r square roots as the *fundamental system (of square roots of unity) mod n.* For all values $i, j = 1, 2 \ldots, n$ we may then define a matrix μ_{ji} of multipliers by the equations

$$c_i \quad = \quad \epsilon_{ij} + p_j^{e_j} \cdot \mu_{ji}\,. \tag{3}$$

We will refer to the positive integers μ_{ji} as the *factor multipliers* of the odd integer n.

The fundamental square roots have an integer sum given as:

$$c_1 + c_2 + \cdots + c_r \equiv (r-2) \mod n. \tag{4}$$

*E-mails: 044153881@t-online.de, thomas.bier@gmail.com

This follows from the fact that for each modulus $p_j^{e_j}$ there is only one value of c_i which in position i yields -1, all the other values c_j yield $+1$, hence the sum of the r quantities is $r-1-1=r-2$.

Hence we may define an integer γ_1, to be called the *sum multiplier* by the equation

$$c_1 + c_2 + \cdots + c_r = (r-2) + n \cdot \gamma_1 \,. \tag{5}$$

Note that (4) and (5) together imply that $\gamma_1 > 0$ holds, as each of the r integer quantities c_i satisfies $c_i \geqslant 2$.

We follow the custom to denote the number of odd prime factors of an integer by $\omega(n) = r$.

Theorem 1 Let n be an odd integer with $\omega(n) = r$. For the determinant of the multiplier matrix $M = (\mu_{ji})$ of the fundamental system of square roots of unity mod n we obtain:

$$\det(M) = \pm 2^{r-1} \cdot \gamma_1 \,. \tag{6}$$

In particular $\det(M) \neq 0$.

Let

$$M = \begin{bmatrix} \mu_{11} & \mu_{12} & \mu_{13} & \cdots & \mu_{1r} \\ \mu_{21} & \mu_{22} & \mu_{23} & & \mu_{2r} \\ \mu_{31} & \mu_{32} & \mu_{33} & & \mu_{3r} \\ \vdots & & & \ddots & \vdots \\ \mu_{r1} & \mu_{r2} & \mu_{r3} & \cdots & \mu_{rr} \end{bmatrix} \tag{7}$$

so that the $i-$th column vector of M is given as

$$m_i = \begin{bmatrix} \mu_{1i} \\ \mu_{2i} \\ \mu_{3i} \\ \cdots \\ \mu_{ri} \end{bmatrix}.$$

We first consider the matrix M' that is obtained by multiplying the column vectors of $M = [m_1, m_2, \ldots, m_r]$ by the constants $p_1^{e_1}, p_2^{e_2}, \ldots, p_r^{e_r}$ so that we obtain

$$M' = [p_1^{e_1} m_1, p_2^{e_2} m_2, \ldots, p_r^{e_r} m_r] \tag{8}$$

and subsequently we get for the determinant

$$\det(M') = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r} \cdot \det(M) = n \cdot \det(M). \tag{9}$$

We let I_r be the $r \times r$ identity matrix, and J_r is the $r \times r$ all one matrix. We remark that with this notation the matrix (ϵ_{ji}) of (2) is just $(\epsilon_{ji}) = J_r - 2I_r$.

We now make use of the identity $c_i = \epsilon_{ji} + p_j^{e_j} \mu_{ji}$ in (3).

This enables us to rewrite the matrix in question as

$$M' = C - J_r + 2I_r \,, \tag{10}$$

where C is the rank one matrix that has the column vectors

$$C = [c_1 u, c_2 u, \ldots, c_r u] \tag{11}$$

with the all one column vector $u = (1, 1, \ldots, 1)^t \in R^r$.

In particular this applies to the matrix

$$A := J_r - C,$$

where C is the matrix consisting of n constant column vectors $(c_i, \dots, c_i)^t$ for $i = 1, 2, \dots, r$ defined in (11). Note that A has constant non-zero columns, and hence it is a matrix of rank one. Also note that its trace is equal to

$$Tr(A) = r - (c_1 + c_2 + \cdots + c_r). \tag{12}$$

The characteristic matrix $xI_r - A$ is the usual polynomial matrix that defines the characteristic polynomial, denoted by

$$\det(xI_r - A) = \chi_A(x),$$

and for the proof of (6) we use the fact that the determinant of any $r \times r$ rank 1 matrix A has a characteristic polynomial of the form

$$\chi_A(x) = x^r - \mathrm{Tr}(A) \cdot x^{r-1} \ . \tag{13}$$

Thus we obtain that

$$\chi_A(x) = x^r - (r - (c_1 + c_2 + \cdots + c_r))\, x^{r-1}. \tag{14}$$

It is clear that for $x = 2$ the characteristic matrix specializes to become the matrix $M' = C - J_r + 2I_r$ of (10). Thus by (13), (12) its determinant is equal to

$$\begin{aligned} \det(M') &= 2^r - (r - c_1 - c_2 - \cdots - c_r) \cdot 2^{r-1} \\ &= 2^{r-1}(c_1 + c_2 + \cdots + c_r - r + 2) \\ &= 2^{r-1} \cdot \gamma_1 \cdot n \quad \text{by (5).} \end{aligned}$$

Using (9) then completes the proof of theorem 1.

2. General moduli

Let $n_1, n_2, n_3, \dots, n_r$ be r pairwise coprime positive integers, and let $n = n_1 n_2 n_3 \cdot \cdots \cdot n_r$ be their product.

By the theorem on the solution of simultaneous congruences (Chinese remaindering) there exists an integral solution of the congruences

$$c_i \equiv \epsilon_{ij} \mod n_j\,, \quad \text{for } 1 \leqslant i, j \leqslant r.$$

They have the property that $c_i^2 \equiv 1 \mod n$ and hence they are a system of solutions of the congruence $x^2 \equiv 1 \mod n$.

Here ϵ_{ij} are given as in (2). We may again define the corresponding multipliers by the equations

$$c_i \quad = \quad \epsilon_{ij} + n_j \cdot \mu_{ji}\,. \tag{15}$$

In the same way as before we see that

$$c_1 + c_2 + \dots c_r \equiv (r - 2) \mod n. \tag{16}$$

This follows from the fact that for each modulus n_j there is only one value of c_i which in position i yields -1, all the other values c_j yield $+1$, hence the sum of the r quantities is $r-1-1 = r-2$.

Hence we may define an integer γ_1, again called the *sum multiplier* by the equation

$$c_1 + c_2 + \cdots + c_r = (r - 2) + n \cdot \gamma_1\,. \tag{17}$$

Theorem 2 For the determinant of the multiplier matrix $M = (\mu_{ji})$ we obtain:

$$\det(M) = 2^{r-1} \cdot \gamma_1. \tag{18}$$

The proof is a direct adaptation of the previous proof of theorem 1.

3. The Smith normal form

Again we assume that n is an odd integer with $\omega(n) = r$.

Theorem 3 (i) Assume that at least one of the c_i in the given system of fundamental square roots of unity mod n is even. Then the $r \times r$-matrix of multipliers M of the fundamental system of square roots of unity mod n defined in (7) has a Smith normal form given as

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 2 & 0 & & 0 & 0 \\ 0 & 0 & 2 & & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & & 2 & 0 \\ 0 & 0 & 0 & \dots & 0 & 2\gamma_1 \end{bmatrix}.$$

(ii) Assume that all of the c_i in the given system of fundamental square roots of unity mod n are odd. Then γ_1 is even, and the Smith normal of the $r \times r-$matrix M is given as

$$\begin{bmatrix} 2 & 0 & 0 & \dots & 0 & 0 \\ 0 & 2 & 0 & & 0 & 0 \\ 0 & 0 & 2 & & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & & 2 & 0 \\ 0 & 0 & 0 & \dots & 0 & \gamma_1 \end{bmatrix}.$$

For the proof we first assume case (i), i.e. we consider the case that **not** all the numbers c_i in the given fundamental system of square roots mod n are odd. We employ the standard localization techniques over the ring $Z_{(p)}$ of $p-$adic integers. Only the case of $p = 2$ even is slightly delicate. As n and all the factors n_i are odd, we see that we may multiply the matrix M columnwise by the n_i in order to get the matrix

$$C = (c_i - \epsilon_{ij}).$$

Then we use elementary row operations top reduce C to the form

$$\begin{bmatrix} \gamma_1 n & c_2 - 1 & c_3 - 1 & \dots & c_{r-1} - 1 & c_r - 1 \\ -2 & 2 & 0 & & 0 & 0 \\ -2 & 0 & 2 & & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ -2 & 0 & 0 & & 2 & 0 \\ -2 & 0 & 0 & \dots & 0 & 2 \end{bmatrix}, \tag{19}$$

where we have used that the top left entry is $c_1 + c_2 + \cdots + c_r - (r-2) = \gamma_1 n$. Under the given assumption there is at least one index i such $c_i - 1$ is odd, and hence (assuming without loss of generality $i \neq 1$) the matrix (19) can be reduced over $Z_{(2)}$ to contain at least one diagonal element 1 in its Smith normal form. The presence of the remaining terms 2 then implies the corresponding version of the statement of the theorem over the $2-$adic integers.

Then we apply standard localization techniques over the $p-$adic integers, keeping track of the powers of p in the factors n_i for the various odd primes involved to show that there is at most one non-trivial factor for any odd prime p.

The case (ii) is proved using the same method, but over $Z_{(2)}$ we cannot get any term 1. Note that in this case from the assumption c_i even, and n odd it follows from (5) that γ_1 is even so that the diagonal form in (ii) above is really a Smith normal form.

We remark that the case (ii) is rare, but it does occur. For example the integer $n = 180285$ with $r = 5$ prime factors $n = 3 \cdot 5 \cdot 7 \cdot 17 \cdot 101$ has a fundamental system of square roots of unity mod n

$$120191, 144229, 154531, 127261, 174931$$

consisting of only odd integers c_1, c_2, c_3, c_4, c_5 such that for $\gamma_1 = 4$ the associated Smith normal form of M is

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}.$$

4. Some general considerations on division with remainder

Assume that two positive integers n, d are given, with $n > d$ and let $\rho \in [0,1]$ be any real constant.

We may consider division of n by d with remainder in the form

$$n = q \cdot d + s \tag{20}$$

with an integer quotient $q \in \mathbb{Z}$ and with r satisfying the inequalities

$$(\rho - 1) \cdot d \leqslant s < \rho \cdot d. \tag{21}$$

In the present paper we stick exclusively to the case of odd integers, and hence if we restrict ρ to a certain class of rationals, then we may avoid the case of equality in (21) as follows.

First we always assume in case of a divisor without remainder that $q = n/d, s = 0$. In particular if $d = 1$ we always have $q = n, s = 0$. This remark mainly takes care of the special cases $\rho = 0, \rho = 1$.

In case of a nontrivial divisor with a non-zero remainder we may then restrict to the inequality

$$(\rho - 1) \cdot d < s < \rho \cdot d, \tag{22}$$

if ρ is chosen in a way to avoid those rationals s that occur during the division. One easy way to avoid rationals is to choose ρ to be irrational, which leads to a standard approach to the study of rational approximations of irrational numbers ρ. But as in the present paper, we always restrict the integers n, d to be odd positive integers, so that another possible choice of ρ is rational numbers with denominator which is a power of 2. In other words in this paper we might consider the following general form as

$$\rho = \frac{e}{2^t} \text{ for any } t \geqslant 0, \text{ with integer } e \in \{0, 1, 3, \ldots, 2^t - 1, 2^t\}. \tag{23}$$

This contains the three major cases [3], which will be referred to as the *classical cases* throughout the following discussion:

Gauss $\rho = 1$, with $q = \lfloor \frac{n}{d} \rfloor$;

Venkov $\rho = 0$, with $q = \lceil \frac{n}{d} \rceil$;

Hurwitz $\rho = \frac{1}{2}$, with $q = \left[\!\left[\frac{n}{d} \right]\!\right]$.

Example 1 Note that $\lfloor \frac{17}{11} \rfloor = 1$, and $\lceil \frac{17}{11} \rceil = 2$, while $[\![\frac{17}{7}]\!] = [\![\frac{17}{11}]\!] = 2$.

In any case for the purposes of the present paper we will then define that ρ is *admissible* if $0 \leqslant \rho \leqslant 1$ holds and ρ is either irrational or of the form (23).

5. Definition of the multiplier matrices

We now assume that an odd squarefree integer n with r distinct prime factors is given. Thus $n = p_1 p_2 \dots p_r$. Then there are precisely 2^r distinct solutions $x = c$ to the congruence $x^2 \equiv 1 \mod n$ in the range $0 < c < n$.

These solutions are to be called the *square roots of unity modulo* n.

They can be indexed by the sets $\alpha \subset \{1, 2, \dots, r\}$ as follows. Let $c = c_\alpha$ in the range $0 < c_\alpha < n$ be defined by the congruences

$$c_\alpha \equiv \begin{cases} +1 \mod p_i\,, & \text{if} \quad i \notin \alpha, \\ -1 \mod p_i\,, & \text{if} \quad i \in \alpha. \end{cases} \tag{24}$$

On the other hand, for any $\beta \subset \{1, 2, \dots, r\}$ we may consider all the 2^r divisors n_β of the integer n. Note that n_β are odd positive integers.

Assume that any $0 < \rho < 1$, as in (23), is given. We then define the $2^r \times 2^r-$*multiplier matrix* $M(n) = (m_{\beta,\alpha})$ by the equations (where for $\rho = 0, 1$ the equality $s_{\beta,\alpha} = 0$ is allowed)

$$c_\alpha = n_\beta \cdot m_{\beta,\alpha} + s_{\beta,\alpha} \text{ with } (\rho - 1)n_\beta < s_{\beta,\alpha} < \rho \cdot n_\beta\,. \tag{25}$$

Example 2 The case $r = 1$ is essentially trivial. Let $p = p_1$. We have $c_\emptyset = 1,\ c_{\{1\}} = p - 1$ and the two divisors $1, p$. This gives the three answers, according to the size of ρ

$$\begin{pmatrix} 1 & p-1 \\ 1 & 1 \end{pmatrix}, \text{ if } \rho < \frac{1}{p}\,; \tag{26}$$

$$\begin{pmatrix} 1 & p-1 \\ 0 & 1 \end{pmatrix}, \text{ if } \frac{1}{p} < \rho < \frac{p-1}{p}\,; \tag{27}$$

$$\begin{pmatrix} 1 & p-1 \\ 0 & 0 \end{pmatrix}, \text{ if } \rho > \frac{p-1}{p}\,. \tag{28}$$

This shows that $\operatorname{rank}(M(p)) = 2$ except for large $\rho > \dfrac{p-1}{p}$ when $\operatorname{rank}(M(p)) = 1$.

The case $r = 2$ with $n = p_1 p_2$ is somehow more interesting and its discussion is a starting point of all that follows. Clearly in this case we get a $4 \times 4-$matrix $M(n)$.

It was shown in chapter 2 of [1] that for the classical cases we always have

$$\operatorname{rank}(M(p_1 p_2)) = 3 \text{ if } \rho = 0, \frac{1}{2}, 1. \tag{29}$$

This result, and even a weaker inequality $\operatorname{rank}(M(p_1 p_2) \leqslant 3$, can however not be extended to the case of general ρ.

Example 3 Fix $\rho = 3/4$. Let $n = 77$, and consider the four square roots of unity $1, 34, 43, 76$. Together with the divisors $1, 7, 11, 77$ they form the following multiplier matrix

$$M(77) = \begin{pmatrix} 1 & 34 & 43 & 76 \\ 0 & 5 & 6 & 11 \\ 0 & 3 & 4 & 7 \\ 0 & 1 & 1 & 1 \end{pmatrix} \text{ with } \rho = \frac{3}{4}\,. \tag{30}$$

It is easy to check that $M(77)$ is non-singular and hence $\operatorname{rank}(M(77)) = 4$.

6. Rank inequalities

Theorem 4 Let $\rho = 1/2$. Let $n = p_1 p_2 \dots p_r$ be an odd integer with r distinct prime factors. Then the rank of the multiplier matrix $M(n)$ satisfies the inequalities

$$r + 1 \leqslant \operatorname{rank}(M(n)) \leqslant 2^{r-1} + 1\ . \tag{31}$$

We assume for the proof that the columns are in natural ordering. The proof of the lower bound comes essentially out of the theorem 1. However first we remark that the first row of the matrix $M(n)$, i.e. the row indexed by the empty set corresponding to the divisor 1 just consists of the line of integers

$$1 = c_1 < c_2 < \cdots < c_{2^r} < n.$$

We also note that all other rows have the first entry zero, since n is odd with $c_1 = 1$ the congruence conditions force $r_{\alpha,1} = 1$, and thus $m_{\alpha,1} = 0$. This is because the divisors are $d_\alpha \geqslant 3$ for all non-empty index sets $\alpha \neq \emptyset$. Thus the first column of the matrix $M(n)$ is just the column vector with a single 1 in the first position and with zeroes in all subsequent positions.

Note that this implies that the first row is never linearly dependent on any other combination of rows.

Next we recall that the rows indexed by the sets of singletons $d_1 = p_1, d_2 = p_2, \ldots, d_r = p_r$ contain a $r \times r$ submatrix with a non-vanishing determinant by theorem 1. Hence these r rows are also linearly independent, and they together with the first row form $r+1$ linearly independent rows. This proves the lower bound $r + 1 \leqslant rk(M(n))$.

We now prove the upper bound. For any column indexed by a set θ let $\eta = \{1, 2, \ldots, r\} \backslash \theta$ be the index of the "complementary" column. Note that the equation

$$c_\theta + c_\eta = n \tag{32}$$

holds, as it is easy to see that both c_θ and $n - c_\theta = c_\eta$ are solutions of the congruence $x^2 \equiv 1 \mod n$ which satisfy the corresponding congruences. We note that the condition (24) implies

$$\begin{aligned} c_\theta &= r_{\alpha,\theta} + m_{\alpha,\theta} \cdot d_\alpha , && (33)\\ c_\eta &= r_{\alpha,\eta} + m_{\alpha,\eta} \cdot d_\alpha , && (34) \end{aligned}$$

where $r_{\alpha,\theta} \equiv +1 \mod p_i$ if $r_{\alpha,\eta} \equiv -1 \mod p_i$ for all $i \in \alpha$. This implies

$$d_\alpha \text{ divides } r_{\alpha,\theta} + r_{\alpha,\eta} . \tag{35}$$

On the other hand

$$|r_{\alpha,\eta}| < \frac{d_\alpha}{2}, \qquad |r_{\alpha,\theta}| < \frac{d_\alpha}{2}.$$

This implies $|r_{\alpha,\theta} + r_{\alpha,\eta}| < d_\alpha$ by the triangle inequality. By (35) we get that $r_{\alpha,\theta} + r_{\alpha,\eta} = 0$.

Adding (33) and (34) we then see that

$$n = r_{\alpha,\theta} + r_{\alpha,\eta} + (m_{\alpha,\theta} + m_{\alpha,\eta}) \cdot d_\alpha = (m_{\alpha,\theta} + m_{\alpha,\eta}) \cdot d_\alpha . \tag{36}$$

Hence we get, denoting the complementary row index set of α by $\beta = \{1, 2, \ldots, r\} \backslash \alpha$,

$$(m_{\alpha,i} + m_{\alpha,j}) = \frac{n}{d_\alpha} = d_\beta . \tag{37}$$

Hence we have shown that entries in the same row which are in "complementary" position with respect to the columns always give the same sums. This means that all but one of a system of 2^{r-1} complementary vectors are linearly dependent, so that the upper inequality is also established.

7. Rank equality for the Gauss and Venkov cases

In this section it is shown that for any factorization $n = p_1 p_2 \ldots p_r$ into (at least two) odd primes the two multiplier matrices $MG(n) = M(n)$ for the case $\rho = 0$ (the Gauss, i.e. floor case) and for $MV(n) = M(n)$ for the case $\rho = 1$ (the Venkov i.e. ceiling case) have the same rowspaces, and hence the same rank.

Theorem 5 Let $n = p_1 p_2 \dots p_r$ be an odd integer with $r > 1$ distinct prime factors. Then the two multiplier matrices $MG(n) = M^0(n)$ and $MV(n) = M^1(n)$ have the same rowspaces:

$$\mathrm{RowSpace}(MG(n)) = \mathrm{RowSpace}(MV(n)). \tag{38}$$

In particular, the ranks agree as well: $\mathrm{rank}(MG(n)) = \mathrm{rank}(MV(n))$.

Let us keep n fixed, and then denote for a row index β as above the corresponding rows in $MG(n)$ and in $MV(n)$ by $RG(\beta)$ and by $RV(\beta)$. Hence $RG(\beta), RV(\beta) \in \mathbb{R}^{2^r}$. Trivially $RG(\emptyset) = RV(\emptyset)$, as in the row indexed by $\emptyset$ there are no fractions appearing.

From the definitions it is easy to see that for the all one vector $u \in \mathbb{R}^{2^r}$ we have the following equations for all non-empty index sets $\beta \neq \emptyset$:

$$RG(\beta) + u = RV(\beta). \tag{39}$$

This follows from the fact that for all $\beta \neq \emptyset$ due to the congruence conditions on the c_α all the fractions

$$\frac{c_\alpha}{n_\beta}$$

are not integral. We also note that for the full index set $\beta = \{1, 2, \dots, r\}$ we get $RG(\beta) = (0, 0, \dots, 0)$ and $RV(\beta) = (1, 1, \dots, 1) = u$. Hence to prove (38) we only have to show that

$$u \in \mathrm{RowSpace}(MG(n)) \ . \tag{40}$$

From $r > 1$ we see that there exist at least 2 distinct indices $i \neq j$. Let us simplify the notation for the corresponding rows to

$$RG(i) = RG(\{i\}), \quad RG(j) = RG(\{j\}), \quad RG(ij) = RG(\{i,j\})$$

respectively. First we consider the following vector in the row space of $MG(n)$:

$$V(i) = RG(\emptyset) - p_i \cdot RG(i) \in \mathrm{RowSpace}(MG(n)) \subset \mathbb{R}^{2^r}. \tag{41}$$

It is apparent from the congruence conditions that for any column index α there are only two values in $V(i)$:

$$V(i)_\alpha = \begin{cases} 1, & \text{if} \quad i \notin \alpha, \\ p_i - 1, & \text{if} \quad i \in \alpha. \end{cases} \tag{42}$$

Indeed we get that for $i \in \alpha$

$$RG(i)_\alpha = \lfloor \frac{c_\alpha}{p_i} \rfloor = \frac{c_\alpha + 1}{p_i} - 1$$

and hence

$$V(i)_\alpha = c_\alpha - p_i \cdot (\frac{c_\alpha + 1}{p_i} - 1) = p_i - 1$$

and similarly for the case $i \notin \alpha$. This shows the formula in (42).

Next we consider the two vectors in $\mathrm{RowSpace}(MG(n))$

$$W(i) = RG(i) - p_j \cdot RG(ij) \text{ and } W(j) = RG(j) - p_j \cdot RG(ij). \tag{43}$$

They may each contain up to four distinct entries according to the distinction of cases with the column coordinates

$$i,j \notin \alpha, \quad i \in \alpha, \quad j \notin \alpha, \quad i \notin \alpha, \quad j \in \alpha, \quad i,j \in \alpha.$$

More explicitly we find the following easy values:

$$W(i)_\alpha = W(j)_\alpha = 0, \quad \text{if} \quad i,j \notin \alpha,$$

$$W(i)_\alpha = p_j - 1, \quad W(j)_\alpha = p_i - 1 \quad \text{if} \quad i, j \in \alpha. \tag{44}$$

The core of the proof is to identify the remaining values $W(i)_\alpha,\ W(j)_\alpha$ in terms of a familiar structure already discussed in chapter 2 of [1] in the Hurwitz case $\rho = 1/2$.

Consider now the case $i \in \alpha, j \notin \alpha$ and let c be any integer that satisfies the congruences

$$c \equiv -1(p_i), \quad c \equiv +1(p_j). \tag{45}$$

For example we can have $c = c_\alpha$. Then the expression

$$w(i, c) = \lfloor \frac{c}{p_i} \rfloor - p_j \cdot \lfloor \frac{c}{p_i p_j} \rfloor \tag{46}$$

for $c = c_\alpha$ clearly is equal to the value under discussion:

$$w(i, c_\alpha) = W(i)_\alpha \, .$$

We use a trick to avoid direct calculation of this number. We first show that for any c as in (45) we have the shifting rule

$$w(i, c + p_i p_j) = w(i, c). \tag{47}$$

This is readily verified:

$$\begin{aligned} w(i, c + p_i p_j) &= \lfloor \frac{c + p_i p_j}{p_i} \rfloor - p_j \cdot \lfloor \frac{c + p_i p_j}{p_i p_j} \rfloor = \lfloor \frac{c}{p_i} + p_j \rfloor - p_j \cdot \lfloor \frac{c}{p_i p_j} + 1 \rfloor \\ &= \lfloor \frac{c}{p_i} \rfloor + p_j - p_j \cdot (\lfloor \frac{c}{p_i p_j} \rfloor + 1) = \lfloor \frac{c}{p_i} \rfloor - p_j \cdot \lfloor \frac{c}{p_i p_j} \rfloor = w(i, c). \end{aligned}$$

First of all this argument shows that for all c_α with $i \in \alpha, j \notin \alpha$ say the values of all the corresponding coordinates $W(i)_\alpha$ are equal. Secondly we may choose any particular c satisfying (45) to compute this value. For this computation we choose the unique solution of (45) that satisfies $1 < c < p_i p_j - 1$. This value then is

$$W(i)_\alpha = \lfloor \frac{c}{p_i} \rfloor = \frac{c+1}{p_i} - 1. \tag{48}$$

The other case for the vector $W(j)$ gives

$$W(j)_\alpha = \lfloor \frac{c}{p_j} \rfloor = \frac{c-1}{p_j} \, . \tag{49}$$

Now in turn consider a column index γ with $i \notin \gamma,\ j \in \gamma$. With a similar reasoning we get for d with $1 < d < p_i p_j - 1$ and $d \equiv +1(p_i),\ d \equiv -1(p_j)$ (indeed $d = p_i p_j - c$ holds) that

$$\begin{aligned} W(i)_\gamma &= \lfloor \frac{d}{p_i} \rfloor = \frac{d-1}{p_i} \, ; && (50) \\ W(j)_\gamma &= \lfloor \frac{d}{p_j} \rfloor = \frac{d+1}{p_j} - 1 \, . && (51) \end{aligned}$$

Hence we are led to consider the matrix

$$WM := \begin{pmatrix} \dfrac{c+1}{p_i} - 1 & \dfrac{d-1}{p_i} \\ \dfrac{c-1}{p_j} & \dfrac{d+1}{p_j} - 1 \end{pmatrix} \tag{52}$$

as well as the closely related matrix (the Hurwitz i.e. the symmetric case)

$$I_2 + WM := \begin{pmatrix} \dfrac{c+1}{p_i} & \dfrac{d-1}{p_i} \\ \dfrac{c-1}{p_j} & \dfrac{d+1}{p_j} \end{pmatrix} . \tag{53}$$

Now the latter matrix (53) has already been analyzed in chapter 2 of [1] and the following computation of the determinant was done:

$$\det(I_2 + WM) \quad = \quad \frac{c+1}{p_i} \cdot \frac{d+1}{p_j} - \frac{c-1}{p_j} \cdot \frac{d-1}{p_i} = \frac{2c+2d}{p_i p_j} = 2.$$

Now all entries in $I_2 + WM$ should be positive integers, as $1 < c, d$ and the congruences (45) hold. Hence we have that

$$WM = \begin{pmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{pmatrix}$$

with integers $w_{12}, w_{21} > 0$ and $w_{11}, w_{22} \geqslant 0$. Thus we may compute

$$\det(WM) = w_{11}w_{22} - w_{12}w_{21} = (1 + w_{11})(1 + w_{22}) - w_{12}w_{21} - 1 - \mathrm{trace}(WM) \tag{54}$$

so that

$$\det(WM) = 3 - \mathrm{trace}(I_2 + WM), \tag{55}$$

and assuming this to be zero leads to the equation $w_{12} \cdot w_{21} = \dfrac{d-1}{p_i} \cdot \dfrac{c-1}{p_j} = 0$, which contradicts the positivity of the entries in $I_2 + WM$.

We have now shown that $\det(WM) \neq 0$. Hence we may use the vectors $W(i)$ and $W(j)$ to construct the characteristic vector

$$\chi[i] \in \mathrm{RowSpace}(MG) \subset \mathbb{R}^{2^r}$$

of the set of column indices $\{\alpha : i \in \alpha\}$. In order to see this, let us order the coordinates α in such a way that those with $i, j \notin \alpha$ come first, then those with $i \notin \alpha, j \in \alpha$, then those with $i \in \alpha, j \notin \alpha$, and finally those with $i, j \in \alpha$. Let

$$a_i = \frac{c+1}{p_i} - 1, \qquad b_i = \frac{d-1}{p_i}, \qquad a_j = \frac{c-1}{p_j}, \qquad b_j = \frac{d+1}{p_j} - 1$$

so that $\det = a_i b_j - a_j b_i \neq 0$ holds. Then the vectors $W(i)$ and $W(j)$ can be represented as

$$W(i) \quad = \quad [0, a_i, b_i, a_i + b_i], \tag{56}$$
$$W(j) \quad = \quad [0, a_j, b_j, a_j + b_j], \tag{57}$$

where the last entry comes via (44) from (48) and (50) as

$$W(i)_\alpha + W(i)_\gamma = p_j - 1$$

and similarly for $a_j + b_j = p_i - 1$. In (56) each entry actually occurs 2^{r-2} times, and the same happens in (57).

Now form the vector

$$a_j \cdot W(i) - a_i \cdot W(j) = [0, 0, -\det, -\det] = -\det \cdot \chi[i].$$

This shows that

$$u = V(i) - (p_i - 2) \cdot \chi[i] \in \mathrm{RowSpace}(MG(n))$$

and concludes the proof of (40). Theorem 5 has now been shown.

We need to use the following consequence of the proof of theorem 5.

Corollary 1 The characteristic vector $\chi[r]$ of the set of column indices $\{\alpha : \; r \in \alpha\}$ is in the row space of the matrix $MG(n)$:

$$\chi[r] \in \mathrm{RowSpace}(MG(n)). \tag{58}$$

8. A periodicity result for the classical cases

Assume that $\rho = 1/2$ is fixed, in this and the following three sections, if not stated otherwise. Assume also that $m = p_1 p_2 \dots p_{r-1}$ is a product of $r-1$ distinct and odd prime numbers, and that p_r, p'_r are two other odd prime numbers distinct from $p_1, p_2, \dots, p_{r-1}$. Then we have that

Theorem 6 Assume that $p_r \equiv p'_r \mod 2m$ holds. Then (in the classical Hurwitz case $\rho = \frac{1}{2}$) the row spaces of the multiplier matrices $M(mp_r)$ and $M(mp'_r)$ as in (25) are equal, and hence

$$\text{rank } (M(mp_r)) = \text{rank } (M(mp'_r)).$$

Hence considering m as fixed, we see that for p'_r and $n' = m \cdot p'_r$ the rank of $M(n')$ depends only on the value of the rank of $M(n)$ for one fixed prime number p_r with $p'_r \equiv p_r \mod 2m$ and $n = m \cdot p_r$. Thus this value of rank $M(n)$ reappears at new primes periodically mod $2m$.

The proof of theorem 6 will be given in the next three sections. In the following section some parametric representations of square roots of unity are derived, which have some dual form, and which are then used in the subsequent two sections to obtain the equality of the row spaces.

9. Parametric properties of square roots of unity in the squarefree case

Assume that for a squarefree odd positive integer n the distinct prime divisors of n are $p_1, p_2, \dots, p_r$. Hence the integer n is in the form

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_{r-1} \cdot p_r. \tag{59}$$

Let index sets be given as $\alpha, \beta, \gamma, .. \subset \{1, 2, \dots, r\}$.

For any $\alpha \subset \{1, 2, \dots, r\}$ we let

$$n_\alpha = \prod_{i \in \alpha} p_i \,. \tag{60}$$

For any $\beta \subset \{1, 2, \dots, r\}$ assume that $0 < c_\beta < n$ is that unique square root of unity mod n which satisfies the congruences

$$c_\beta \equiv \begin{cases} -1 \mod p_i \,, & \text{if} \quad i \in \beta, \\ +1 \mod p_j \,, & \text{if} \quad j \notin \beta. \end{cases} \tag{61}$$

We may represent c_β in the following two forms

$$c_\beta = +1 + k_\beta \cdot \frac{n}{n_\beta} \,, \tag{62}$$

$$c_\beta = -1 + x_\beta \cdot n_\beta \tag{63}$$

with non-negative integers k_β, x_β which satisfy the inequalities

$$0 \leqslant k_\beta < n_\beta, \tag{64}$$

$$0 \leqslant x_\beta < \frac{n}{n_\beta} \,. \tag{65}$$

Clearly the case of equality happens in (64) if $\beta = \emptyset$ and the case of equality happens in (64) if $\beta = \{1, 2, \dots, r\}$. Let us refer to (62) and (63) as the *(first and second) parametric equation* for c_β.

Now let us make the following additional assumptions.

First let as in theorem 6

$$n' = p_1 p_2 \dots p_{r-1} p'_r \tag{66}$$

be another squarefree integer n' with r distinct odd prime factors, such that all except one of the prime factors of n and n' agree. Without loss of generality we may assume $p'_r > p_r$. Now let us denote the common part of n and n' by m, i.e.

$$m = \gcd(n, n') = p_1 p_2 \dots p_{r-1} \,. \tag{67}$$

Then clearly there exists another system of square roots of unity mod n' which we denote as c'_β, and there are the corresponding parametric equations

$$c'_\beta = +1 + k'_\beta \cdot \frac{n'}{n'_\beta}, \tag{68}$$

$$c'_\beta = -1 + x'_\beta \cdot n'_\beta \tag{69}$$

with non-negative integers k'_β, x'_β which satisfy the inequalities

$$0 \leqslant k'_\beta < n'_\beta, \tag{70}$$

$$0 \leqslant x'_\beta < \frac{n'}{n'_\beta}. \tag{71}$$

Secondly assume as in theorem 6 the following congruence, with m as in (67)

$$p'_r - p_r \equiv 0 \mod 2m, \tag{72}$$

i.e. it is assumed there exists a positive integer λ such that

$$p'_r - p_r = 2m \cdot \lambda. \tag{73}$$

With these assumptions and notations we can prove

Lemma 1 For any index set β as above with $r \notin \beta$ the corresponding quantities c_β, c'_β have the same first parameters, i.e.

$$k_\beta = k'_\beta. \tag{74}$$

For any index set β as above with $r \in \beta$ the corresponding quantities c_β, c'_β have the same second parameters, i.e.

$$x_\beta = x'_\beta. \tag{75}$$

For the proof first consider the case $r \notin \beta$. Note that this means $n_\beta = n'_\beta$. Then for all $i \in \beta$ we get from the definition of c_β, c'_β

$$1 + k_\beta \cdot \frac{n}{n_\beta} \equiv -1 \mod p_i, \tag{76}$$

$$1 + k'_\beta \cdot \frac{n'}{n_\beta} \equiv -1 \mod p_i. \tag{77}$$

This implies that

$$k_\beta \frac{n}{n_\beta} \equiv k'_\beta \frac{n'}{n_\beta} \mod p_i, \tag{78}$$

and hence

$$k_\beta p_r \equiv k'_\beta p'_r \mod p_i. \tag{79}$$

Now by the second assumption we have that

$$k_\beta p_r \equiv k'_\beta (p_r + 2m\lambda) \mod p_i, \tag{80}$$

so that

$$k_\beta p_r \equiv k'_\beta p_r \mod p_i, \text{ i.e. } k_\beta \equiv k'_\beta \mod p_i. \tag{81}$$

This holds for all $i \in \beta$, and by the CRT this implies

$$k_\beta \equiv k'_\beta \mod n_\beta. \tag{82}$$

From the inequalities $0 \leqslant k_\beta, k'_\beta < n_\beta$ we then get $k_\beta = k'_\beta$.

Now consider the case $r \in \beta$. Note that this means $\frac{n}{n_\beta} = \frac{n'}{n'_\beta}$. Then for all $j \notin \beta$ we get from the definition of c_β, c'_β

$$\begin{aligned} -1 + x_\beta \cdot n_\beta &\equiv 1 \mod p_j \,, && (83)\\ -1 + x'_\beta \cdot n'_\beta &\equiv 1 \mod p_j \,. && (84)\end{aligned}$$

This implies that

$$x_\beta n_\beta \equiv k'_\beta n'_\beta \mod p_j \,, \tag{85}$$

and hence

$$x_\beta p_r \equiv x'_\beta p'_r \mod p_j \,. \tag{86}$$

Now by the second assumption we have that

$$x_\beta p_r \equiv x'_\beta (p_r + 2m\lambda) \mod p_j \,, \tag{87}$$

so that

$$x_\beta p_r \equiv x'_\beta p_r \mod p_j \,, \text{ i.e. } x_\beta \equiv x'_\beta \mod p_j \,. \tag{88}$$

This holds for all $j \notin \beta$, and using the remark in the beginning of this case by the CRT this implies

$$x_\beta \equiv x'_\beta \mod \frac{n}{n_\beta} \,. \tag{89}$$

From the inequalities $0 \leqslant x_\beta, x'_\beta < \frac{n}{n_\beta}$ we then get $x_\beta = x'_\beta$. This completes the proof of lemma 1.

Corollary 2 (a) For any index set β as above with $r \notin \beta$ the corresponding quantities c_β, c'_β differ by an integer multiple of $2m$, more precisely

$$c'_\beta - c_\beta = 2m \cdot \lambda k_\beta \frac{m}{n_\beta} \tag{90}$$

holds.
(b) For any index set β as above with $r \in \beta$ let $\gamma = \beta - \{r\}$. Then the corresponding quantities c_β, c'_β differ by an integer multiple of $2m$, more precisely

$$c'_\beta - c_\beta = 2m \cdot \lambda x_\beta n_\gamma \tag{91}$$

holds.

First consider the case $r \notin \beta$. Then we trivially have $n_\beta = n'_\beta$ and from the first part of the lemma $k'_\beta = k_\beta$. Hence (62), (68) may be written in the form

$$\begin{aligned} c'_\beta &= +1 + k_\beta \cdot \frac{n'}{n_\beta} \,, && (92)\\ c_\beta &= +1 + k_\beta \cdot \frac{n}{n_\beta} \,. && (93)\end{aligned}$$

By taking the difference we then get

$$c'_\beta - c_\beta = k_\beta \frac{m}{n_\beta}(p'_r - p_r) = 2m \cdot \lambda k_\beta \frac{m}{n_\beta} \,. \tag{94}$$

This proves part (a) of the corollary.

Now consider the case $r \in \beta$. Then from the second part of the lemma $x'_\beta = x_\beta$. Hence (63) (69) may be written in the form

$$\begin{aligned} c_\beta &= -1 + x_\beta \cdot n_\beta \,, && (95)\\ c'_\beta &= -1 + x_\beta \cdot n'_\beta \,. && (96)\end{aligned}$$

By taking the difference we then get using the definition of γ

$$c'_\beta - c_\beta = x_\beta n_\beta (p'_r - p_r) = 2m \cdot \lambda k_\beta n_\gamma \,. \tag{97}$$

This proves part (b) of the corollary.

10. Lemma on equality of rows

Consider the multiplier matrices $M(n) = (m_{\beta,\alpha})$ and $M(n') = (m'_{\beta,\alpha})$ with n, n' as above, defined with respect to the fixed admissible value of $\rho = 1/2$, and with rows of the matrices indexed by the subsets $\beta \subset \{1, 2, \ldots, r\}$, and with columns of the matrices indexed by the subsets $\alpha \subset \{1, 2, \ldots, r\}$.

Note that by definition of the matrices in (25) this gives us two sets of equations

$$c_\alpha = n_\beta \cdot m_{\beta,\alpha} + s_{\beta,\alpha} \text{ with } |s_{\beta,\alpha}| < \frac{n_\beta}{2}\ , \tag{98}$$

$$c'_\alpha = n'_\beta \cdot m'_{\beta,\alpha} + s'_{\beta,\alpha} \text{ with } |s'_{\beta,\alpha}| < \frac{n'_\beta}{2}\ . \tag{99}$$

Here the quantities $s_{\beta,\alpha},\ s'_{\beta,\alpha}$ are considered to be the (symmetric) remainders after division by $n_\beta,\ n'_\beta$.

The proof then naturally splits into two parts. We distinguish index sets β according to the conditions $r \in \beta$ or $r \notin \beta$.

We shall first show that for any subset β with $r \in \beta$ the row $R(\beta)$ indexed by β in the matrix $M(n)$ and the row $R'(\beta)$ indexed by the same β in the matrix $M(n')$ are actually the same:

$$R(\beta) = R'(\beta) \text{ if } r \in \beta\ . \tag{100}$$

We state this fact as a separate lemma as follows.

Lemma 2 Assume (in the classical Hurwitz case $\rho = 1/2$) that $r \in \beta$, so that n_β is a divisor of n, and n'_β is a divisor of n'. Then the row $R(\beta)$ in the matrix $M(n)$ and the row $R'(\beta)$ in the matrix $M(n')$ (with both rows corresponding to the same index set β) are equal.

The equality of the rows will be shown componentwise, of course. First we consider those components with a column index α such that $r \notin \alpha$.

Let us denote as before $\gamma = \beta - \{r\}$. Then clearly $n_\gamma = n'_\gamma$ divides m and it also divides the two (distinct) integers n_β and n'_β.

Now (as $r \notin \alpha$ and the general assumptions of the previous section are valid) we may use (90) but replacing the index set β there by α. This gives us a congruence

$$c'_\alpha \equiv c_\alpha \mod 2m$$

and hence a fortiori

$$c'_\alpha \equiv c_\alpha \mod n_\gamma\ . \tag{101}$$

Using (101) from the equations in (98) and in (99) it follows that

$$s'_{\beta,\alpha} \equiv s_{\beta,\alpha} \mod n_\gamma\ . \tag{102}$$

Next we observe that from the standing assumption $r \notin \alpha$ it follows that the two congruences $c_\alpha \equiv 1 \mod p_r$ and $c'_\alpha \equiv 1 \mod p'_r$ hold. Thus by $r \in \beta$ it follows from the equations in (98) and in (99) that the two congruences

$$s_{\beta,\alpha} \equiv 1 \mod p_r\ , \tag{103}$$

$$s'_{\beta,\alpha} \equiv 1 \mod p'_r \tag{104}$$

also hold. Now consider the corresponding integral quotients

$$\frac{s_{\beta,\alpha} - 1}{p_r} \text{ and } \frac{s'_{\beta,\alpha} - 1}{p'_r} \tag{105}$$

and let us see what happens if we reduce these integers modulo n_γ.

First we get from our standing assumption $p_r \equiv p'_r \mod 2m$ and the distinctness of all primes involved that a fortiori $p_r \equiv p'_r \not\equiv 0 \mod n_\gamma$. Hence $\dfrac{1}{p_r} \equiv \dfrac{1}{p'_r} \mod n_\gamma$ holds. This together with (102) implies that the two integers in (105) are congruent modulo n_γ :

$$\frac{s_{\beta,\alpha}-1}{p_r} \equiv \frac{s'_{\beta,\alpha}-1}{p'_r} \mod n_\gamma\,. \tag{106}$$

Finally we need to consider the inequalities in (98) and (99). The first one implies

$$-\frac{n_\gamma}{2} - \frac{1}{p_r} < \frac{s_{\beta,\alpha}-1}{p_r} < \frac{n_\gamma}{2} - \frac{1}{p_r}\,, \tag{107}$$

where the upper side of the following (108) is now trivial, and since $\dfrac{s_{\beta,\alpha}-1}{p_r}$ is an integer, and n_γ, p_r are both odd, and p_r is a prime we also get the lower side of the following inequality

$$-\frac{n_\gamma}{2} < \frac{s_{\beta,\alpha}-1}{p_r} < \frac{n_\gamma}{2}\,. \tag{108}$$

A similar argument holds in the second case and shows

$$-\frac{n_\gamma}{2} < \frac{s'_{\beta,\alpha}-1}{p'_r} < \frac{n_\gamma}{2}\,. \tag{109}$$

Putting together (106) with (108), (109) we get

$$\frac{s_{\beta,\alpha}-1}{p_r} = \frac{s'_{\beta,\alpha}-1}{p'_r}\,. \tag{110}$$

Next rewrite (98) and (99) as

$$\frac{s_{\beta,\alpha}-1}{p_r} = \frac{c_\alpha-1}{p_r} - n_\gamma m_{\beta,\alpha}\,, \tag{111}$$

$$\frac{s'_{\beta,\alpha}-1}{p'_r} = \frac{c'_\alpha-1}{p'_r} - n_\gamma m'_{\beta,\alpha}\,. \tag{112}$$

Now use the parametric forms (62), (68) to obtain via $r \notin \alpha$ and lemma 1 (replacing β by α in the first part of that lemma) that

$$\frac{s_{\beta,\alpha}-1}{p_r} = k_\alpha \frac{m}{n_\alpha} - n_\gamma m_{\beta,\alpha}\,, \tag{113}$$

$$\frac{s'_{\beta,\alpha}-1}{p'_r} = k_\alpha \frac{m}{n_\alpha} - n_\gamma m'_{\beta,\alpha}\,. \tag{114}$$

Now feeding the information (110) into these equations it follows that $m_{\beta,\alpha} = m'_{\beta,\alpha}$, which completes the proof of lemma 2 in case when the condition $r \notin \alpha$ holds.

For the case of $r \in \alpha$ it is perfectly feasible but lengthy to repeat the above arguments with the use of the corresponding dual results of the previous section. However there is a shortcut which for the sake of brevity may be used here instead.

For any index set $\alpha \subset \{1, 2, \ldots, r\}$ let us denote its complementary set by $\bar{\alpha} := \{1, 2, \ldots, r\} - \alpha$. The equation

$$c_\alpha + c_{\bar{\alpha}} = n \tag{115}$$

is clear.

Assume as before that β is fixed. The condition $r \in \beta$ is not assumed at this moment. We use equation (98) and the one similar to (99):

$$c_{\bar{\alpha}} = n_\beta \cdot m_{\beta,\bar{\alpha}} + s_{\beta,\bar{\alpha}} \text{ with } |s_{\beta,\bar{\alpha}}| < \frac{n_\beta}{2}\,. \tag{116}$$

By adding (98) and (116) and using (115) we get that

$$n = n_\beta \cdot (m_{\beta,\alpha} + m_{\beta,\bar{\alpha}}) + (s_{\beta,\alpha} + s_{\beta,\bar{\alpha}}). \tag{117}$$

As n_β divides n, it follows that

$$n_\beta \text{ divides } s_{\beta,\alpha} + s_{\beta,\bar{\alpha}}\,. \tag{118}$$

But on the other hand, from the inequalities in (98) and (116) we get by using the triangle inequality

$$|s_{\beta,\alpha} + s_{\beta,\bar{\alpha}}| \leqslant |s_{\beta,\alpha}| + |s_{\beta,\bar{\alpha}}| < n_\beta\,. \tag{119}$$

Now (118) and (119) imply that

$$s_{\beta,\alpha} + s_{\beta,\bar{\alpha}} = 0\ , \tag{120}$$

which implies via (117) that

$$m_{\beta,\alpha} + m_{\beta,\bar{\alpha}} = \frac{n}{n_\beta} \tag{121}$$

which is independent of α.

Now continue to assume that $r \in \beta$ holds, and that n, n' are given as above. Then we get two sets of equations

$$m_{\beta,\alpha} + m_{\beta,\bar{\alpha}} \quad = \quad \frac{n}{n_\beta}\,, \tag{122}$$

$$m'_{\beta,\alpha} + m'_{\beta,\bar{\alpha}} \quad = \quad \frac{n'}{n'_\beta}\,. \tag{123}$$

From the assumption $r \in \beta$ we get that

$$\frac{n'}{n'_\beta} = \frac{n}{n_\beta}\ .$$

If $r \in \alpha$, then $r \notin \bar{\alpha}$ and for the numbers $m_{\beta,\bar{\alpha}},\ m'_{\beta,\bar{\alpha}}$ we may apply the result already proved for the first case which is

$$m_{\beta,\bar{\alpha}} = m'_{\beta,\bar{\alpha}}\,. \tag{124}$$

Now using (121) we can complete the argument

$$m_{\beta,\alpha} \quad = \quad \frac{n}{n_\beta} - m_{\beta,\bar{\alpha}} = \frac{n'}{n'_\beta} - m'_{\beta,\bar{\alpha}} = m'_{\beta,\alpha} \quad .$$

This proves lemma 2.

We now give an example which shows that in the case of general admissible ρ the conclusion of the lemma is not true.

Example 4 Consider the case $r = 3$, with $p_1 = 3, p_2 = 5$, and with $p_3 = 11, p'_3 = 41$. This satisfies the assumptions of lemma 2. With the (admissible) value of $\rho = \frac{12\sqrt{2}}{25}$ it can be computed that for $p_3 = 11$ we get the multiplier matrix

$$\begin{pmatrix}
1 & 56 & 34 & 89 & 76 & 131 & 109 & 164 \\
0 & 18 & 11 & 29 & 25 & 43 & 36 & 54 \\
0 & 11 & 7 & 18 & 15 & 26 & 22 & 33 \\
0 & 4 & 2 & 6 & 5 & 9 & 7 & 11 \\
0 & 5 & 3 & 8 & 7 & 12 & 10 & 15 \\
0 & 2 & 1 & 3 & 2 & 4 & 3 & 5 \\
0 & 1 & 0 & 1 & 1 & 2 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1
\end{pmatrix}$$

while for $p_3' = 41$ we get

$$\begin{pmatrix} 1 & 206 & 124 & 329 & 286 & 491 & 409 & 614 \\ 0 & 68 & 41 & 109 & 95 & 163 & 136 & 204 \\ 0 & 41 & 25 & 66 & 57 & 98 & 82 & 123 \\ 0 & 14 & 8 & 22 & 19 & 33 & 27 & 41 \\ 0 & 5 & 3 & 8 & 7 & 12 & 10 & 15 \\ 0 & 1 & 1 & 2 & 2 & 4 & 3 & 5 \\ 0 & 1 & 0 & 1 & 1 & 2 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

In the sixth line (corresponding to the index set $\beta = \{1,3\}$) we find distinct entries.

11. The proof of the periodicity theorem

We now turn to the case of those rows $R(\beta)$, $R'(\beta)$ with $r \notin \beta$. Here the situation is more interesting, as these rows are not equal but just linearly dependent by adding a certain multiple of the row vector $R(\{r\})$.

The proof will depend on the following formula between the row vectors:

$$R'(\beta) = R(\beta) + 2\lambda \cdot \frac{m}{n_\beta} R(\{r\}) \ . \tag{125}$$

Here the vector $R(\{r\})$ is easily seen to have the following coordinates:

$$R(\{r\})_\alpha = \begin{cases} \dfrac{c_\alpha - 1}{p_r}, & \text{if} \quad r \notin \alpha, \\ \dfrac{c_\alpha + 1}{p_r}, & \text{if} \quad r \in \alpha. \end{cases} \tag{126}$$

We will show (125) by verifying it for all (column-)coordinates α. Note that as in our case $r \notin \beta$ we get the relation $n_\beta = n'_\beta$. Hence the two inequalities in (98), (99) take the same form:

$$|s_{\beta,\alpha}| < \frac{n_\beta}{2}, \quad |s'_{\beta,\alpha}| < \frac{n_\beta}{2} \, . \tag{127}$$

By the triangle inequality this implies

$$|s'_{\beta,\alpha} - s_{\beta,\alpha}| < n_\beta \, . \tag{128}$$

First we consider those coordinates with $r \notin \alpha$. From corollary 2 (90) with α instead of β we have that n_β divides the difference $c'_\alpha - c_\alpha$. By (98), (99) we get that n_β divides the difference $s'_{\beta,\alpha} - s_{\beta,\alpha}$. Together with (128) this proves

$$s'_{\beta,\alpha} = s_{\beta,\alpha} \, . \tag{129}$$

With these preparations let us compute the difference of the vectors $R'(\beta) - R(\beta)$ at the coordinate α:

$$\begin{aligned} R'(\beta)_\alpha - R(\beta)_\alpha \quad &= \quad \frac{c'_\alpha - s'_{\beta,\alpha}}{n_\beta} - \frac{c_\alpha - s_{\beta,\alpha}}{n_\beta} = \frac{c'_\alpha - c_\alpha}{n_\beta} - \frac{s'_{\beta,\alpha} - s_{\beta,\alpha}}{n_\beta} \\ &= \quad \frac{c'_\alpha - c_\alpha}{n_\beta} \qquad \text{by (129)} \\ &= \quad 2\lambda \frac{m}{n_\alpha} \frac{m}{n_\beta} k_\alpha \qquad \text{by (90)} \, . \end{aligned} \tag{130}$$

On the other hand with the parametric equation (62) we can rewrite the first expression in (126) as

$$\frac{c_\alpha - 1}{p_r} = \frac{k_\alpha n}{n_\alpha p_r} = \frac{m}{n_\alpha} \cdot k_\alpha \, . \tag{131}$$

Comparing (130) with (131) we obtain the proof of (125), at least in the case $r \notin \alpha$. The other case $r \in \alpha$ can be obtained starting from the second part of (126) by rerunning the argument with the corresponding dual formulas, or by using complements. The details are left to the reader. This ends the proof of (125).

It is now clear that lemma 2 together with (125) proves that

$$\mathrm{RowSpace}(M(n')) \subset \mathrm{RowSpace}(M(n)) \; .$$

Using lemma 2 in the special case $R'(\{r\}) = R(\{r\})$ it also shows the reverse inclusion

$$\mathrm{RowSpace}(M(n')) \supset \mathrm{RowSpace}(M(n)) \; ,$$

and hence the proof of theorem 6 is complete.

Example 5 Let $r = 4$, and consider the odd prime numbers $p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 13$ and $p'_4 = 223$. Let ρ be any admissible value close to the fraction $\frac{167}{249}$. We have computed for $n = 1365$ and $n' = 23415$ that $\mathrm{rank}(M(n)) = 12$, while $\mathrm{rank}(M(n')) = 11$. Thus for the case of general ρ, a statement like theorem 6 cannot hold.

12. Periodicity for other cases

For the classical Gauss (floor) case of $\rho = 0$ and dually for the classical Venkov (ceiling) case $\rho = 1$ the periodicity theorem also holds.

Theorem 7 Assume that $p_r \equiv p'_r \mod 2m$ holds. Then (in the classical Gauss case $\rho = 0$ or dually in the classical Venkov case $\rho = 1$) the row spaces of the multiplier matrices $M(mp_r)$ and $M(mp'_r)$ as in (25) are equal, and hence

$$\mathrm{rank}\ (M(mp_r)) = \mathrm{rank}\ (M(mp'_r)).$$

The proof is quite similar to the above, and in order to avoid unnecessary repetitions we just comment on the differences for the case $\rho = 0$ instead of $\rho = \frac{1}{2}$. Clearly the section on parametric properties is independent of ρ. In the following section on equality of rows with $r \in \beta$ the equations (98) and (99) are replaced by

$$\begin{aligned} c_\alpha &= n_\beta \cdot m_{\beta,\alpha} + s_{\beta,\alpha} \text{ with } 0 \leqslant s_{\beta,\alpha} < n_\beta \; , && (132) \\ c'_\alpha &= n'_\beta \cdot m'_{\beta,\alpha} + s'_{\beta,\alpha} \text{ with } 0 \leqslant s'_{\beta,\alpha} < n'_\beta \; . && (133) \end{aligned}$$

By an obviously parallel argument (for $r \notin \alpha$) one then arrives at the inequalities

$$0 \leqslant \frac{s_{\beta,\alpha} - 1}{p_r} < n_\gamma \text{ and } 0 \leqslant \frac{s'_{\beta,\alpha} - 1}{p'_r} < n_\gamma \tag{134}$$

from which using the congruences one may conclude

$$\frac{s_{\beta,\alpha} - 1}{p_r} = \frac{s'_{\beta,\alpha} - 1}{p'_r}$$

and then as before one gets $m_{\beta,\alpha} = m'_{\beta,\alpha}$.

For the case $r \in \alpha$ the same kind of duality argument as before may be used.

The only real difference is in the adaptation of (125). This now takes the form

$$R'(\beta) = R(\beta) + 2\lambda \cdot \frac{m}{n_\beta} \cdot (R(\{r\}) + \chi[r]) \ , \tag{135}$$

with $\chi[r]$ as in (58).

The proof of (135) is again quite similar to the one given earlier for (125) and thus need not be repeated here. An application of corollary 1 then shows equality of row spaces, and hence proves theorem 7.

13. The existence theorem

Assume again that $\rho = \frac{1}{2}$ is fixed. Assume also that $m = p_1 p_2 \ldots p_{r-1}$ is a product of $r-1$ distinct and odd prime numbers, and that p_r is another odd prime number distinct from $p_1, p_2, \ldots, p_{r-1}$. Then we have that

Theorem 8 Assume that $p_r \equiv 1 \mod 2m$ holds. Then (in the classical Hurwitz case $\rho = \frac{1}{2}$) the rank of $M(mp_r)$ is one more than the rank of $M(m)$, that is

$$\text{rank } (M(mp_r)) \ = \ \text{rank } (M(m)) \ + 1.$$

In particular, we observe for any integer $r \geqslant 2$ the existence of infinitely many factorizations of positive odd integers n into r distinct prime factors $n = p_1 p_2 \ldots p_r$ such that $\text{rank} M(n) = r + 1$.

Let us remark here that the same statement is true under the hypothesis $p_r \equiv -1 \mod 2m$. This will not be elaborated below, but the adaptation of the proof should present no major difficulties.

Corollary 3 For any integer $r \geqslant 2$ there exist infinitely many distinct $r-$ tuples of distinct odd prime numbers $(p_1, p_2, \ldots, p_r)$ such that

$$\text{rank } M(p_1 p_2 \ldots p_r) \ = \ r + 1. \tag{136}$$

We note that although there is some analogy between theorem 8 and the previous theorem 6 which also shows up in the proof, there are clear differences. On the one hand theorem 8 does not hold for the cases $\rho = 0, \ \rho = 1$ as opposed to theorem 6, and on the other hand in the proof of the present theorem 8 a natural distinction between the prime $p = 3$ and the other odd primes shows up, which makes the argument somewhat more intricate.

The strategy of the proof is to compare the row space of the larger matrix $M(p_1 p_2 \ldots p_{r-1} p_r) = M(mp_r)$ with the row space of the *double* of the matrix $M(m)$. Here we define the *double* of any $s \times n$ matrix M as the $s \times 2n-$matrix $DM = [M, M]$ that is obtained from M by writing each of the s rows of M twice in the corresponding s rows so as to get s vectors in $\mathbb{R}^{2n}$. These s vectors then form the double DM. Hence, it is obvious that

$$\text{rank } DM \ = \text{rank } M. \tag{137}$$

Note that in the case of $M(m)$ under discussion, the extent of the double $DM(m)$ is $2^{r-1} \times 2^r$. In the calculations below, the reader should remember that for such matrices we make an obvious convention concerning the column index α, the second half of the double being indexed by those α with $r \in \alpha$. More formally, letting $DM(n) = (d_{\beta,\alpha})$ if $r \in \alpha$, then we have $d_{\beta,\alpha} = d_{\beta,\epsilon}$ with $\epsilon = \alpha - \{r\}$. Recall that the rows of $M(mp_r)$ are indexed by the subsets $\beta \subset \{1, 2, \ldots, r\}$ and that they are denoted by $R(\beta)$. Our task is to show that the row space of the matrix $M(mp_r)$ is given as

$$\text{RowSpace}(M(mp_r)) = \text{LinSpan}(\text{RowSpace}(DM(m)), R(\{r\}). \tag{138}$$

We also let the 2^r solutions of the congruence $x^2 \equiv 1 \mod mp_r$ in the range $1 \leqslant x \leqslant mp_r - 1$ be denoted by c_α, and we let the 2^{r-1} solutions of the congruence $x^2 \equiv 1 \mod m$ in the range $1 \leqslant x \leqslant m - 1$ be denoted by b_α. We also let as before $p_r = 1 + 2 \cdot m \cdot \lambda$. With these notations and with the assumptions of theorem 8 we then get the following lemmas.

Lemma 3 (i) For a fixed index set $\alpha \subset \{1, 2, \ldots, r-1\}$ the difference of the corresponding roots of unity is given as either of the following two expressions

$$\begin{aligned} c_\alpha - b_\alpha &= 2m \cdot (b_\alpha - 1) \cdot \lambda \ , \\ c_\alpha - p_r b_\alpha &= 1 - p_r \ . \end{aligned} \tag{139}$$

(ii) For a fixed set $\alpha \subset \{1, 2, \ldots, r\}$ with $r \in \alpha$ let $\epsilon = \alpha - \{r\}$. Then the difference of the corresponding roots of unity is given as either of the following two expressions

$$\begin{aligned} c_\alpha - b_\epsilon &= 2m \cdot (b_\epsilon + 1) \cdot \lambda \, , \\ c_\alpha - p_r b_\epsilon &= p_r - 1 \ . \end{aligned} \tag{140}$$

In order to prove the first part of lemma 3 we use the results and notations of section 9 on parametric properties. We first consider the case $r \notin \alpha$ and we use the equation (62) in the forms

$$c_\alpha = 1 + k_\alpha \cdot p_r \cdot \frac{m}{n_\alpha} \, , \tag{141}$$

$$b_\alpha = 1 + h_\alpha \cdot \frac{m}{n_\alpha} \tag{142}$$

with the constraints as in (64)

$$0 \leqslant k_\alpha < n_\alpha \, , \qquad 0 \leqslant h_\alpha < n_\alpha \, . \tag{143}$$

We may use the complementary index set $\zeta = \{1, 2, \ldots, r-1\} - \alpha$ to write $n_\zeta = \dfrac{m}{n_\alpha}$. Then from the conditions

$$c_\alpha \equiv -1 \mod n_\alpha \quad \text{and} \quad b_\alpha \equiv -1 \mod n_\alpha \tag{144}$$

we see that

$$k_\alpha p_r n_\zeta \equiv -2 \mod n_\alpha \, , \tag{145}$$

$$h_\alpha n_\zeta \equiv -2 \mod n_\alpha \tag{146}$$

so that from the assumptions $p_r \equiv 1 \mod m$ and $\gcd(n_\alpha, n_\zeta) = 1$ we have that

$$k_\alpha \equiv h_\alpha \mod n_\alpha \quad \text{and} \quad 1 \leqslant h_\alpha, k_\alpha < n_\alpha \, . \tag{147}$$

Then from (147) it follows that $k_\alpha = h_\alpha$. Substituting this back into (142) and forming the difference $c_\alpha - p_r b_\alpha$ the equation (139) then easily follows.

Also (147) implies via (141), (142) that

$$c_\alpha - b_\alpha = h_\alpha \cdot (p_r - 1) \cdot n_\gamma \tag{148}$$

$$= 2\lambda m (b_\alpha - 1) \ . \tag{149}$$

This shows (139) and hence proves the first part of the lemma.

For the second part it was assumed that $\alpha \subset \{1, 2, \ldots, r\}$ contains $r \in \alpha$ and that $\epsilon = \alpha - \{r\}$. By (63) applied to c_α and to b_ϵ respectively we get

$$c_\alpha = -1 + x_\alpha \cdot p_r n_\epsilon \, , \tag{150}$$

$$b_\epsilon = -1 + y_\epsilon \cdot n_\epsilon \tag{151}$$

with

$$0 \leqslant x_\alpha < n_\xi \quad \text{and} \quad 0 \leqslant y_\epsilon < n_\xi \, , \tag{152}$$

where $\xi = \{1, 2, \ldots, r-1\} - \epsilon = \{1, 2, \ldots, r-1, r\} - \alpha$ is the complementary set. From the definitions of c_α and b_ϵ we also have the congruences

$$c_\alpha \equiv 1 \mod n_\xi \quad \text{and} \quad b_\epsilon \equiv 1 \mod n_\xi \, . \tag{153}$$

This implies that

$$x_\alpha n_\epsilon \equiv x_\alpha p_r n_\epsilon \equiv 2 \mod n_\xi \,, \tag{154}$$
$$y_\epsilon n_\epsilon \equiv 2 \mod n_\xi \tag{155}$$

which implies via $\gcd(n_\epsilon, n_\xi) = 1$ that

$$x_\alpha \equiv y_\epsilon \mod n_\xi \,. \tag{156}$$

Combining this with (152) we get an equality of integers

$$x_\alpha = y_\epsilon \,. \tag{157}$$

Feeding this back into (151) and forming the difference $c_\alpha - p_r b_\epsilon$ we get (140). Similarly

$$c_\alpha - b_\epsilon = x_\alpha (p_r - 1) n_\epsilon \tag{158}$$
$$= (b_\epsilon + 1) 2m\lambda \,. \tag{159}$$

This proves the second part of the lemma.

Next let us consider the rows of $M(mp_r)$ indexed by subsets $\beta \subset \{1, 2, \ldots, r\}$ and written as $R(\beta)$. In the special case $\beta = \{r\}$ the vector $R(\{r\})$ can be easily computed as follows.

Lemma 4 The components at α of the row vector $R(\{r\})$ admit the following two representations:

(I)

$$R(\{r\})_\alpha = \begin{cases} \dfrac{c_\alpha - 1}{p_r}, & \text{if} \quad r \notin \alpha, \\ \dfrac{c_\alpha + 1}{p_r}, & \text{if} \quad r \in \alpha \end{cases} \tag{160}$$

(II)

$$R(\{r\})_\alpha = \begin{cases} b_\alpha - 1, & \text{if} \quad r \notin \alpha, \\ b_\epsilon + 1, & \text{if} \quad r \in \alpha \,,\ \epsilon = \alpha - \{r\}. \end{cases} \tag{161}$$

As a simple consequence of the lemma note that

$$R(\{r\}) \notin \mathrm{RowSpace}(DM(m)) \tag{162}$$

as the coordinates of the first and second half of $R(\{r\})$ are manifestly distinct.

For the proof we recall the general defining relation

$$R(\beta)_\alpha \cdot n_\beta = c_\alpha - s_{\beta,\alpha} \tag{163}$$

with $|s_{\alpha,\beta}| < \dfrac{n_\beta}{2}$. In particular if $\beta = \{r\}$ and if $r \notin \alpha$ then we see that

$$R(\{r\})_\alpha \cdot p_r = c_\alpha - s_{\beta,\alpha} \tag{164}$$

with $s_{\beta,\alpha} = 1$. This is clear from $c_\alpha \equiv 1 \mod p$ and from $|s_{\beta,\alpha}| < \dfrac{p_r}{2}$. Substituting this value into (164) we get the first half of (160).

The second half of (160), with the condition $r \in \alpha$ being very similar, is omitted. This proves part (I) of lemma 4. Part (II) then follows by using the relations (139) and (140).

Next it will be shown that any row $R(\beta)$ of the matrix $M(mp_r)$ with $r \notin \beta$ is a linear combination of the corresponding row in $DM(m)$ and a multiple of the vector $R(\{r\})$.

Lemma 5 Assume that $r \notin \beta$. Let $d_{\beta,\alpha}$ be the entry of the matrix $DM(m)$ in the position as indicated by the subsets. Then we have

$$R(\beta)_\alpha - d_{\beta,\alpha} = \begin{cases} \dfrac{2m\lambda}{n_\beta} \cdot (b_\alpha - 1), & \text{if} \quad r \notin \alpha, \\ \dfrac{2m\lambda}{n_\beta} \cdot (b_\alpha + 1), & \text{if} \quad r \in \alpha. \end{cases} \tag{165}$$

This is now almost trivial. First consider the case with $r \notin \alpha$. Let us abbreviate $m_{\beta,\alpha} = R(\beta)_\alpha$. First note that as above

$$c_\alpha = n_\beta \cdot m_{\beta,\alpha} + s_{\beta,\alpha} \quad \text{with} \quad |s_{\beta,\alpha}| < \frac{n_\beta}{2}, \tag{166}$$

$$b_\alpha = n_\beta \cdot d_{\beta,\alpha} + \sigma_{\beta,\alpha} \quad \text{with} \quad |\sigma_{\beta,\alpha}| < \frac{n_\beta}{2}. \tag{167}$$

Subtracting the above two equations and dividing by n_β we see that

$$m_{\beta,\alpha} - d_{\beta,\alpha} = \frac{c_\alpha - b_\alpha}{n_\beta} - \frac{s_{\beta,\alpha} - \sigma_{\beta,\alpha}}{n_\beta}. \tag{168}$$

Now as $r \notin \alpha, r \notin \beta$ we get $c_\alpha - b_\alpha \equiv 0 \mod n_\beta$, and thus each term in (168) should be an integer, so that from

$$|\frac{s_{\beta,\alpha} - \sigma_{\beta,\alpha}}{n_\beta}| < 1$$

it follows that $s_{\beta,\alpha} = \sigma_{\beta,\alpha}$ holds.

Then the difference vector entry in question in (165) is

$$m_{\beta,\alpha} - d_{\beta,\alpha} = \frac{c_\alpha - b_\alpha}{n_\beta} \tag{169}$$

$$= \frac{2m\lambda}{n_\beta} \cdot (b_\alpha - 1) \text{ by (139)}. \tag{170}$$

This shows the first line in (165). The second line follows in a similar way by using (140). The details are omitted. This shows lemma 5.

We now give an interpretation of the results of lemma 4 (II) and of lemma 5 in terms of row vectors. For the case $r \notin \beta$ we see that the difference vector $R(\beta) - d_\beta$ is just a constant multiple (with factor $\dfrac{2m\lambda}{n_\beta}$) of the row vector $R(\{r\})$. In other words in case $r \notin \beta$ the vectors $R(\beta)$ lie in the space LinSpan(RowSpace($DM(m)$), $R(\{r\})$. And conversely the row vectors d_β of the doubled matrix $DM(m)$ lie in the row space RowSpace($M(mp_r)$).

The second half of the proof will show the same for the vectors $R(\beta) - d_\beta$ in case $r \in \beta$ and $\beta \neq \{r\}$. Unfortunately the situation is more complicated here, and we need some further estimates to conclude the proof.

Assume then that $r \in \beta$, that $\beta \neq \{r\}$, and regard first of all those coordinates which are indexed by sets α with $r \notin \alpha$. We let $\gamma = \beta - \{r\}$ and we wish to compare the rows $R(\beta)$ in the matrix $M(mp_r)$ and d_γ in the matrix $DM(m)$.

As before we abbreviate $m_{\beta,\alpha} = R(\beta)_\alpha$ and $d_{\gamma,\alpha}$ as the corresponding entries in row β or γ and in column α.

For convenience we also assume that the prime numbers are ordered according to their sizes, so that $p_1 < p_2 < \cdots < p_{r-1} < p_r$. There is no loss of generality in assuming such an ordering. Of course the assumption $p_r = 1 + 2m\lambda$ guarantees that p_r is the largest of these primes.

Lemma 6 The difference $m_{\beta,\alpha} - d_{\gamma,\alpha}$ takes one of the values 0 or -1. If there exists any α with $m_{\beta,\alpha} - d_{\gamma,\alpha} = -1$, then we must have $\beta = \{1, r\}$, and hence $\gamma = \{1\}$, and the corresponding prime p_1 then necessarily is $p_1 = 3$.

In particular if the smallest prime $p_1 > 3$, then we get an equality of vectors $R(\beta) = d_\gamma$ for all β with $r \in \beta$.

First we deal with the case $r \notin \alpha$. Recall by using (166) and an equation analogous to (167) for the index set γ and from (139) that the difference $c_\alpha - p_r b_\alpha$ can be worked out in two ways as

$$1 - p_r = c_\alpha - b_\alpha = (m_{\beta,\alpha} - d_{\gamma,\alpha})n_\beta + (s_{\beta,\alpha} - p_r\sigma_{\gamma,\alpha})\,. \tag{171}$$

Hence rearranging and applying the triangle inequality gives

$$\begin{aligned} |m_{\beta,\alpha} - d_{\gamma,\alpha}| \cdot n_\beta &\leqslant p_r - 1 + |s_{\beta,\alpha} - p_r\sigma_{\gamma,\alpha}| \leqslant p_r - 1 + |s_{\beta,\alpha}| + p_r|\sigma_{\gamma,\alpha}| \\ &< p_r - 1 + \frac{n_\beta}{2} + \frac{n_\gamma}{2} \cdot p_r = p_r - 1 + n_\beta. \end{aligned}$$

so that

$$|m_{\beta,\alpha} - d_{\gamma,\alpha}| < \frac{p_r - 1}{n_\beta} + 1 < 2 \tag{172}$$

and consequently $m_{\beta,\alpha} - d_{\gamma,\alpha} \in \{0, +1, -1\}$ should hold.

The inequality $|s_{\beta,\alpha} - p_r\sigma_{\gamma,\alpha}| < n_\beta$ implies $-n_\beta < s_{\beta,\alpha} - p_r\sigma_{\gamma,\alpha}$ and in connection with (171) this shows that the case $m_{\beta,\alpha} - d_{\gamma,\alpha} = +1$ is not possible.

Let us now assume that $m_{\beta,\alpha} - d_{\gamma,\alpha} = -1$ holds. Then like before,

$$n_\beta \quad \leqslant \quad p_r - 1 + |s_{\beta,\alpha} - p_r\sigma_{\gamma,\alpha}| < p_r - 1 + \frac{n_\beta}{2} + p_r \cdot |\sigma_{\gamma,\alpha}|$$

holds, so that

$$n_\beta < 2p_r(|\sigma_{\gamma,\alpha}| + 1) - 1, \tag{173}$$

and hence

$$n_\gamma < 2(|\sigma_{\gamma,\alpha}| + 1). \tag{174}$$

We claim now that $|\sigma_{\gamma,\alpha}| = \frac{n_\gamma - 1}{2}$ should hold. As $|\sigma_{\gamma,\alpha}|$ is an integer less than $\frac{n_\gamma}{2}$, it is either equal to $\frac{n_\gamma - 1}{2}$, or it is bounded by

$$|\sigma_{\gamma,\alpha}| \leqslant \frac{n_\gamma}{2} - C \text{ for some constant } C \geqslant 1. \tag{175}$$

But (175) leads to a contradiction with (174):

$$n_\gamma < 2(|\sigma_{\gamma,\alpha}| + 1) \leqslant n_\gamma + 2 - 2C \leqslant n_\gamma\,. \tag{176}$$

Thus we must have $\sigma_{\gamma,\alpha} = \pm\frac{n_\gamma - 1}{2}$.

Now as we have $b_\gamma \equiv \pm 1 \mod p_i$, for all $i = 1, 2, .., r-1$ it follows that for all prime divisors p_j of n_γ the congruences $\sigma_{\gamma,\alpha} \equiv \pm 1 \mod p_j$ also hold. This proves that the integer $\sigma_{\gamma,\alpha}$ satisfies the congruence

$$\sigma_{\gamma,\alpha}^2 \equiv 1 \mod n_\gamma. \tag{177}$$

Hence n_γ should be an odd integer that satisfies the condition

$$\left(\frac{n_\gamma - 1}{2}\right)^2 \equiv 1 \mod n_\gamma\,. \tag{178}$$

Hence there exists an integer g such that

$$n_\gamma^2 - 2n_\gamma + 1 = 4 + 4gn_\gamma, \tag{179}$$

and rearranging and factoring we get that

$$n_\gamma(n_\gamma - 2 - 4g) = 3, \text{ i.e. } n_\gamma \text{ divides } 3. \tag{180}$$

This forces $\gamma = \{1\}$, as γ is not empty, and then $p_1 = 3$ as claimed.

A similar argument can be given in case of coordinates indexed by α with $r \in \alpha$, where the exceptional case occurring is now $m_{\beta,\alpha} - d_{\gamma,\alpha} = +1$. This, however, is omitted for the sake of brevity.

This completes the proof of lemma 6.

We have now shown that in all cases we will have $R(\beta) = d_\gamma$, except for the case $p_1 = 3$ where a single row, namely the one indexed by $\beta = \{1, r\}$ has not yet been decided.

We will discuss this example in conclusion, thereby establishing the proof of theorem 8. To this end we first consider the case of a coordinate indexed by α with $1 \in \alpha, r \notin \alpha$ and such that $p_1 = 3$. We need to compute the corresponding entry of $R(\{1, r\}) - d_{\{1\}}$ which is

$$\left[\!\left[\frac{c_\alpha}{3p_r}\right]\!\right] - \left[\!\left[\frac{b_\alpha}{3}\right]\!\right].$$

We let $z = \dfrac{m}{3} = \dfrac{m}{p_1}$ and as $p_r = 1 + 6z\lambda$ is the largest prime involved we get

$$\left[\!\left[\frac{c_\alpha}{3p_r}\right]\!\right] = \left[\!\left[\frac{c_\alpha + 1}{3p_r}\right]\!\right]. \tag{181}$$

Now consider the congruences $c_\alpha + 1 \equiv 2 \mod p_r$ and $\frac{1}{3} \equiv -2z\lambda \mod p_r$ which can be combined into

$$\frac{c_\alpha + 1}{3} \equiv -4z\lambda \mod p_r\,. \tag{182}$$

Hence we can calculate

$$\begin{aligned}
\left[\!\left[\frac{c_\alpha + 1}{3p_3}\right]\!\right] - \left[\!\left[\frac{b_\alpha}{3}\right]\!\right] &= \frac{\frac{c_\alpha+1}{3} - 2z\lambda - 1}{p_r} - \frac{b_\alpha + 1}{3} && (183)\\
&= \frac{c_\alpha - p_r b_\alpha}{3p_r} - \frac{6z\lambda + 2}{3p_r} - \frac{p_r}{3p_r} && (184)\\
&= \frac{1 - p_r}{3p_r} - \frac{p_r + 1}{3p_r} - \frac{p_r}{3p_r} && (185)\\
&= -1. && (186)
\end{aligned}$$

This shows us to facts. Firstly whenever $p_1 = 3$ is one of the primes involved, then really the case

$$m_{\beta,\alpha} - d_{\gamma,\alpha} = -1$$

considered above does occur. Secondly this case occurs whenever $1 \in \alpha, r \notin \alpha$ happens.

Very similar calculations which are suppressed for brevity's sake show that (with $\beta = \{1, r\}$ and $p_1 = 3$ only)

$$m_{\beta,\alpha} - d_{\gamma,\alpha} = 0 \text{ if } 1 \notin \alpha\ , r \notin \alpha\,; \tag{187}$$

$$m_{\beta,\alpha} - d_{\gamma,\alpha} = 1 \text{ if } 1 \notin \alpha\ , r \in \alpha\,; \tag{188}$$

$$m_{\beta,\alpha} - d_{\gamma,\alpha} = 0 \text{ if } 1 \in \alpha\ , r \in \alpha\,. \tag{189}$$

Now via lemma 4 and the above method it is easy to directly compute the row vector $R(\{r\}) - 3 \cdot R(\{1, r\})$ in its coordinates as

$$R(\{r\})_\alpha - 3 \cdot R(\{1, r\})_\alpha = \begin{cases} 0, & \text{if} \quad 1 \notin \alpha,\ r \notin \alpha, \\ -1, & \text{if} \quad 1 \in \alpha, r \notin \alpha, \\ +1, & \text{if} \quad 1 \notin \alpha, r \in \alpha, \\ 0, & \text{if} \quad 1 \in \alpha, r \in \alpha. \end{cases} \tag{190}$$

Putting things together we get (case $\beta = \{1, r\}, \gamma = \{1\}$)

$$R(\{1, r\}) - d_{\{1\}} = R(\{r\}) - 3 \cdot R(\{1, r\}) \tag{191}$$

and this completes the proof of equality in (138) for the case $p_1 = 3$. Using (162) and (137) we get the rank formula and hence the proof of theorem 8 is done in all cases.

In order to prove the corollary we may use induction on r, starting with $r = 2$, where any two distinct odd primes p_1, p_2 will do, and then each time we step by step build up using theorem 8. The existence of infinitely many examples follows from the Dirichlets theorem on the infinity of primes in an arithmetic progression.

14. Conclusion

In the present paper a matrix of multipliers $M(n)$ was considered. Several properties were derived, and the existence of n attaining a lower bound in case $\rho = \frac{1}{2}$ was established. In the course of the proof it turned out that certain modular calculations were necessary. So the question of the $\mod p$ rank of the matrices $M(n)$ deserves some more interest.

On the other hand, one may form symmetric matrices of the $(c_\alpha c_\beta)$ type [2] and consider their multipliers. This already being of interest in relation with the present material may throw further light on the matrices $M(n)$.

References

1. TB , MRW, Mathematical Aspects of Clasical and Quantum Cryptography, has appeared in IIUM Monograph Series 2003, 216 pages, ISBN 983–2957–19–4.
2. Kamel A.M. Atan, Thomas Bier, A Semi Quadratic Pair of Diophantine Equations, INSPEM, Jabatan Matematik, Universiti Putra Malaysia 2003.
3. B.A. Venkov, Elementary Number Theory, English Translation, Wolters Noordhoff, Groningen, 1970.

Про матриці, зв'язані з розкладом на прості множники непарних цілих чисел

Т.Бір

Факультет природничих наук, університет Султан Кабус, Оман

Отримано 31 січня 2008 р.

В цій роботі у параграфі 5 ми вводимо цілочисельні матриці $M(n)$ для довільної факторизації непарного цілого числа n на r різних непарних простих чисел. Матриці мають декілька версій індексованих параметром $\rho \in [0,1]$, розміром $2^n \times 2^n$, їх ранг задовільняє, наприклад, для $\rho = 1/2$, нерівність з Теореми 4: $r+1\ldots$, що одержується за допомогою Теореми 1, яка обговорюється окремо у перших параграфах. Випадки $\rho = 0, 1, 1/2$ аналізуються більш детально, наводяться різноманітні приклади для $\rho \neq 0, 1, 1/2$. Подаємо ряд головних результатів: Теорема 5, що описує дуальність випадків $\rho = 0$ і $\rho = 1$, Теорема 6, що описує періодичність. Можливо найголовнішою є Теорема 8 (дійсна тільки для $\rho = 1/2$) про існування непарних, без квадратів, цілих чисел n з r непарними простими множниками, таких, що $\mathrm{rank}(M(n)) = r + 1$, тобто досягає нижньої межі, згаданої вище.

Ключові слова: *факторизація, матриці*

PACS: *02.10.Yn*