A theorem on roots of unity and a combinatorial principle

Simon Lentner and Daniel Nett
Algebra and Number Theory, Hamburg University,
Bundesstraße 55, D-20146 Hamburg

ABSTRACT. Given a finite set of roots of unity, we show that all power sums are non-negative integers iff the set forms a group under multiplication. The main argument is purely combinatorial and states that for an arbitrary finite set system the non-negativity of certain alternating sums is equivalent to the set system being a filter.

As an application we determine all discrete Fourier pairs of $\{0, 1\}$-matrices. This technical result is an essential step in the classification of R-matrices of quantum groups.

CONTENTS

1. INTRODUCTION

In this paper we prove the following main theorem:

Theorem (3.1). *Let U be a non-empty finite set of complex roots of unity and consider the power sums $a_k := \sum_{\zeta \in U} \zeta^k$. Then all a_k are non-negative integers iff U is actually a multiplicative group of roots of unity (i.e. all n-th roots of unity for some n).*

The proof of the theorem is combinatorial in nature. Especially if the order of all ζ are squarefree numbers and hence correspond to subsets of primes, the statement amounts to the following apparently new combinatorial principle, which is interesting in its own right:

Theorem (2.1). *Let N be finite set, $\mathcal{P}(N)$ denote the power set of N and $\mathcal{E} \subset \mathcal{P}(N)$. Let $\mu \colon \mathcal{P}(N) \to [0, \infty]$ be a measure on $\mathcal{P}(N)$. Then the following is equivalent:*

(i) $a_C := (-1)^{|N|} \sum_{D \in \mathcal{E}} (-1)^{|C \cup D|} e^{\mu(C-D)} \geq 0$ *for all $C \subset N$.*
(ii) $\mathcal{E} = \{D \subset N \mid D \supset A\}$ *for some $A \subset N$. Such a set $\mathcal{E}$ is called a filter in N.*

The proof of the main theorem proceeds along these lines with μ some explicit number theoretic function. But to include the non-square-free case the set system $\mathcal{E} \subset \mathcal{P}(N)$ is roughly replaced by the set of orders of $\zeta \in U$, which is partially ordered via divisibility. It would be nice to prove the main theorem even more generally for any partially ordered set. Note that the expressions we calculate remind very strongly on partition functions in statistical physics.

We briefly discuss the proof strategy: We perform an induction on the greatest common multiple N of the orders of the $\zeta \in U$. Given the set of numbers $\mathcal{E} = \{N/ord(\zeta) \mid \zeta \in U\}$ we define sets $\mathcal{E}_p$ by decreasing the power of a prime p in each number and removing non-divisible ones (Definition 3.7). In Lemma 3.8 we show that the assumption of $a_k \geq 0$ for $\mathcal{E}$ implies it also for all $\mathcal{E}_p$. In Lemma 3.9 we use the induction hypothesis that all $\mathcal{E}_p$ are filters to show that $\mathcal{E}_p$ is almost a filter. Since an explicit calculation in Lemma 3.6 has shown that small modifications of a filter usually violate the condition $a_k \geq 0$ for some k we see that $\mathcal{E}$ is actually a filter.

As an application we prove the following theorem:

Theorem (4.3). *All idempotents ε/N of the group algebra $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$ with $\varepsilon_{ij} \in \{0,1\}$, or equivalently all discrete Fourier pairs $\varepsilon, \bar{\varepsilon}$ of $\{0,1\}$-matrices are either*

$$\varepsilon_{ij} = \delta_{(\frac{N}{d}|i)}\delta_{(d|j-t\frac{i}{N/d})}, \tag{1.1}$$

for a unique $d \mid N$ and $0 \leq t \leq d-1$ or they are trivial $\varepsilon = \bar{\varepsilon} = 0$.

The significance of this technical result is the classification of R-matrices for quantum groups and hence for constructing certain braided categories. Lusztig's ansatz for such R-matrices [Lus93] Sec. 32.1, contains a free parameter $R_0 \in \mathbb{C}[\Lambda \times \Lambda]$ for some abelian group Λ and a system of equations on R_0. In the last section of this paper, using the previous theorem, we will solve a subset of these equations only depending on an abelian group.

Once these explicit solutions have been obtained, they can be plugged into the remaining equations which depend heavily on the specific parameters of the quantum group. This is done in a rather Lie-theoretic case-by-case argument in [LN14].

2. A combinatorial principle

Before we turn to the proof of the main Theorem 3.1 we prove the following combinatorial principle. It shows that the main Theorem does not depend on specific properties of prime numbers, but is cominatorial in nature. It also gives the blueprint for the proof of the main theorem.

Theorem 2.1. *Let N be finite set, $\mathcal{P}(N)$ denote the power set of N and $\mathcal{E} \subset \mathcal{P}(N)$. Let $\mu\colon \mathcal{P}(N) \to [0, \infty]$ be a measure on $\mathcal{P}(N)$. Then the following is equivalent:*

(i) $a_C := (-1)^{|N|} \sum_{D \in \mathcal{E}} (-1)^{|C \cup D|} e^{\mu(C-D)} \geq 0$ for all $C \subset N$.

(ii) $\mathcal{E} = \{D \subset N \mid D \supset A\}$ *for some* $A \subset N$. *Such a set* $\mathcal{E}$ *is called a* filter *in* N *(see e.g.* [Bou66] *§6).*

The remainder of this section is devoted to the proof of this theorem.

A straightforward calculation gives the values of the a_C if $\mathcal{E}$ is a filter. It shows immediately the implication $(i) \rightarrow (ii)$, but the precise value will also be crucial to the proof of the converse in what follows:

Lemma 2.2. *Let* $\mathcal{E}$ *be a filter, i.e.* $\mathcal{E} = \{D \subset N \mid D \supset A\}$ *for some* $A \subset N$. *Then for any* $C \subset N$ *we have*

$$a_C := (-1)^{|N|} \sum_{D \in \mathcal{E}} (-1)^{|C \cup D|} e^{\mu(C-D)} = \begin{cases} e^{\mu(N-A)} \prod_{p \in N-A} \left(1 + e^{-\mu(p)}\right), & C \cup A = N \\ 0, & else \end{cases}$$

Proof.

$$a_C = (-1)^{|N|} \sum_{A \subset D \subset N} (-1)^{|C \cup D|} e^{\mu(C-D)}$$

$$= (-1)^{|N|} \sum_{D' \subset N-A} (-1)^{|C \cup A \cup D'|} e^{\mu(C-A-D')}$$

$$= (-1)^{|N-A|} \sum_{D' \subset N-A} (-1)^{|(C-A) \cup D'|} e^{\mu(C-A-D')}$$

This shows that the value of a_C for the filter generated by A in N is equal to the value of a_{C-A} for the filter generated by $\varnothing$ in $N - A$. Thus is suffices to show the claim for the filter $\mathcal{E} = \mathcal{P}(N)$ generated by $A = \varnothing$:

$$a_C = (-1)^{|N|} \sum_{D \subset N} (-1)^{|C \cup D|} e^{\mu(C-D)}$$

$$= (-1)^{|N|} \sum_{D_1 \subset C, D_2 \subset N-C} (-1)^{|C|+|D_2|} e^{\mu(C)-\mu(D_1)}$$

$$= (-1)^{|N|+|C|} e^{\mu(C)} \left(\sum_{D_2 \subset N-C} (-1)^{|D_2|} \right) \left(\sum_{D_1 \subset C} e^{-\mu(D_1)} \right)$$

$$= (-1)^{|N|+|C|} e^{\mu(C)} \left(\prod_{p \in N-C} (1-1) \right) \left(\prod_{p \in C} \left(1 + e^{-\mu(p)}\right) \right)$$

$$= \begin{cases} e^{\mu(N)} \prod_{p \in N} \left(1 + e^{-\mu(p)}\right), & C = N \\ 0, & else \end{cases}$$

The general formula for arbitrary A follows by again replacing N with $N - A$ and C by $C - A$. ∎

We use this result to show that if $\mathcal{E}$ is a small modification of a filter, the main assumption $a_C \geq 0$ for all $C \subset N$ usually fails to be true.

Lemma 2.3.

(a) *Let* $\mathcal{E} \neq \mathcal{P}(N)$ *be a filter in* $|N| > 1$, *then* $\mathcal{E} \cup \{\varnothing\}$ *gives* $a_C < 0$ *for some* $C \subset N$.

(b) Let $\mathcal{E} = \mathcal{P}(N)$ in $|N| > 1$, then $\mathcal{E} \setminus \{\varnothing\}$ gives $a_C < 0$ for some $C \subset N$.

Note that on the other hand for $|N| = 1$ and $\mathcal{E}$ the only filter $\mathcal{E} \neq \mathcal{P}(N)$ we have that both $\mathcal{E} \cup \varnothing$ and $\mathcal{P}(N) - \varnothing$ are filters (namely $\mathcal{P}(N)$ and $\mathcal{E}$).

Proof. (a) By assumption $\mathcal{E}$ is a filter generated by some $A \neq \varnothing$ for $|N| > 1$. We wish to find a negative value of some $\tilde{a}_C$ for the set system $\tilde{\mathcal{E}} := \mathcal{E} \cup \{\varnothing\}$: Suppose first that also $A \neq N$ and choose some $p \in N - A$, then $a_{N-p} = 0$ by Lemma 2.2 and thus:

$$\tilde{a}_{N-p} = (-1)^{|N|} \sum_{D \in \mathcal{E} \cup \{\varnothing\}} (-1)^{|C \cup D|} e^{\mu(C-D)}$$
$$= a_{N-p} + (-1)^{|N|+|N-p|} e^{\mu(N-p)}$$
$$= -e^{\mu(N-p)} < 0$$

Suppose now that $A = N$ and choose some $q \in N$, then again by Lemma 2.2:

$$\tilde{a}_{N-q} = (-1)^{|N|} \sum_{D \in \mathcal{E} \cup \{\varnothing\}} (-1)^{|C \cup D|} e^{\mu(C-D)}$$
$$= a_{N-q} + (-1)^{|N|+|N-q|} e^{\mu(N-q)}$$
$$= 1 - e^{\mu(N-q)} < 0$$

(b) By assumption $\mathcal{E} = \mathcal{P}(N)$ for $|N| > 1$, so $\mathcal{E}$ is the filter generated by $A = \{\varnothing\}$. Then again by Lemma 2.2 $a_C = 0$ for $C \neq N$. Choose any $q \neq p \in N$, then we calculate $\tilde{a}_{N-\{p,q\}}$ for the filter $\tilde{\mathcal{E}} := \mathcal{E} - \{\varnothing\}$:

$$\tilde{a}_{N-\{p,q\}} = (-1)^{|N|} \sum_{D \in \mathcal{E} - \{\varnothing\}} (-1)^{|C \cup D|} e^{\mu(C-D)}$$
$$= a_{N-q} - (-1)^{|N|+|N-\{p,q\}|} e^{\mu(N-\{p,q\})}$$
$$= 1 - e^{\mu(N-\{p,q\})} < 0$$

∎

We now proceed by introducing the induction step along $|N|$:

Definition 2.4. Let $\mathcal{E}$ be any set system in N and $p \in N$, then we define a new set system for $N - p$ by
$$\mathcal{E}_p = \{D - p \mid p \in D, D \in \mathcal{E}\}$$
For $C \subset N - p$ we denote by a_C^p the corresponding sum over $\mathcal{E}_p$, i.e.
$$a_C^p = (-1)^{|N-p|} \sum_{D \in \mathcal{E}_p} (-1)^{|C \cup D|} e^{\mu(C-D)}$$

We will in the following only consider $\mathcal{E}_p$ for all p, such that there exists any $D \in \mathcal{E}$ with $p \in D$, so $\mathcal{E}_p$ is not empty.

We first wish to prove that our main assumption $a_C \geq 0$ implies $a_C^p \geq 0$ in $\mathcal{E}_p$:

Lemma 2.5. *For any $p \in N$ we get for all $C \in \mathcal{E}_p$ (note that $p \notin C$):*
$$a_C^p = \frac{e^{\mu(p)}}{1 + e^{\mu(p)}} a_C + \frac{1}{1 + e^{\mu(p)}} a_{C \cup p}$$
In particular, $a_C \geq 0$ for all $C \in \mathcal{E}$ implies $a_C^p \geq 0$ for all $C \in \mathcal{E}_p$.

Proof. We calculate the right hand side by splitting the sum over all $D \in \mathcal{E}$ into two summands for all $p \notin D$ resp. $p \in D$ and use $p \notin C$. The latter set of D then correspond to $D' = D - p$ in $\mathcal{E}_p$:

$$\frac{e^{\mu(p)}}{1+e^{\mu(p)}}a_C + \frac{1}{1+e^{\mu(p)}}a_{C+p}$$

$$= (-1)^{|N|}\frac{e^{\mu(p)}}{1+e^{\mu(p)}}\sum_{p\in D\in\mathcal{E}}(-1)^{|C\cup D|}e^{\mu(C-D)} + (-1)^{|N|}\frac{1}{1+e^{\mu(p)}}\sum_{p\in D\in\mathcal{E}}(-1)^{|C\cup p\cup D|}e^{\mu((C\cup p)-D)}$$

$$+ (-1)^{|N|}\frac{e^{\mu(p)}}{1+e^{\mu(p)}}\sum_{p\notin D\in\mathcal{E}}(-1)^{|C\cup D|}e^{\mu(C-D)} + (-1)^{|N|}\frac{1}{1+e^{\mu(p)}}\sum_{p\notin D\in\mathcal{E}}(-1)^{|C\cup p\cup D|}e^{\mu((C\cup p)-D)}$$

$$= (-1)^{|N|}\frac{e^{\mu(p)}}{1+e^{\mu(p)}}\sum_{p\in D\in\mathcal{E}}(-1)^{|C\cup D|}e^{\mu(C-D)} + (-1)^{|N|}\frac{1}{1+e^{\mu(p)}}\sum_{p\in D\in\mathcal{E}}(-1)^{|C\cup D|}e^{\mu(C-D)}$$

$$+ (-1)^{|N|}\frac{e^{\mu(p)}}{1+e^{\mu(p)}}\sum_{p\notin D\in\mathcal{E}}(-1)^{|C\cup D|}e^{\mu(C-D)} + (-1)^{|N|}\frac{1}{1+e^{\mu(p)}}\sum_{p\notin D\in\mathcal{E}}(-1)^{|C\cup D|+1}e^{\mu(C-D)+\mu(p)}$$

$$= \left(\frac{e^{\mu(p)}}{1+e^{\mu(p)}} + \frac{1}{1+e^{\mu(p)}}\right)\cdot(-1)^{|N|}\sum_{p\in D\in\mathcal{E}}(-1)^{|C\cup D|}e^{\mu(C-D)}$$

$$+ \left(\frac{e^{\mu(p)}}{1+e^{\mu(p)}} - \frac{1}{1+e^{\mu(p)}}\cdot e^{\mu(p)}\right)\cdot(-1)^{|N|}\sum_{p\notin D\in\mathcal{E}}(-1)^{|C\cup D|}e^{\mu(C-D)}$$

$$= (-1)^{|N|}\sum_{p\in D\in\mathcal{E}}(-1)^{|C\cup D|}e^{\mu(C-D)} = (-1)^{|N-p|}\sum_{D'\in\mathcal{E}_p}(-1)^{|C\cup D'|}e^{\mu(C-D')} = a_C^p$$

∎

Thus if all $a_C \geq 0$ by induction hypothesis all $\mathcal{E}_p$ are filters. We now conclude the induction that $\mathcal{E}$ is a filter if all possible reductions $\mathcal{E}_p$ are filters. As induction step, we use the following lemma.

Lemma 2.6. *Let $\mathcal{E}$ be a set system for N such that all $\mathcal{E}_p$ are filters generated by sets $A_p \subset N - p$. Then either there exists a $p \in N$ with $p \in A_q$ for all $p \neq q$ or for all $p \in N$ we have $A_p = \varnothing$.*
In the first case we show that $\mathcal{E}$ is the filter generated by $p \cup A_p$ or $\mathcal{E}$ is the set system consisting of this filter together with $D = \varnothing$. In the second case we show $\mathcal{E} = \mathcal{P}(N)$ or $\mathcal{E} = \mathcal{P}(N) - \varnothing$.

Proof. Assume there exists q' with $A_{q'} \neq \varnothing$ and let $p \in A_{q'}$, then we claim $p \in A_q$ for all $q \neq p$. We prove this by contradiction, since if $p \notin A_q$ for some q then we consider $q' \cup A_q \in \mathcal{E}_q$ (since $\mathcal{E}_q$ is a filter) and hence $q \cup q' \cup A_q \in \mathcal{E}$ (by definition of $\mathcal{E}_q$). But then $q \cup A_q \in \mathcal{E}_{q'}$ and $A_{q'} \subset q \cup A_q$ (since $\mathcal{E}_{q'}$ is a filter). But this contradicts $p \notin A_q$, which shows the first part of the Lemma.

We now prove the consequences in the two cases. In the first case we assume it exists $p \in A_q$ for all $q \neq p$. Let $\mathcal{D} \supset p \cup A_p$ then $D \in \mathcal{E}_p$ (since E_p is a filter) and $D \in \mathcal{E}$ (by definition of $\mathcal{E}_p$). Let now conversely by $D \in \mathcal{E}$. If $p \in D$ then we have $D - p \in \mathcal{E}_p$ (by

definition of $\mathcal{E}_p$) and hence also $D \supset A_p$ (since $\mathcal{E}_p$ is a filter), implying $\mathcal{D} \supset p \cup A_p$. If $p \notin D$ then either $D = \varnothing$ or some $q \in D$. In the latter case $D - q \in \mathcal{E}_q$, hence $D - q \supset A_q \ni p$ which is a contradicion. So either $\mathcal{D} \supset p \cup A_p$ or $D = \varnothing$ as asserted.

In the second case we assume $A_p = \varnothing$ for all $p \in N$, hence any for any set $D \neq \varnothing$ we may chose some $p \in D$ and yield $D - p \in \mathcal{E}_p$ and hence $D \in \mathcal{E}_q$. Hence any set with the possible exception of $D = \varnothing$ is in $\mathcal{E}$ as asserted. ∎

We can now conclude the inductive proof of the implication (i)→(ii) in Theorem 2.1: For $|N| = 0$ the only set system is $\mathcal{E} = \{\varnothing\}$ and is a filter. Let $|N| \geq 1$ and $\mathcal{E}$ such that all $a_C \geq 0$, then $a_C^p \geq 0$ for all $p \in N$ by Lemma 2.5. Thus by induction hypothesis all $\mathcal{E}_p$ are filters. Then by Lemma 2.6 we have that either $\mathcal{E}$ is a filter (in which case the induction step is finished) or some filter $\mathcal{E} \neq \mathcal{P}(N)$ together with $\varnothing$ or $\mathcal{E} = \mathcal{P}(N) - \{\varnothing\}$. By Lemma 2.3 these two cases can only fulfill $a_C \geq 0$ for $|N| = 1$ where both are filters. This concludes the proof of Theorem 2.1.

3. A THEOREM ABOUT ROOTS OF UNITY

Theorem 3.1. *Let U be a non-empty finite set of complex roots of unity and consider the power sums $a_k := \sum_{\zeta \in U} \zeta^k$. Then all a_k are non-negative integers iff U is actually a multiplicative group of roots of unity (i.e. all n-th roots of unity for some n).*

The remainder of this section is devoted to the proof of this theorem.

Since U is finite, we may assume some integer N such that $U \subset \Sigma_N = \{\zeta \in \mathbb{C} \mid \zeta^N = 1\}$. Let ξ_N the primitive N-th root of unity $\exp(2\pi i/N)$. We start with the observation, that the set U is a union of Galois orbits of $\mathrm{Gal}(\xi_N)$ acting on Σ_N.

In the following, we denote by (a,b) the greatest common divisor of two integers a, b.

Lemma 3.2. *Any U as in Theorem 3.1 is invariant under the Galois group $G = \mathrm{Gal}(\xi_N)$, i.e. it is a union of orbits of G acting on Σ_N. Each orbit consist of all primitive roots of unity for some divisor of N and hence a_k only depends on (k, N).*

Proof. Let $p(x) = \prod_{\zeta \in U} (x - \zeta) \in \mathbb{C}[x]$, i.e. $p(\zeta) = 0$ for all $\zeta \in U$. Denote $t = |U|$ and $U = \{\zeta_1, \ldots, \zeta_t\}$. For $0 \leq k \leq t$ let $\sigma_k(x_1, \ldots, x_t) = \sum_{1 \leq j_1 < \ldots < j_k \leq t} x_{j_1} \cdot \ldots \cdot x_{j_k}$ be the elementary symmetric polynomials. Then $p(x) = \sum_{k=0}^{t} (-1)^{t-k} \sigma_{t-k}(\zeta_1, \ldots, \zeta_t) x^k$. Let $s_k(x_1, \ldots, x_t) = \sum_{i=1}^{t} x_i^k$, then we have in particular, $a_k = s_k(\zeta_1, \ldots, \zeta_t)$. By the Newton identities, the $\sigma_k(x_1, \ldots, x_t)$ can be expressed as sums of powers of the s_k with rational coefficients, e.g. $\sigma_2 = \frac{1}{2}s_1^2 - \frac{1}{2}s_2$. Thus, we have that the coefficients of $p(x)$, the $\sigma_k(\zeta_1, \ldots, \zeta_k)$, are sums of integers with rational coefficients, hence $p(x) \in \mathbb{Q}[x]$. (In fact, we have $p(x) \in \mathbb{Z}[x]$, since the $\sigma_k(\zeta_1, \ldots, \zeta_t)$ are algebraic integers in $\mathbb{Q}$, hence in $\mathbb{Z}$.) Thus we get, that the Galois group G permutes the roots of $p(x)$, i.e. U consists of orbits of G. ∎

Definition 3.3. *Let $N \in \mathbb{N}$. The set $\mathcal{D}(N) = \{d \in \mathbb{N} \mid d \mid N\}$ is the set of all divisors of N. We call a set $\mathcal{E} \subset \mathcal{D}(N)$ a filter in $\mathcal{D}(N)$ if there exist an $e \mid N$ such that $\mathcal{E} = e\mathcal{D}(N/e) = \{d \mid N \mid e \mid d\}$. In this case we write $\mathcal{E} = (e)_N$ or shortly (e) for the filter in $\mathcal{D}(N)$.*

By Lemma 3.2, the set U is of the form $U = \bigcup_{d \in \mathcal{E}} \{\xi_N^i \mid (N, i) = d\}$ for a set $\mathcal{E} \subset \mathcal{D}(N)$. We wish to prove that $\mathcal{E}$ is a filter and hence U is a subgroup. For $c \mid N$ we have

$$a_c = \sum_{\zeta \in U} \zeta^c = \sum_{d \in \mathcal{E}} \sum_{(i,N)=d} \xi_N^{ic}.$$

A straightforward calculation gives the values of the a_c.

Lemma 3.4. *For $N \in \mathbb{N}$ and $c \in \mathcal{D}(N)$, we have*

$$a_c = \sum_{d \in \mathcal{E}} \frac{\varphi(N/d)}{\varphi(N/(N, dc))} \mu\left(\frac{N}{(N, dc)}\right).$$

Here, $\varphi \colon \mathbb{N} \to \mathbb{N}$ is the Euler φ-function, given by $\varphi(\prod_{i=1}^t p_i^{r_i}) = \prod_{i=1}^t (p_i - 1)p_i^{r_i - 1}$ for mutually different prime numbers p_i, and $\mu \colon \mathbb{N} \to \{-1, 0, 1\}$ is the Moebius function, defined by $\mu(n) = 1$ if n is square-free and has an even number of prime factors, $\mu(n) = -1$ if n is square-free and has an odd number of prime factors and $\mu(n) = 0$ if n has a squared prime factor.

Proof. It is an elementary number theoretical fact, that for an primitive N-th root of unity ξ we have

$$\sum_{\substack{i=1 \\ (i,N)=1}}^N \xi^i = \mu(N)$$

with the Moebius function μ. For $d \mid N$ we have

$$\sum_{\substack{i=1 \\ (i,N)=d}}^N \xi_N^i = \sum_{\substack{i=1 \\ (i,N/d)=1}}^{N/d} \xi_{N/d}^i = \mu(N/d)$$

with primitive (N/d)-th root of unity $\xi_{N/d}$. For $c \mid N$ we get

$$\sum_{\substack{i=1 \\ (i,N)=d}}^N \xi^{ic} = \sum_{\substack{i=1 \\ (i,N/d)=1}}^{N/d} \xi_{N/d}^{ic} = \sum_{\substack{i=1 \\ (i,N/d)=1}}^{N/d} \xi_{N/(N,dc)}^i = \frac{\varphi(N/d)}{\varphi(N/(N, dc))} \mu\left(\frac{N}{(N, dc)}\right),$$

since the last sum has $\varphi(N/d)$ summands which contain $\varphi(N/(N, dc))$-times all primitive $N/(N, dc)$-th roots of unity and their sum gives $\mu(N/(N, dc))$. ∎

Next, we calculate the a_c explicitly in the case $\mathcal{E}$ is a filter in $\mathcal{D}(N)$.

Lemma 3.5. *Let $c \mid N$ and $\mathcal{E} = (e)$ be a filter for some $e \mid N$. Then*

$$a_c = \begin{cases} N/e, & c \in (N/e)_e = (N/e)\mathcal{D}(e), \\ 0, & else. \end{cases}$$

Especially, for a $\mathcal{E}$ being a filter, we have $a_c \geq 0$ for all $c \in \mathcal{D}(N)$.

Proof. We calculate a_c for all $c \in \mathcal{D}(N)$:

$$
\begin{aligned}
a_c &= \sum_{d \in \mathcal{E}} \frac{\varphi(N/d)}{\varphi(N/(N,dc))} \mu\left(\frac{N}{(N,dc)}\right) \\
&= \sum_{d' \in \mathcal{D}(N/e)} \frac{\varphi(N'e/d'e)}{\varphi(N'e/(N'e,d'ec))} \mu\left(\frac{N'e}{(N'e,d'ec)}\right) \qquad (N' = N/e, \ d' = d/e) \\
&= \sum_{d' \in \mathcal{D}(N/e)} \frac{\varphi(N'/d')}{\varphi(N'/(N',d'c))} \mu\left(\frac{N'}{(N',d'c)}\right)
\end{aligned}
$$

Thus, we can assume $\mathcal{E} = \mathcal{D}(N)$ and omit the superscript $'$. Since φ and μ are multiplicative functions, we may assume $N = p^{N_p}$, $N_p > 0$, for a prime p and $d = p^{d_p}$, $c = p^{c_p}$ for $d, c \mid N$ and $0 \le d_p, c_p \le N_p$. Then

$$
\begin{aligned}
a_c &= \sum_{d \in \mathcal{D}(N)} \frac{\varphi(N/d)}{\varphi(N/(N,dc))} \mu\left(\frac{N}{(N,dc)}\right) \\
&= \sum_{d \in \mathcal{D}(N)} \frac{\varphi(p^{N_p - d_p})}{\varphi(p^{N_p - \min\{d_p + c_p, N_p\}})} \mu\left(p^{N_p - \min\{d_p + c_p, N_p\}}\right) \\
&= \sum_{i=0}^{N_p} \frac{\varphi(p^{N_p - i})}{\varphi(p^{N_p - \min\{i + c_p, N_p\}})} \mu\left(p^{N_p - \min\{i + c_p, N_p\}}\right)
\end{aligned}
$$

Since the μ-term equals 0 if $i + c_p < N_p - 1$, is equal to -1 if $i + c_p = N_p - 1$ and $+1$ otherwise, we get

$$
\begin{aligned}
a_c &= \sum_{i=0}^{N_p - 1} (p-1)p^{N_p - i - 1} + 1 \\
&= (p-1)p^{N_p - 1} \frac{p^{-N_p} - 1}{p^{-1} - 1} + 1 \\
&= p^{N_p} - 1 + 1 = p^{N_p} = N,
\end{aligned}
$$

for $c_p = N_p$, and

$$
\begin{aligned}
a_c &= \sum_{i = N_p - c_p - 1}^{N_p - 1} \frac{\varphi(p^{N_p - i})}{\varphi(p^{N_p - \min\{i + c_p, N_p\}})} \mu\left(p^{N_p - \min\{i + c_p, N_p\}}\right) + 1 \\
&= -\frac{(p-1)p^{N_p - (N_p - c_p - 1) - 1}}{(p-1)p^{N_p - (N_p - c_p - 1 + c_p) - 1}} + \sum_{i = N_p - c_p}^{N_p - 1} (p-1)p^{N_p - i - 1} + 1 \\
&= -p^{c_p} + (p-1)p^{N_p - 1} p^{-(N_p - c_p)} \sum_{i=0}^{c_p - 1} p^{-i} + 1 \\
&= -p^{c_p} - (1 - p^{c_p}) + 1 = 0,
\end{aligned}
$$

for $0 \le c_p < N_p$. Thus, in the general case $\mathcal{E} = (e)$, we have $a_c = N' = N/e$ for $c = N/e$ and all multiples, hence the lemma is proven. ∎

We use this result to show that if $\mathcal{E}$ is a small modification of a filter, the main assumption $a_c \geq 0$ for all $c \in \mathcal{D}(N)$ usually fails to be true.

Lemma 3.6.

(a) Let $\mathcal{E} = (e) \neq \mathcal{D}(N)$ be a filter, but not (p) for $N = p^n$ a prime power. Then $\mathcal{E} \cup \{1\}$ gives $a_c < 0$ for some c. If $N = p^n$ for some prime number p, $n \in \mathbb{N}$, and $\mathcal{E} = (p)$ a filter, then $\mathcal{E} \cup \{1\}$ is a filter as well.

(b) Let $\mathcal{E} = (1) = \mathcal{D}(N)$ and N be not a prime power. Then $\mathcal{E} \setminus \{1\}$ gives $a_c < 0$ for some c. In the case $N = p^n$, the set $\mathcal{E} \setminus \{1\}$ is a also a filter, namely (p).

Proof. (a) Assume at first, that $N = \prod_{p|N} p^{N_p}$, $N_p \geq 1$ for all p, is not a prime power. If $p \nmid e$ for a prime divisor $p \mid N$, we have $N/e \nmid N/p$, and therefore $a_{N/p} = 0$ by Lemma 3.5. We calculate the value $\tilde{a}_{N/p}$ for $\mathcal{E} \cup \{1\}$:

$$\tilde{a}_{N/p} = \sum_{d \in \mathcal{E} \cup \{1\}} \frac{\varphi(N/d)}{\varphi(N/(N, d(N/p)))} \mu(N/(N, d(N/p)))$$

$$= a_{N/p} + \frac{\varphi(N)}{\varphi(p)} \mu(p) = 0 + \frac{\varphi(N)}{p-1}(-1) < 0.$$

Let $e = \prod_{p|N} p^{e_p}$ with primes p. If $e_p \geq 1$ for all p we have $N/e \leq N/(\prod_{p|N} p) = \prod_{p|N} p^{N_p - 1}$. We calculate $\tilde{a}_{N/q}$ for some prime divisor q and $\mathcal{E} \cup \{1\}$:

$$\tilde{a}_{N/q} = a_{N/q} + \frac{\varphi(N)}{\varphi(q)} \mu(q)$$

$$\leq \prod_{p|N} p^{N_p - 1} - \frac{\prod_{p|N}(p-1)p^{N_p - 1}}{q-1}$$

$$= \prod_{p|N} p^{N_p - 1} \left(1 - \prod_{p \neq q}(p-1)\right) < 0.$$

Assume now, $N = p^n$ and $e = p^k$ for $1 < k \leq n$, thus $a_c = p^{n-k}$ for all $c = p^{n-k+l}$ for $0 \leq l \leq k$. We calculate $\tilde{a}_{p^{n-1}}$ for $\mathcal{E} \cup \{1\}$:

$$\tilde{a}_{p^{n-1}} = a_{p^{n-1}} + \frac{\varphi(p^n)}{\varphi(p)} \mu(p) = p^{n-k} - p^{n-1} < 0.$$

If $N = p^n$ and $\mathcal{E} = (p)$, we have $\mathcal{E} \cup \{1\} = \mathcal{D}(N)$, hence it is a filter.

(b) If $\mathcal{E} = \mathcal{D}(N)$, it is $a_c = N$ for $c = N$ and 0 otherwise by Lemma 3.5. Since N is not a prime power, there exist distinct primes $p, q \mid N$. We calculate $\tilde{a}_c$ for $c = N/(pq)$ and $\mathcal{E} \setminus \{1\}$:

$$\tilde{a}_c = a_c - \frac{\varphi(N)}{\varphi(N/(N, N/(pq)))} \mu(N/(N, N/(pq)))$$

$$= 0 - \frac{\varphi(N)}{\varphi(pq)} \mu(pq) = -\frac{\varphi(N)}{(p-1)(q-1)} < 0.$$

$\blacksquare$

The main part of the proof of Theorem 3.1 is the following claim, which we show by induction: Let $N \in \mathbb{N}$, $\mathcal{D}(N)$ the set of all divisors of N and $\mathcal{E} \subset \mathcal{D}(N)$. If

$$a_c = \sum_{d \in \mathcal{E}} \frac{\varphi(N/d)}{\varphi(N/(cd, N))} \mu(N/(cd, N)) \geq 0 \tag{3.1}$$

for all $c \in \mathcal{D}(N)$, then $\mathcal{E}$ is a filter in $\mathcal{D}(N)$ as is Definition 3.3.

Definition 3.7. Let $N \in \mathbb{N}$ and $\mathcal{E} \subset \mathcal{D}(N)$. For a prime factor $p \mid N$ we define a new set of divisors of N/p, namely

$$\mathcal{E}_p = \{ d/p \mid d \in \mathcal{E}, \ p \mid d \} \subset \mathcal{D}(N/p).$$

For $c \in \mathcal{D}(N/p)$ we denote by a_c^p the corresponding sum over $\mathcal{E}_p$, i.e.

$$a_c^p = \sum_{(d/p) \in \mathcal{E}_p} \frac{\varphi\left(\frac{N/p}{d/p}\right)}{\varphi\left(\frac{N/p}{(N/p, cd/p)}\right)} \mu\left(\frac{N/p}{(N/p, cd/p)}\right).$$

We will in the following only consider $\mathcal{E}_p$ for all p, such that there exists any $d \in \mathcal{E}$ with $p|d$, so $\mathcal{E}_p$ is not empty.

We use this as induction step $N/p \mapsto N$. We first wish to prove that $a_c \geq 0$ for $\mathcal{E}$ implies $a_c^p \geq 0$ for $\mathcal{E}_p$ and all $c \in \mathcal{D}(N/p)$.

Lemma 3.8. *For any $p|N$ with $\mathcal{E}_p$ we get for all $c \in \mathcal{D}(N/p)$:*

$$a_c^p = \begin{cases} a_c, & \text{if } pc \mid N/p, \\ \frac{1}{p}((p-1)a_c + a_{pc}) & \text{if } pc \nmid N/p. \end{cases}$$

In particular, $a_c \geq 0$ for all $c \in \mathcal{D}(N)$ implies $a_c^p \geq 0$ for all $c \in \mathcal{D}(N/p)$.

Proof. For $\mathcal{E}$ and $p \in \mathcal{D}(N)$ such that p divides at least one $d \in \mathcal{E}$, the set $\mathcal{E}_p$ is non-empty. We calculate the value of a_c^p for all $c \in \mathcal{D}(N/p)$:

$$\begin{aligned} a_c^p &= \sum_{(d/p) \in \mathcal{E}_p} \frac{\varphi\left(\frac{N/p}{d/p}\right)}{\varphi\left(\frac{N/p}{(N/p, cd/p)}\right)} \mu\left(\frac{N/p}{(N/p, cd/p)}\right) \\ &= \sum_{\substack{d \in \mathcal{E} \\ p|d}} \frac{\varphi\left(\frac{N}{d}\right)}{\varphi\left(\frac{N}{(N, cd)}\right)} \mu\left(\frac{N}{(N, cd)}\right) \\ &= a_c - \underbrace{\sum_{\substack{d \in \mathcal{E} \\ p \nmid d}} \frac{\varphi\left(\frac{N}{d}\right)}{\varphi\left(\frac{N}{(N, cd)}\right)} \mu\left(\frac{N}{(N, cd)}\right)}_{=:a_c^{p'}}. \end{aligned}$$

For $n \in \mathbb{N}$ and prime number p let $\nu_p(n) \geq 0$ the maximal p-part of n, i.e. $p^{\nu_p(n)} \mid n$ and $p^{\nu_p(n)+1} \nmid n$. Let $k = \nu_p(N)$. If $\nu_p(c) \leq k - 2$, i.e. in particular it is $k \geq 2$, then $\nu_p(N/(cd, N)) \geq 2$ for $d \in \mathcal{E}$, $p \nmid d$. Thus, we have $\mu(N/(cd, N)) = 0$ and $a_c^p = a_c$ in the

case $pc \mid (N/p)$. For $\nu_p(c) = k - 1$ we have

$$a_c^{p'} = \sum_{\substack{d \in \mathcal{E} \\ p \nmid d}} \frac{\varphi\left(\frac{N}{d}\right)}{\varphi\left(\frac{N}{(N,cd)}\right)} \mu\left(\frac{N}{(N,cd)}\right)$$

$$= \sum_{\substack{d \in \mathcal{E} \\ p \nmid d}} \frac{\varphi(p^k)\varphi\left(\frac{N/p^k}{d}\right)}{\varphi(p)\varphi\left(\frac{N/p^k}{(N/p^k, dc/p^{k-1})}\right)} \underbrace{\mu(p)}_{=-1} \mu\left(\frac{N/p^k}{(N/p^k, dc/p^{k-1})}\right)$$

$$= -p^{k-1} \underbrace{\sum_{\substack{d \in \mathcal{E} \\ p \nmid d}} \frac{\varphi\left(\frac{N/p^k}{d}\right)}{\varphi\left(\frac{N/p^k}{(N/p^k, dc/p^{k-1})}\right)} \mu\left(\frac{N/p^k}{(N/p^k, dc/p^{k-1})}\right)}_{=:X(c)}.$$

Assume now $\nu_p(c) = \nu_p(N) = k$. We write $N' = N/p^k$ and $c' = c/p^k$, then we get

$$a_c = \sum_{d \in \mathcal{E}} \frac{\varphi\left(\frac{N'p^k}{d}\right)}{\varphi\left(\frac{N'p^k}{(N'p^k, c'p^k d)}\right)} \mu\left(\frac{N'p^k}{(N'p^k, c'p^k d)}\right)$$

$$= \sum_{\substack{d \in \mathcal{E} \\ p \nmid d}} \frac{\varphi(p^k)\varphi\left(\frac{N'}{d}\right)}{\varphi\left(\frac{N'}{(N',c'd)}\right)} \mu\left(\frac{N'}{(N',c'd)}\right) + \underbrace{\sum_{\substack{d \in \mathcal{E} \\ p \mid d}} \frac{\varphi\left(\frac{N'}{d}\right)}{\varphi\left(\frac{N'}{(N',c'd)}\right)} \mu\left(\frac{N'}{(N',c'd)}\right)}_{=a_{(c'p^{k-1})}^p}$$

$$= (p-1)p^{k-1}X(c) + a_{(c'p^{k-1})}^p.$$

We combine the two expressions for a_c, $c = c'p^k$. Then, $c/p = c'p^{k-1} \mid N/p$ and $X(c'p^{k-1}) = X(c'p^k) = X(c)$. Since $xa_{(c'p^{k-1})} + ya_{(c'p^k)} \geq 0$ for $x, y \geq 0$ we get from

$$xa_{(c'p^{k-1})} + ya_{(c'p^k)} = x\left(a_{(c'p^{k-1})}^p - p^{k-1}X(c)\right) + y\left((p-1)p^{k-1}X(c) + a_{(c'p^{k-1})}^p\right)$$

$$= pa_{(c'p^{k-1})}^p, \qquad\qquad (x = p-1, \ y = 1)$$

and this proves the lemma. ∎

We now conclude by induction that $\mathcal{E}$ is a filter if all possible reductions $\mathcal{E}_p$, $p \mid N$, are filters. Under this assumption, it follows that no $\mathcal{E}_p$ is empty: Let $p \mid N$ such that $p \mid d$ for some $d \in \mathcal{E}$, then $\mathcal{E}_p$ is not empty, hence equals (e_p) for some e_p. Since $\mathcal{E}_p$ is a filter, we have $N/p \in \mathcal{E}_p$, and hence $N = p \cdot N/p \in \mathcal{E}$. As induction step, we use the following lemma.

Lemma 3.9. *Let $\mathcal{E} \subset \mathcal{D}(N)$ and for all $p \mid N$ the set $\mathcal{E}_p$, defined as in Definition 3.7, a filter, namely $(e_p) = (e_p)_{N/p}$ for some $e_p \mid N/p$. Then either there exist a prime $p \mid N$ with $p \mid e_q$ for all $p \neq q$ or it is $e_p = 1$ for all p.*
In the first case we have $\mathcal{E} = (pe_p)$ or $\mathcal{E} = (pe_p) \cup \{1\}$. In the second case we have $\mathcal{E} = (1) = \mathcal{D}(N)$ or $\mathcal{E} = (1) \setminus \{1\}$.

Proof. Assume, there exist q' with $e_{q'} \neq 1$ and $p \mid e_{q'}$. Then $p \mid e_q$ for all $q \neq p$. We prove this by contradiction, then if $p \nmid e_q$ for some q, then $q'e_q \in \mathcal{E}_q$ (since $\mathcal{E}_q$ is a filter) and

hence $qq'e_q \in \mathcal{E}$ (by definition of $\mathcal{E}_q$). Then $qe_q \in \mathcal{E}_{q'}$ and $e_{q'} \mid qe_q$, hence a contradiction to $p \nmid e_q$. This proves the first part of the lemma.

We now prove the consequences in the two cases. Firstly, we assume it exist p with $p \mid e_q$ for all $q \neq p$. Let $x \in (pe_p)$, then $e_p \mid x/p$, and since $\mathcal{E}_p$ is a filter, $x/p \in \mathcal{E}_p$. Thus we have $x = p \cdot x/p \in \mathcal{E}$, i.e. $(pe_p) \subset \mathcal{E}$. Let now $x \in \mathcal{E}$. If $p \mid x$ we have $x/p \in \mathcal{E}_p$, hence $e_p \mid x/p$ and therefore $pe_p \mid x$. If $p \nmid x$, then $x = 1$ or it exists q with $q \mid x$. In this case is $x/q \in \mathcal{E}_q$ and $e_q \mid x/q$, which is a contradiction to $p \nmid x$. This proves $(pe_p) = \mathcal{E} \setminus \{1\}$ (which may be equal to $\mathcal{E}$).
In the case $e_p = 1$ for all p, we have $(p) \subset \mathcal{E}$ for all p. Since it is $\bigcup_{p \in \mathcal{D}(N)} (p) = \mathcal{D}(N) \setminus \{1\}$, this proves the assertion. ∎

We can now conclude the proof of the claim of (3.1). Let $\mathcal{E}$ such that

$$a_c = \sum_{d \in \mathcal{E}} \frac{\varphi(N/d)}{\varphi(N/(cd, N))} \mu(N/(cd, N)) \geq 0$$

for all $c \in \mathcal{D}(N)$, then $a_c^p \geq 0$ for all $\mathcal{E}_p$ and $c \in \mathcal{D}(N/p)$ by Lemma 3.8. By induction, all $\mathcal{E}_p$ are filters, namely (e_p) for some $e_p \mid N/p$. Then, by Lemma 3.9, we have that $\mathcal{E}$ is a filter (e) for some $e \mid N$ or $(e) \cup \{1\}$ for some $e \neq 1$ or $(1) \setminus \{1\}$. By Lemma 3.6, the last cases are only possible for $N = p^n$ and $e = p$. In this cases $\mathcal{E}$ is a filter as well. This proves the claim (3.1) and hence concludes the proof of Theorem 3.1.

4. Fourier pairs of $\{0, 1\}$-matrices

In the following, we consider idempotents ε/N of the group algebra $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$, i.e.

$$\varepsilon/N \cdot \varepsilon/N = \varepsilon/N. \tag{4.1}$$

If we introduce a basis $\{g^i \otimes g^j \mid 0 \leq i, j < N\}$, with $\langle g \rangle = \mathbb{Z}_N$, and write $\varepsilon = \sum_{i,j} \varepsilon_{ij} g^i \otimes g^j$, equation (4.1) translates to

$$\frac{1}{N^2} \sum_{i',i''} \sum_{j',j''} \varepsilon_{i'j'} \varepsilon_{i''j''} (g^{i'} \otimes g^{j'})(g^{i''} \otimes g^{j''}) = \frac{1}{N} \sum_{i,j} \varepsilon_{ij} g^i \otimes g^j,$$

and by comparing coefficients, we get

$$\frac{1}{N^2} \sum_{i'+i''=i} \sum_{j'+j''=j} \varepsilon_{i'j'} \varepsilon_{i''j''} = \frac{1}{N} \varepsilon_{ij}. \tag{4.2}$$

Let $\xi = \xi_N$ be a primitive N-th root of unity and $\{e_k = 1/N \sum_{r=0}^N \xi^{kr} g^r \mid 0 \leq k < N\}$ be the set of primitive idempotents of the group algebra $\mathbb{C}[\mathbb{Z}_N]$. Then $\{e_k \otimes e_l\}$ is the set of primitive idempotents of $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$ and we can express ε/N as sum of these primitive idempotents: $\varepsilon/N = \sum_{k,l} \bar{\varepsilon}_{kl} e_k \otimes e_l$ with $\bar{\varepsilon}_{kl} \in \{0, 1\}$ for all $0 \leq k, l < N$. This leads to

$$\varepsilon_{ij} = \frac{1}{N} \sum_{k,l} \bar{\varepsilon}_{kl} \xi^{ik+jl}, \tag{4.3}$$

which means, that the matrix $\varepsilon = (\varepsilon_{ij})_{ij}$ is the discrete Fourier transformation of the $\{0, 1\}$-matrix $\bar{\varepsilon}$. This considerations lead to the following problem.

Problem 4.1. We wish to determine all idempotents ε/N of $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$, such that $\varepsilon = (\varepsilon_{ij})_{ij}$ is $\{0, 1\}$-matrix, or equivalent, all Fourier pairs of $\{0, 1\}$-matrices ε and $\bar{\varepsilon}$.

Example 4.2. We consider some examples of Fourier transformed matrices, where ε is not necessarily a $\{0,1\}$-matrix.

(i) Let $\bar{\varepsilon}$ the matrix with $\bar{\varepsilon}_{00} = 1$ and $\bar{\varepsilon}_{kl} = 0$ otherwise. Then $\varepsilon_{ij} = 1/N$ for all j, j.

(ii) Let $\bar{\varepsilon}$ the matrix with $\bar{\varepsilon}_{0l} = 1$ for all l and $\bar{\varepsilon}_{kl} = 0$ otherwise. Then $\varepsilon_{i0} = 1$ for all i and $\varepsilon_{ij} = 0$ otherwise.

(iii) Let $\bar{\varepsilon}$ the matrix with $\bar{\varepsilon}_{kk} = 1$ for all k and $\bar{\varepsilon}_{kl} = 0$ otherwise. Then $\varepsilon_{ij} = 1$ for all i, j with $i + j \equiv 0 \mod N$ and $\varepsilon_{ij} = 0$ otherwise. We give the matrices explicitly for $N = 4$:

$$\bar{\varepsilon} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \varepsilon = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

The following theorem completely solves this problem, relying heavily on our main Theorem 3.1:

Theorem 4.3. *All idempotents ε/N of the group algebra $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$ with $\varepsilon_{ij} \in \{0,1\}$, or equivalently all discrete Fourier pairs $\varepsilon, \bar{\varepsilon}$ of $\{0,1\}$-matrices are either*

$$\varepsilon_{ij} = \delta_{(\frac{N}{d}|i)}\delta_{(d|j-t\frac{i}{N/d})}, \tag{4.4}$$

for a unique $d \mid N$ and $0 \le t \le d - 1$ or they are trivial $\varepsilon = \bar{\varepsilon} = 0$.

Before we proceed to the proof of the theorem, we give another Example.

Example 4.4. Let $N = 12$, $d = 3$ and $t = 2$, then ε as in (4.4) is given by

$$
\begin{array}{c}
 \\
0 \\
 \\
 \\
N/d \\
 \\
 \\
\bar{d} \\
 \\
 \\
 \\
 \\

\end{array}
\begin{array}{ccc}
0 & t & d \\
\end{array}
\left(\begin{array}{cccccccccccc}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & . & . & . & . & . & . & . & . \\
\end{array}\right).
$$

Proof. By the Fourier transformation (4.3), we have $\varepsilon_{00} = \frac{1}{N}\sum_{k,l}\bar{\varepsilon}$. Since ε and $\bar{\varepsilon}$ are $\{0,1\}$-matrices, this gives either $\bar{\varepsilon}_{kl} = 0$ for all k, l or $\sum_{k,l}\bar{\varepsilon}_{kl} = N$. In the first case we have $\varepsilon = 0$ as well. Applying the same argument to the dual Fourier transformation,

$$\bar{\varepsilon}_{kl} = 1/N \sum_{ij} \varepsilon_{ij}\xi^{-(ik+jl)}, \tag{4.5}$$

we get $\sum_{i,j}\varepsilon_{ij} = N$ in the second case.

Assume in the following $\varepsilon \neq 0$. We now calculate the row-, resp. column-sums of the matrices ε and $\bar{\varepsilon}$. Let a_k the k-th row sum of ε and a'_l the l-th column-sum for ε, and $\bar{a}_k$,

$\bar{a}'_l$ the according sums of $\bar{\varepsilon}$. Then

$$a_k = \sum_j \varepsilon_{kj} = \frac{1}{N} \sum_{l,i,j} \bar{\varepsilon}_{ij} \xi^{ik+jl} = \frac{1}{N} \sum_i \xi^{ik} \sum_j \bar{\varepsilon}_{ij} \underbrace{\sum_l \xi^{jl}}_{=N\delta_{(j=0)}} = \sum_i \xi^{ik} \bar{\varepsilon}_{i0} \qquad (4.6)$$

Since the row sum a_k is a non-negative integer, we get by Theorem 3.1, that $\{i \mid \bar{\varepsilon}_{i0} = 1\}$ is a subgroup of $\mathbb{Z}_N$, thus it exist $d \mid N$ with $\bar{\varepsilon}_{i0} = \delta_{(d|i)}$. Analogously, we get by calculating the column sum a'_l that $d' \mid N$ exist, such that $\bar{\varepsilon}_{0j} = \delta_{(d'|j)}$. As a consequence, we get $a_k = N/d$ for k being an N/d-multiple and $a'_l = N/d'$ for l being an N/d'-multiple, and the other row, resp. column sums being 0. We now calculate the row and column sums of $\bar{\varepsilon}$ using the dual transformation (4.5). This gives, again by application of Theorem 3.1, that there exist $\bar{d}, \bar{d}' \mid N$ such that $\varepsilon_{i0} = \delta_{(\bar{d}|i)}$ and $\varepsilon_{0j} = \delta_{(\bar{d}'|j)}$, and $\bar{a}_k = N/\bar{d}$ for k being $N/\bar{d}$-multiple and $\bar{a}_l = N/\bar{d}'$ for l being $N/\bar{d}'$-multiple. Since $N/d = a_0 = \sum_j \varepsilon_{0j} = N/\bar{d}'$, we get $d = \bar{d}'$. Analogously, we get $\bar{d} = d'$. Since only the N/d-th rows have entries 1 and $\varepsilon_{i0} = \delta_{(\bar{d}|i)}$, we get $N/d \mid \bar{d} = d'$, hence $N \mid dd'$.

The case $N = dd'$, i.e. $d' = N/d$ corresponds to the non-shifted solution of (4.2), since in this case there maximal $N/d \cdot N/d' = N$ entries 1.

We consider now a solution with $N < dd'$ and show, that a suitably shifted version of this is also a solution of (4.2) with smaller dd'. The claim then follows by induction over dd'. For a solution ε of (4.2) the shifted matrix, defined by

$$\varepsilon_{ij}^{[t]} := \begin{cases} \varepsilon_{i,j-t\frac{i}{N/d}}, & N/d \mid i, \\ \varepsilon_{i,j} = 0, & \text{otherwise.} \end{cases}$$

for some $0 \le t \le d-1$, is also a solution of (4.2). This follows easily by inserting $\varepsilon_{ij}^{[t]}$ in (4.2), since the shift gives only a new ordering of the summands. Let now ε be a solution with $dd' > N$. We now want to shift this ε in a way, that no 1 entries in the first column are moved, i.e. the d'-th rows are shifted by multiple of d, and some of the other rows are shifted, such that $\varepsilon^{[t]}$ has at least one 1-entry more in the first column, than ε:

Consider the N/d-row. By hypothesis, $N/d < d'$, hence $\varepsilon_{N/d,0} = 0$, but $\varepsilon_{N/d,t} = 1$ for some t, since the row sum $a_{N/d} = N/d > 0$. Since the column sum $a'_t \ne 0$, we have $N/d' \mid t$, hence $d \mid t \cdot dd'/N$. Thus the shifted solution $\varepsilon_{ij}^{[-t]}$ has in the 0-column still $\varepsilon_{i0} = 1$ for $d' \mid i$ and it has now additionally $\varepsilon_{N/d,0} = 1$. The expression dd' for $\varepsilon^{[t]}$ has to be strictly smaller than dd' for ε, this reduces the claim by induction to the unshifted case $dd' = N$, which has been solved above. ∎

5. A SYSTEM OF EQUATIONS AND R-MATRICES OF QUANTUM GROUPS

The following system of equations for an abelian group G arises as a necessary condition on the the element $R_0 \in \mathbb{C}[\Lambda \times \Lambda]$ in Lusztig's ansatz for R-matrices for a quantum group $U_q(\mathfrak{g})$ with coradical $\mathbb{C}[\Lambda]$. In this application, the abelian group G will be the fundamental group of $\mathfrak{g}$, and hence cyclic except for $\mathfrak{g} = D_{2n}$. We will not discuss this matter further, but refer the reader to our respective paper [LN14]. Note Remark 5.4.

Definition 5.1. For an abelian group G we define a set of $2|G|^2 + 2$ quadratic equations in $|G|^2$ formal complex variables $g(x,y)$ indexed by $x, y \in G$:

$$g(x,y) = \sum_{y_1+y_2=y} g(x,y_1)g(x,y_2), \tag{5.1}$$

$$g(x,y) = \sum_{x_1+x_2=x} g(x_1,y)g(x_2,y), \tag{5.2}$$

$$1 = \sum_{y \in G} g(0,y), \tag{5.3}$$

$$1 = \sum_{x \in G} g(x,0). \tag{5.4}$$

As a side remark, note that these equations are a subset of the equations for a Hopf pairing $g : \mathbb{C}^G \otimes \mathbb{C}^G \to \mathbb{C}$, but it allows for significantly more solutions containing 0's, as the next theorem shows. The result of this article is in some sense, that g is still a pairing on a pair of subgroups.

Theorem 5.2. *Let G be an abelian group and H_1, H_2 subgroups with equal cardinality $|H_1| = |H_2| = d$ (not necessarily isomorphic!). Let $\omega\colon H_1 \times H_2 \to \mathbb{C}^\times$ be a pairing of groups. Here, the group G is written additively and $\mathbb{C}^\times$ multiplicatively, thus we have $\omega(x,y)^d = 1$ for all $x \in H_1, y \in H_2$. Then the assignment*

$$g\colon G \times G \to \mathbb{C}, \ (x,y) \mapsto \frac{1}{d}\,\omega(x,y)\delta_{(x\in H_1)}\delta_{(y\in H_2)} \tag{5.5}$$

is a solution of the equations (5.1)-(5.4) *for G.*

Proof. The claim follows by straightforward calculations:

$$\sum_{y_1+y_2=y} g(x,y_1)g(x,y_2) = \left(\frac{1}{d}\right)^2 \sum_{y_1+y_2=y} \omega(x,y_1)\omega(x,y_2)\delta_{(x\in H_1)}\delta_{(y_1\in H_2)}\delta_{(y_2\in H_2)}$$

$$= \left(\frac{1}{d}\right)^2 \sum_{y_1+y_2=y} \omega(x,y_1+y_2)\delta_{(x\in H_1)}\delta_{(y_1\in H_2)}\delta_{(y_2\in H_2)}$$

$$= \left(\frac{1}{d}\right)^2 |H_2|\,\omega(x,y)\delta_{(x\in H_1)}\delta_{(y\in H_2)} = g(x,y).$$

$$\sum_{y\in G} g(0,y) = \frac{1}{d}\sum_{y\in G} \omega(0,y)\delta_{(y\in H_2)} = \frac{1}{d}\sum_{y\in H_2} 1 = 1.$$

∎

Question 5.3. Are these all solutions of the equations (5.1)-(5.4)?

As an application of the theorems proved in this paper we will below positively answer this question for a **cyclic group** G. We would actually hope to completely resolve the question with the combinatorial results of this article.

Remark 5.4. For the application in quantum groups, the only non-cyclic case of interest is $\mathbb{Z}_2 \times \mathbb{Z}_2$ (the fundamental group of the Lie algebra $\mathfrak{g} = D_{2n}$), which can be checked explicitly to hold as well. Most other Lie algebras have $G = \mathbb{Z}_1, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4$

It is quite remarkable that the only highly nontrivial case solved with this articles result is hence the Lie algebra A_n with $G = \mathbb{Z}_{n+1}$, which depends highly on the prime divisors of $n+1$. This is due to the **unusually large center** $\mathbb{Z}_{n+1}$ of the algebraic group SL_{n+1}, which makes it notoriously hard to deal with (e.g. in Deligne-Lusztig theory). We hope that the technical tools developed in this article might be useful in addressing such issues.

Example 5.5. Let $G = \mathbb{Z}_N$ and consider for any divisor $d|N$ the unique subgroup $H = \frac{N}{d}\mathbb{Z}_N \cong \mathbb{Z}_d$ of G of order d. By Theorem 5.2 we have for any pairing $\omega\colon H \times H \to \mathbb{C}^\times$ the function g as in (5.5) as a solution of the equations (5.1)-(5.4).
We give the solution explicitly: For $H = \langle h \rangle$, $h \in \frac{n}{d}\mathbb{Z}_n$, we define a pairing $\omega\colon H \times H \to \mathbb{C}^\times$ by $\omega(h,h) = \xi$ with ξ a d-th root of unity, not necessarily primitive.
Thus the general solution ansatz in Lemma 5.2 translates for cyclic groups G to

$$g\colon G \times G, \ (x,y) \mapsto \frac{1}{d}\xi^{\frac{xy}{(N/d)^2}}\delta_{(\frac{N}{d}|x)}\delta_{(\frac{N}{d}|y)}. \tag{5.6}$$

Theorem 5.6. *For $G = \mathbb{Z}_N$ the solutions given in Lemma 5.2 (and worked out in this case in example 5.5), are in fact all solutions to the system of equations (5.1)-(5.4).*

Proof. (a) The proof is an application of Theorem 4.3, which follows from the main Theorem 3.1. Let $g : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{C}$ be a solution of the equations (5.1)-(5.4). We write shortly g_{ij} for $g(i,j)$, $0 \le i,j \le N-1$. Let $\mathbb{Z}_N = \langle g \rangle$, then

$$\sum_{j',j''}(g_{ij'}x^{j'})(g_{ij''}x^{j''}) = \sum_j g_{ij}x^i$$

for all i by (5.1), hence $\sum_j g_{ij}x^i$ is an idempotent in $\mathbb{C}[\mathbb{Z}_N]$. Let $\xi = \xi_N$ be a primitive N-th root of unity, then primitive idempotents of $\mathbb{C}[\mathbb{Z}_N]$ are all of the form $e_k = \frac{1}{N}\sum_{r=0}^{N-1}\xi^{kr}x^r$. Thus, we have $\sum_j g_{ij}x^i = \sum_k \varepsilon_{ik}e_k$ for $\varepsilon_{ik} \in \{0,1\}$ for all i, and therefore

$$g_{ij} = \frac{1}{N}\sum_{k=1}^{N-1}\varepsilon_{ik}\xi^{jk}$$

for $\{0,1\}$-matrix $\varepsilon = (\varepsilon_{ik})$. By inserting this in (5.2), $\sum_{i'+i''=i}g_{i'j}g_{i''j} = g_{ij}$, we get

$$\frac{1}{N^2}\sum_{i'+i''=i}\sum_{k',k''}\varepsilon_{i'k'}\varepsilon_{i''k''}\xi^{(k'+k'')j} = \frac{1}{N}\sum_k \varepsilon_{ik}\xi^{kj}.$$

By comparing the coefficients on both sides we get

$$\frac{1}{N^2}\sum_{i'+i''=i}\sum_{k'+k''=k}\varepsilon_{i'k'}\varepsilon_{i''k''} = \frac{1}{N}\varepsilon_{ik}, \tag{5.7}$$

which is equation (4.2). Thus, ε/N is an idempotent in $\mathbb{C}[\mathbb{Z}_N \times \mathbb{Z}_N]$ and ε is $\{0,1\}$-matrix and we can apply Theorem 4.3. We have

$$\varepsilon_{ij} = \begin{cases} \delta_{(\frac{N}{d}|i)}\delta_{(d|j-t\frac{i}{N/d})}, & \text{if } N/d \mid i, \\ 0, & \text{otherwise,} \end{cases}$$

for some $d \mid N$ and $0 \leq t \leq d - 1$. We insert in (a):

$$g_{ij} = \frac{1}{N} \sum_{k=0}^{N-1} \delta_{(\frac{N}{d}|i)} \delta_{(d|k-t\frac{i}{N/d})} \xi^{jk}$$

$$= \frac{1}{N} \delta_{(\frac{N}{d}|i)} \sum_{k'=0}^{N/d-1} \xi^{j(t\frac{i}{N/d}+dk')} \qquad (k = t\frac{i}{N/d} + dk', \ k' = 0, \ldots, d-1)$$

$$= \frac{1}{d} \left(\xi^{N/d} \right)^{t\frac{i}{N/d}\frac{j}{N/d}} \delta_{(\frac{N}{d}|i)} \underbrace{\frac{1}{N/d} \sum_{k'=0}^{N/d-1} (\xi^d)^{jk'}}_{=\delta_{\frac{N}{d}|j}}$$

Thus, g is the solution given already in Example 5.5, which was the explicitly worked out case of Lemma 5.2 for G cyclic.

$\blacksquare$

References

[Bou66] N. Bourbaki, *General topology, part 1*, Hermann, Paris and Addison-Wesley (1966).

[LN14] S. Lentner, D. Nett: *New R-matrices for small quantum groups*, Preprint, `arXiv:1409.5824` (2014).

[Lus93] G. Lusztig, *Introduction to quantum groups*, Birkhäuser (1993).