Uncertainty Principles and Sum Complexes

Roy Meshulam[*]

March 28, 2014

Abstract

Let p be a prime and let A be a nonempty subset of the cyclic group C_p. For a field $\mathbb{F}$ and an element f in the group algebra $\mathbb{F}[C_p]$ let T_f be the endomorphism of $\mathbb{F}[C_p]$ given by $T_f(g) = fg$. The *uncertainty number* $u_{\mathbb{F}}(A)$ is the minimal rank of T_f over all nonzero $f \in \mathbb{F}[C_p]$ such that $\text{supp}(f) \subset A$.

The following topological characterization of uncertainty numbers is established. For $1 \leq k \leq p$ define the *sum complex* $X_{A,k}$ as the $(k-1)$-dimensional complex on the vertex set C_p with a full $(k-2)$-skeleton whose $(k-1)$-faces are all $\sigma \subset C_p$ such that $|\sigma| = k$ and $\prod_{x\in\sigma} x \in A$. It is shown that if $\mathbb{F}$ is algebraically closed then

$$u_{\mathbb{F}}(A) = p - \max\{k : \tilde{H}_{k-1}(X_{A,k}; \mathbb{F}) \neq 0\}.$$

The main ingredient in the proof is the determination of the homology groups of $X_{A,k}$ with field coefficients. In particular it is shown that if $|A| \leq k$ then $\tilde{H}_{k-1}(X_{A,k}; \mathbb{F}_p) = 0$.

1 Introduction

Uncertainty type inequalities reflect various quantitative aspects of the general principle that a nonzero function and its Fourier transform cannot both be sharply localized. The first such result is the Fourier theoretic version

[*]Department of Mathematics, Technion, Haifa 32000, Israel. e-mail: meshulam@math.technion.ac.il . Supported by an ISF grant.

of the Heisenberg quantum-mechanical uncertainty principle: If $f \in L^2(\mathbb{R})$ satisfies $||f||_2 = 1$ then

$$\|xf\|_2 \, \|\xi\widehat{f}\|_2 \geq \frac{1}{4\pi} \quad . \tag{1}$$

This classical inequality and its numerous extensions (see e.g. [3]) have major applications in diverse areas ranging from mathematical physics and differential equations to signal recovery and number theory. Here we are concerned with discrete versions of the uncertainty principle. Let G be a finite abelian group and let $\mathbb{F}[G]$ be the group algebra of G over the field $\mathbb{F}$. For an element $f \in \mathbb{F}[G]$ let $T_f : \mathbb{F}[G] \to \mathbb{F}[G]$ be given by $T_f g = fg$. Let A be a subset of G. Here and throughout the paper we assume that $A \neq \emptyset$. The *uncertainty number* of $A \subset G$ is defined by

$$u_{\mathbb{F}}(A) = \min\{\operatorname{rank} T_f \ : \ \emptyset \neq \operatorname{supp}(f) \subset A\}.$$

The motivation for this definition is as follows. Let m be the exponent of G and suppose $\mathbb{F}$ contains a primitive m-th root of unity. Let $\widehat{G}$ denote the group of $\mathbb{F}$-valued characters of G. Identifying $\mathbb{F}[G]$ with the space of $\mathbb{F}$-valued functions on G, the Fourier Transform of a function $f \in \mathbb{F}[G]$ is the function $\widehat{f} \in \mathbb{F}[\widehat{G}]$ given by $\widehat{f}(\chi) = \sum_{x \in G} \chi(x^{-1}) f(x)$. The characters $\chi \in \widehat{G}$ are eigenfunctions of T_f with eigenvalues $\widehat{f}(\chi)$, hence $\operatorname{rank} T_f = |\operatorname{supp}(\widehat{f})|$. Therefore in the semisimple case

$$u_{\mathbb{F}}(A) = \min\{|\operatorname{supp}(\widehat{f})| \ : \ \emptyset \neq \operatorname{supp}(f) \subset A\}.$$

The discrete counterpart of (1) (see e.g. [1]) asserts that for any $\mathbb{F}$ and $A \subset G$

$$u_{\mathbb{F}}(A) \geq \frac{|G|}{|A|}. \tag{2}$$

In the semisimple case (2) is equivalent to

$$|\operatorname{supp}(f)| \cdot |\operatorname{supp}(\widehat{f})| \geq |G|$$

for all nonzero f's. While (2) is sharp when A is a coset of G, it can often be improved for particular choices of G, A and $\mathbb{F}$. One such result (see [9]) states that if p is prime and A is a nonempty subset of the cyclic group C_p then $u_{\mathbb{C}}(A) = p - |A| + 1$. See [7] for an extension to general abelian groups.

For a finite abelian group G let Δ_G denote the $(|G|-1)$-dimensional simplex with vertex set G and let $\Delta_G^{(j)}$ be the j-dimensional skeleton of Δ_G.

Let $A \subset G$ and let $1 \leq k \leq |G|$. The *Sum Complex* $X_{A,k}$ was defined in [6] by

$$X_{A,k} = \Delta_G^{(k-2)} \ \cup \ \{\sigma \subset G \ : \ |\sigma| = k \ , \ \prod_{x \in \sigma} x \in A\}.$$

Here we obtain the following topological characterization of uncertainty numbers of subsets of C_p.

Theorem 1.1. *Let $A \subset C_p = G$. If $\mathbb{F}$ is algebraically closed then*

$$u_{\mathbb{F}}(A) = p - \max\{1 \leq k \leq p : \tilde{H}_{k-1}(X_{A,k};\mathbb{F}) \neq 0\}. \qquad (3)$$

If $\tilde{H}_{k-1}(X_{A,k};\mathbb{F}) = 0$ for all $1 \leq k \leq p$ then the right-hand side of (3) is defined as p.

Example: Let $p = 7$ and $A = \{1, z, z^3\} \subset C_7 = \langle z \rangle$. The sum complex $X_{A,3}$ is depicted in Figure 1b) where vertex label α corresponds to the element z^α. Note that $X_{A,3}$ is obtained from a 7-point triangulation of the real projective plane $\mathbb{RP}^2$ (Figure 1a) by adding the faces $\{z^2, z^3, z^5\}$, $\{1, z^2, z^6\}$ and $\{z, z^2, z^4\}$. $X_{A,3}$ is clearly homotopy equivalent to $\mathbb{RP}^2$, hence $H_2(X_{A,3};\mathbb{F}_2) \neq 0$. Theorem 1.1 then implies that $u_{\overline{\mathbb{F}_2}}(A) \leq 4$. Together with the easy fact that $u_{\mathbb{F}}(B) \geq p - \max B$ for any $\mathbb{F}$ and $B \subset C_p$ it follows that $u_{\overline{\mathbb{F}_2}}(A) = 4$. It can be checked that in fact $u_{\mathbb{F}_2}(A) = 4$.

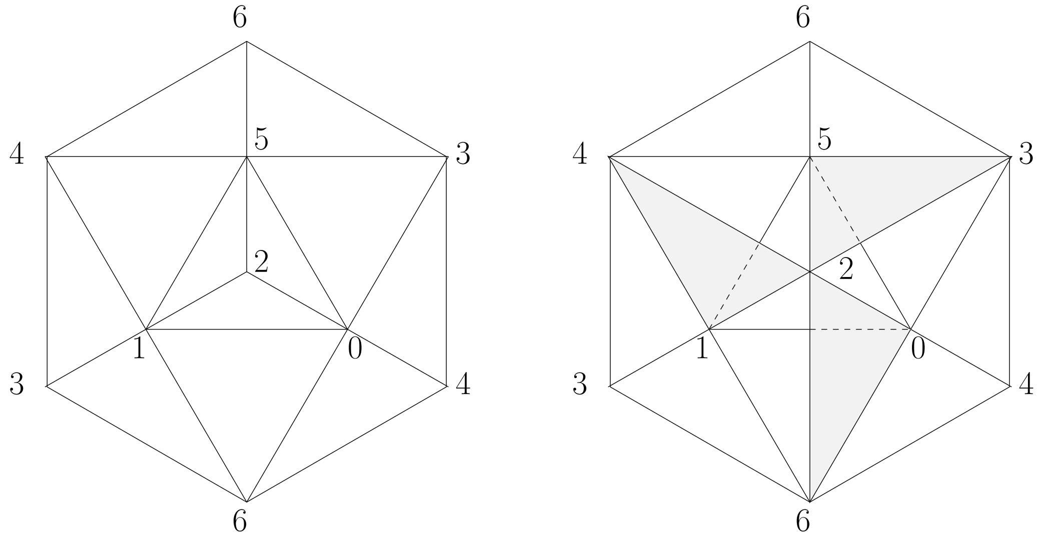
Let z be a fixed generator of C_p and let $A = \{a_1, \ldots, a_m\} \subset C_p$ where $a_i = z^{\alpha_i}$ and α_i is an element of the prime field $\mathbb{F}_p = \{0, \ldots, p-1\}$. Let $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_p^m$. The main ingredient in the proof of Theorem 1.1 is the computation of the homology of $X_{A,k}$ with arbitrary field coefficients. Let $\mathbb{F}$ be a field of characteristic ℓ. First suppose that $\ell \neq p$ and let ω be a primitive p-th root of unity in the algebraic closure $\overline{\mathbb{F}}$. For $\beta = (\beta_1, \ldots, \beta_k) \in \mathbb{F}_p^k$ let $M_{\beta,\alpha}$ be the $k \times m$ matrix given by $M_{\beta,\alpha}(i,j) = \omega^{\beta_i \alpha_j}$. Let

$$\mathcal{B}_k = \{\beta_1, \ldots, \beta_k) : 0 \leq \beta_1 < \cdots < \beta_k \leq p-1\}.$$

The case $m = k$ of the following result is implicit in [6].

Theorem 1.2. *Let $A = \{z^{\alpha_1}, \ldots, z^{\alpha_m}\} \subset C_p$ and let $\alpha = (\alpha_1, \ldots, \alpha_m)$. If* $\operatorname{char} \mathbb{F} \neq p$ *then for* $1 \leq k \leq p$

$$\dim \tilde{H}_{k-1}(X_{A,k};\mathbb{F}) = \frac{m}{k}\binom{p-1}{k-1} - \frac{1}{p}\sum_{\beta \in \mathcal{B}_k} \operatorname{rank} M_{\beta,\alpha}. \qquad (4)$$



(a) A 7-point triangulation of $\mathbb{RP}^2$

(b) $X_{A,3}$ for $A = \{1, z, z^3\} \subset C_7$

Figure 1

Our main result concerns the homology of $X_{A,k}$ with $\mathbb{F}_p$ coefficients.

Theorem 1.3. *Let $A \subset C_p$ such that $|A| = m$. Then for $1 \le k \le p$*

$$\dim \tilde{H}_{k-1}(X_{A,k}; \mathbb{F}_p) = \begin{cases} 0 & \text{if } \ m \le k \\ (\frac{m}{k} - 1)\binom{p-1}{k-1} & \text{if } \ m > k. \end{cases} \tag{5}$$

Remarks:
1) The case $k = p$ of both Theorems 1.2 and 1.3 is straightforward. On one hand, since $X_{A,p}$ is a subcomplex of the $(p-1)$-simplex it follows that $\tilde{H}_{p-1}(X_{A,p}; \mathbb{F}) = 0$ for any A and $\mathbb{F}$. On the other hand, let $\beta = (0, 1, \ldots, p-1)$ be the unique element of $\mathcal{B}_p$. Then $M_{\beta,\alpha}$ consists of m full columns of the Fourier matrix and thus has full rank m. Hence the right hand side of (4) is also zero. In the sequel we will therefore assume that $1 \le k < p$.
2) The argument given in [6] for the case $m = k$ of Theorem 1.2 does not extend to the modular case. The approach here is different and is also utilized in the proof of our main result Theorem 1.3.
3) The f-vector of $X_{A,k}$ satisfies $f_i(X_{A,k}) = \binom{p}{i+1}$ for $0 \le i \le k-2$ and $f_{k-1}(X_{A,k}) = \frac{m}{p}\binom{p}{k} = \frac{m}{k}\binom{p-1}{k-1}$. The reduced Euler characteristic of $X_{A,k}$ is

therefore

$$\begin{aligned}\tilde{\chi}(X_{A,k}) &= -1+\sum_{i=0}^{k-2}(-1)^i\binom{p}{i+1}+(-1)^{k-1}\frac{m}{p}\binom{p}{k} \\ &= (-1)^{k-1}(\frac{m}{k}-1)\binom{p-1}{k-1}.\end{aligned} \tag{6}$$

Since $\tilde{H}_i(X_{A,k};\mathbb{F}_p)=0$ for $0\leq i<k-2$ it follows that

$$\begin{aligned}\dim\tilde{H}_{k-2}(X_{A,k};\mathbb{F}_p) &= \dim\tilde{H}_{k-1}(X_{A,k};\mathbb{F}_p)-(\frac{m}{k}-1)\binom{p-1}{k-1} \\ &= \left\{\begin{array}{cc} (1-\frac{m}{k})\binom{p-1}{k-1} & \text{if} \;\; m\leq k \\ 0 & \text{if} \;\; m>k. \end{array}\right.\end{aligned} \tag{7}$$

4) A classical result of Chebotarëv (see e.g. [8]) asserts that for $\mathbb{F}=\mathbb{Q}$ all $M_{\beta,\alpha}$'s have full rank. Theorem 1.2 therefore implies that (5) and (7) remain true for $\tilde{H}_*(X_{A,k};\mathbb{Q})$.
5) Theorem 1.3 does not hold for all fields $\mathbb{F}$ and in fact $\tilde{H}_{k-1}(X_{A,k};\mathbb{F})$ may be nontrivial even if $k>|A|=m$. For example, using Theorem 1.2 it can be shown that if $A=\{1,z^3,z^4,z^5,z^8\}\subset C_{17}$ then $\tilde{H}_7(X_{A,8};\mathbb{F}_2)\neq 0$.

The paper is organized as follows. In Section 2 we consider $X_{A,k}$ where A is a subset of an arbitrary abelian group G and identify $\tilde{H}_{k-1}(X_{A,k};\mathbb{F})$ with a certain subspace $\mathcal{H}(A)$ of skew-symmetric elements of the group algebra $\mathbb{F}[G^k]$. In Section 3 we use this characterization in the special case $G=C_p$ to prove Theorem 1.2. The proof of Theorem 1.3 given in Section 4 is more involved and depends additionally on some properties of generalized Vandermonde determinants over the group algebra $\mathbb{F}_p[C_p^k]$. Theorem 1.1 is derived in Section 5 as a direct consequence of Theorems 1.2 and 1.3. We conclude in Section 6 with some comments and open problems.

2 A Characterization of Cycles

Let A be a nonempty subset of a finite abelian group G and let $\mathbb{F}$ be a field. In this section we provide a characterization (Claim 2.1) of the homology group $\tilde{H}_{k-1}(X_{A,k};\mathbb{F})$ in terms of the group algebra $F[G^k]$. A simplified version valid under the assumption $gcd(|G|,k)=1$ is given in Claim 2.2.

We first introduce some terminology. Fix $1 \leq k \leq |G|$. For an element $g \in G$ and $1 \leq i \leq k$ let $e_i(g) = (1, \ldots, 1, g, 1, \ldots, 1) \in G^k$ with g appearing in the i-th coordinate. An element

$$s = \sum_{(g_1,\ldots,g_k)\in G^k} s(g_1, \ldots, g_k)(g_1, \ldots, g_k) \in \mathbb{F}[G^k]$$

is *skew-symmetric* if $s(g_{\sigma^{-1}(1)}, \ldots, g_{\sigma^{-1}(k)}) = \mathrm{sgn}(\sigma)s(g_1, \ldots, g_k)$ for all $(g_1, \ldots, g_k) \in G^k$ and σ in the symmetric group S_k. If $\mathrm{char}\,\mathbb{F} = 2$ then s is additionally required to satisfy $s(g_1, \ldots, g_k) = 0$ if $g_i = g_j$ for some $i \neq j$. Let $\mathcal{S}$ denote the space of skew-symmetric elements of $\mathbb{F}[G^k]$. For $h \in G$ let $W_h = \{(g_1, \ldots, g_k) \in G^k : \prod_{i=1}^{k} g_i = h\}$ and let $\mathcal{S}_h = \{s \in \mathcal{S} : \mathrm{supp}(s) \subset W_h\}$. Let ρ_h denote the projection from $\mathcal{S}$ onto $\mathcal{S}_h$ given by $\rho_h(\sum_{u\in G^k} s(u)u) = \sum_{u\in W_h} s(u)u$.

Let Y be a $(k-1)$-dimensional simplicial complex on the vertex set V and let $Y(\ell)$ denote the set of its (unordered) ℓ-simplices. Let $C_{k-1}(Y;\mathbb{F})$ denote the space of $\mathbb{F}$-valued $(k-1)$-chains of Y. Recall that $\phi \in C_{k-1}(Y;\mathbb{F})$ is a skew symmetric $\mathbb{F}$-valued function on the ordered $(k-1)$-simplices of Y. A $(k-1)$-chain $\phi \in C_{k-1}(Y;\mathbb{F})$ is a reduced $(k-1)$-cycle if for all $\{v_1, \ldots, v_{k-1}\} \in Y(k-2)$ it holds that

$$\sum_{\{v_k\in V:\{v_1,\ldots,v_{k-1},v_k\}\in Y(k-1)\}} \phi(v_1, \ldots, v_{k-1}, v_k) = 0. \tag{8}$$

Specializing to the case $Y = X_{A,k}$ it is clear that

$$C_{k-1}(X_{A,k}, \mathbb{F}) = \{s \in \mathcal{S} : \mathrm{supp}(s) \subset \cup_{a\in A} W_a\} = \bigoplus_{a\in A} \mathcal{S}_a.$$

By (8), $s \in C_{k-1}(X_{A,k}, \mathbb{F})$ is a reduced $(k-1)$-cycle of $X_{A,k}$ if for all $(g_1, \ldots, g_{k-1}) \in G^{k-1}$

$$\sum_{a\in A} s(g_1, \ldots, g_{k-1}, a \prod_{j=1}^{k-1} g_j^{-1}) = 0. \tag{9}$$

Let

$$\mathcal{H}(A) = \{s \in \bigoplus_{a\in A} \mathcal{S}_a \;:\; \sum_{a\in A} e_i(a^{-1})\rho_a(s) = 0 \text{ for all } 1 \leq i \leq k\}.$$

The homology space $\tilde{H}_{k-1}(X_{A,k};\mathbb{F})$ is characterized by the following

Claim 2.1.

$$\tilde{H}_{k-1}(X_{A,k};\mathbb{F}) = \mathcal{H}(A).$$

Proof: First note that by skew symmetry

$$\mathcal{H}(A) = \{s \in \bigoplus_{a\in A} \mathcal{S}_a \ : \ \sum_{a\in A} e_k(a^{-1})\rho_a(s) = 0\}. \tag{10}$$

Now let $s \in C_{k-1}(X_{A,k};\mathbb{F}) = \bigoplus_{a\in A} \mathcal{S}_a$. Then

$$\begin{aligned}
&\sum_{a\in A} e_k(a^{-1})\rho_a(s) \\
&= \sum_{a\in A} e_k(a^{-1}) \sum_{(g_1,\ldots,g_{k-1})\in G^{k-1}} s(g_1,\ldots,g_{k-1},a\prod_{j=1}^{k-1} g_j^{-1})(g_1,\ldots,g_{k-1},a\prod_{j=1}^{k-1} g_j^{-1}) \\
&= \sum_{(g_1,\ldots,g_{k-1})\in G^{k-1}} \left(\sum_{a\in A} s(g_1,\ldots,g_{k-1},a\prod_{j=1}^{k-1} g_j^{-1})\right)(g_1,\ldots,g_{k-1},\prod_{j=1}^{k-1} g_j^{-1}).
\end{aligned}$$

Therefore $\sum_{a\in A} e_k(a^{-1})\rho_a(s) = 0$ iff

$$\sum_{a\in A} s(g_1,\ldots,g_{k-1},a\prod_{j=1}^{k-1} g_j^{-1}) = 0 \tag{11}$$

for all $(g_1,\ldots,g_{k-1}) \in G^{k-1}$. Hence the Claim follows from (9) and (10).

□

Let $\mathcal{S}^A = \oplus_{a\in A}\mathcal{S} = \{(r_a)_{a\in A} : r_a \in \mathcal{S}\}$ and let

$$\mathcal{R}(A) = \{(r_a)_{a\in A} \in \mathcal{S}^A \ : \ \sum_{a\in A} e_i(a^{-1})r_a = 0 \ \text{ for all } \ 1 \le i \le k\}.$$

For $g \in G$ let $e(g) = \prod_{i=1}^k e_i(g) = (g,\ldots,g) \in G^k$. In Section 3 we shall need the following

Claim 2.2. *Assume that $gcd(|G|,k) = 1$. Then the mapping $\Psi : \mathbb{F}[G] \otimes_{\mathbb{F}} \mathcal{H}(A) \to \mathcal{R}(A)$ given by*

$$\Psi(g \otimes s) = (e(g)\,\rho_a(s))_{a\in A}$$

is an isomorphism.

Proof: We first show injectivity. Let $w \in \ker \Psi$ and write $w = \sum_{g \in G} g \otimes s_g$ where $s_g \in \mathcal{H}(A)$. Then for all $a \in A$

$$\sum_{g \in G} e(g)\rho_a(s_g) = 0.$$

Since $e(g)\rho_a(s_g) \in \mathcal{S}_{ag^k}$ and $ag^k \neq ah^k$ for $g \neq h$ (by the assumption $gcd(|G|, k) = 1$), it follows that $e(g)\rho_a(s_g) = 0$ and hence $\rho_a(s_g) = 0$ for all $g \in G$ and $a \in A$. Therefore $w = 0$. To show surjectivity let $(r_a)_{a \in A} \in \mathcal{R}(A)$. For $g \in G$ let

$$s_g = e(g^{-1}) \sum_{a \in A} \rho_{ag^k}(r_a) \in \bigoplus_{a \in A} \mathcal{S}_a.$$

We first show that $s_g \in \mathcal{H}(A)$. For $1 \leq i \leq k$ and $g \in G$ let

$$t_{i,g} = \sum_{a \in A} e_i(a^{-1})\rho_{ag^k}(r_a) \in \mathcal{S}_{g^k}.$$

Then

$$\begin{aligned}\sum_{g \in G} t_{i,g} &= \sum_{g \in G}\sum_{a \in A} e_i(a^{-1})\rho_{ag^k}(r_a) \\ &= \sum_{a \in A} e_i(a^{-1}) \left(\sum_{g \in G} \rho_{ag^k}(r_a) \right) = \sum_{a \in A} e_i(a^{-1}) r_a = 0.\end{aligned}$$

It follows that $t_{i,g} = 0$ for all $1 \leq i \leq k$ and $g \in G$. Therefore for $1 \leq i \leq k$ and $g \in G$

$$\begin{aligned}\sum_{a \in A} e_i(a^{-1})\rho_a(s_g) &= \sum_{a \in A} e_i(a^{-1})\rho_a \left(e(g^{-1}) \sum_{a' \in A} \rho_{a'g^k}(r_{a'}) \right) \\ &= \sum_{a \in A} e_i(a^{-1}) e(g^{-1})\rho_{ag^k}(r_a) = e(g^{-1}) t_{i,g} = 0.\end{aligned}$$

Hence $s_g \in \mathcal{H}(A)$ and thus $w = \sum_{g \in G} g \otimes s_g \in \mathbb{F}[G] \bigotimes_{\mathbb{F}} \mathcal{H}(A)$. Finally, for all $a \in A$

$$\sum_{g \in G} e(g)\rho_a(s_g) = \sum_{g \in G} e(g) \left(e(g^{-1})\rho_{ag^k}(r_a) \right) = \sum_{g \in G} \rho_{ag^k}(r_a) = r_a$$

and therefore $\Psi(w) = (r_a)_{a \in A}$.

□

Corollary 2.3. *If* $gcd(|G|, k) = 1$ *then*

$$\dim \tilde{H}_{k-1}(X_{A,k}; \mathbb{F}) = \frac{\dim \mathcal{R}(A)}{|G|}.$$

□

3 The Semisimple Case

Let G be the cyclic group of prime order $C_p = \langle z \rangle$ and let $A = \{a_1, \ldots, a_m\} \subset C_p$ where $a_j = z^{\alpha_j}$. Let $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_p^k$. In this section we compute $\dim \tilde{H}_{k-1}(X_{A,k}; \mathbb{F})$ when $char\,\mathbb{F} \neq p$. We may assume that $\mathbb{F}$ is algebraically closed. Recall that ω is a primitive p-th root of unity in $\mathbb{F} = \overline{\mathbb{F}}$. The character group $\widehat{C_p}$ consists of all characters η_u where $u \in \mathbb{F}_p$ and $\eta_u(z) = \omega^u$. Similarly, $\widehat{C_p^k} = \{\chi_\beta : \beta = (\beta_1, \ldots, \beta_k) \in \mathbb{F}_p^k\}$ where for $\gamma = (\gamma_1, \ldots, \gamma_k) \in \mathbb{F}_p^k$

$$\chi_\beta(z^{\gamma_1}, \ldots, z^{\gamma_k}) = (\eta_{\beta_1} \times \ldots \times \eta_{\beta_k})(z^{\gamma_1}, \ldots, z^{\gamma_k}) = \omega^{\beta\gamma}$$

and $\beta\gamma = \sum_{i=1}^k \beta_i\gamma_i$ is the standard inner product in $\mathbb{F}_p^k$. The Fourier transform of $f \in \mathbb{F}[C_p^k]$ is thus $\widehat{f} \in \mathbb{F}[\widehat{C_p^k}]$ given by

$$\widehat{f}(\chi_\beta) = \sum_{\gamma=(\gamma_1,\ldots,\gamma_k)\in\mathbb{F}_p^k} f(z^{\gamma_1}, \ldots, z^{\gamma_k})\omega^{-\beta\gamma}.$$

As already remarked, in proving Theorem 1.2 we may assume that $k < p$. Corollary 2.3 then implies that $\dim \tilde{H}_{k-1}(X_{A,k}; \mathbb{F}) = \frac{\dim \mathcal{R}(A)}{p}$. Theorem 1.2 will thus follow from

Proposition 3.1.

$$\dim \mathcal{R}(A) = m\binom{p}{k} - \sum_{\beta \in \mathcal{B}_k} \operatorname{rank} M_{\beta,\alpha}.$$

Proof: Define an $\mathbb{F}$-linear mapping

$$\Phi : \mathcal{S}^A \to \bigoplus_{\beta \in \mathcal{B}_k} \mathbb{F}^m$$

as follows. For $r = (r_{a_j})_{j=1}^m \in \mathcal{S}^A$ let

$$\Phi(r) = \left(\begin{bmatrix} \widehat{r_{a_1}}(\chi_\beta) \\ \vdots \\ \widehat{r_{a_m}}(\chi_\beta) \end{bmatrix} \ : \ \beta \in \mathcal{B}_k \right).$$

Note that since r_{a_j} is a skew symmetric element of $\mathbb{F}[C_p^k]$, it follows that $\widehat{r_{a_j}}$ is a skew symmetric element of $\mathbb{F}[\widehat{C_p^k}]$ and hence is determined by its values on $\mathcal{B}_k$. Therefore Φ is an isomorphism.

Claim 3.2. *Φ restricts to an isomorphism from $\mathcal{R}(A)$ onto $\oplus_{\beta \in \mathcal{B}_k} \ker M_{\beta,\alpha}$.*

Proof: Note that if $1 \leq i \leq k$ and $\beta = (\beta_1, \dots, \beta_k) \in \mathbb{F}_p^k$ then

$$\widehat{e_i(a_j^{-1})}(\chi_\beta) = \widehat{e_i(z^{-\alpha_j})}(\chi_\beta) = \omega^{\beta_i \alpha_j}.$$

Let $r = (r_{a_j})_{j=1}^m \in \mathcal{S}^A$ and fix $1 \leq i \leq k$ and $\beta = (\beta_1, \dots, \beta_k) \in \mathbb{F}_p^k$. Evaluating the Fourier transform of the element $\sum_{j=1}^m e_i(a_j^{-1}) r_{a_j}$ at the character χ_β we obtain

$$\begin{aligned} &(\sum_{j=1}^m e_i(a_j^{-1}) r_{a_j})\hat{}(\chi_\beta) \\ &= \sum_{j=1}^m \widehat{e_i(a_j^{-1})}(\chi_\beta) \widehat{r_{a_j}}(\chi_\beta) \\ &= \sum_{j=1}^m \omega^{\beta_i \alpha_j} \widehat{r_{a_j}}(\chi_\beta). \end{aligned}$$

It follows that $r = (r_{a_j})_{j=1}^m \in \mathcal{R}(A)$ iff for all $\beta = (\beta_1, \dots, \beta_k) \in \mathbb{F}_p^k$

$$M_{\beta,\alpha} \begin{bmatrix} \widehat{r_{a_1}}(\chi_\beta) \\ \vdots \\ \widehat{r_{a_m}}(\chi_\beta) \end{bmatrix} = \begin{bmatrix} \omega^{\beta_1 \alpha_1} & \cdots & \omega^{\beta_1 \alpha_m} \\ \vdots & \ddots & \vdots \\ \omega^{\beta_k \alpha_1} & \cdots & \omega^{\beta_k \alpha_m} \end{bmatrix} \begin{bmatrix} \widehat{r_{a_1}}(\chi_\beta) \\ \vdots \\ \widehat{r_{a_m}}(\chi_\beta) \end{bmatrix} = 0.$$

Therefore $r = (r_{a_j})_{j=1}^m \in \mathcal{R}(A)$ iff $\Phi(r) \in \oplus_{\beta \in \mathcal{B}_k} \ker M_{\beta,\alpha}$. The Claim now follows from the bijectivity of Φ.

□

Proof of Proposition 3.1: By Claim 3.2

$$\begin{aligned}\dim \mathcal{R}(A) &= \sum_{\beta\in\mathcal{B}_k} \dim\ker M_{\beta,\alpha} = \sum_{\beta\in\mathcal{B}_k} (m - \operatorname{rank} M_{\beta,\alpha}) \\ &= m\binom{p}{k} - \sum_{\beta\in\mathcal{B}_k} \operatorname{rank} M_{\beta,\alpha}.\end{aligned}$$

□

4 The Modular Case

In subsections 4.1 and 4.2 we study certain properties of determinants of generalized Vandermonde matrices over the group algebra $\mathbb{F}_p[C_p^k]$. These results are then used in subsection 4.3 to prove Theorem 1.3.

4.1 A Generalized Vandermonde

Recall that z is a fixed generator of C_p and let $1 \le k \le p$. For $1 \le i \le k$ let $x_i = e_i(z)$. Then $\{x_1, \ldots, x_k\}$ is a generating set of C_p^k. Let $x = (x_1, \ldots, x_k)$. For $\beta = (\beta_1, \ldots, \beta_k) \in \mathcal{B}_k$ let

$$N_\beta = \begin{bmatrix} x_1^{-\beta_1} & \cdots & x_1^{-\beta_k} \\ \vdots & \ddots & \vdots \\ x_k^{-\beta_1} & \cdots & x_k^{-\beta_k} \end{bmatrix}.$$

Proposition 4.1. *Let $1 \le k \le p$. Then*

$$\det N_\beta = w_\beta \prod_{1\le i<j\le k} (x_i - x_j) \tag{12}$$

where w_β is a unit of $\mathbb{F}_p[C_p^k]$.

Recall the definition of Schur polynomials (see e.g. [2]). Let $\xi = (\xi_1, \ldots, \xi_k)$ be a vector of variables. For a partition $\lambda = (\lambda_1 \ge \cdots \ge \lambda_k)$ let

$$D_\lambda(\xi) = D_\lambda(\xi_1, \ldots, \xi_k) = \det([\xi_i^{\lambda_j+k-j}]_{i,j=1}^k) \in \mathbb{Z}[\xi_1, \ldots, \xi_k].$$

Note that for the zero partition $0 = (0, \ldots, 0)$

$$D_0(\xi) = \det \begin{bmatrix} \xi_1^{k-1} & \xi_1^{k-2} & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ \xi_k^{k-1} & \xi_k^{k-2} & \cdots & 1 \end{bmatrix} = \prod_{1 \le i < j \le k} (\xi_i - \xi_j).$$

The Schur polynomial associated with λ is

$$\mathbb{S}_\lambda(\xi) = \frac{D_\lambda(\xi)}{D_0(\xi)} \in \mathbb{Z}[\xi_1, \ldots, \xi_k].$$

The dimension formula (see e.g. Proposition 5.21.2 in [2]) asserts that

$$\mathbb{S}_\lambda(1, \ldots, 1) = \prod_{1 \le i < j \le k} \frac{\lambda_i - \lambda_j + j - i}{j - i}. \tag{13}$$

Proof of Proposition 4.1: Let

$$\lambda = (\lambda_1, \ldots, \lambda_k) = (p - \beta_1 - k + 1, p - \beta_2 - k + 2, \ldots, p - \beta_k).$$

Note that $\beta = (\beta_1, \cdots, \beta_k) \in \mathcal{B}_k$ implies that $\lambda_1 \ge \cdots \ge \lambda_k$. Then

$$\begin{aligned} \det N_\beta &= D_\lambda(x) = \mathbb{S}_\lambda(x) D_0(x) \\ &= \mathbb{S}_\lambda(x) \prod_{1 \le i < j \le k} (x_i - x_j). \end{aligned}$$

By (13) the image of $\mathbb{S}_\lambda(x) \in \mathbb{F}_p[C_p^k]$ under the augmentation map $\mathbb{F}_p[C_p^k] \to \mathbb{F}_p$ is

$$\mathbb{S}_\lambda(1, \ldots, 1) \,(\mathrm{mod}\, p) = \prod_{1 \le i < j \le k} \frac{\beta_j - \beta_i}{j - i} \,(\mathrm{mod}\, p) \ne \; 0 \,(\mathrm{mod}\, p).$$

It follows that $w_\beta = \mathbb{S}_\lambda(x)$ is invertible in $\mathbb{F}_p[C_p^k]$.

□

4.2 Skew-Symmetric Annihilators of $\mathbf{D_0(x)}$

Recall that $\mathcal{S}$ is the space of skew symmetric elements of $\mathbb{F}_p[C_p^k]$. In this subsection we show

Proposition 4.2. *Assume that* $1 \leq k < p$ *and let* $s \in \mathcal{S}$. *If* $D_0(x)s = 0$ *then* $s = 0$.

The proof of Proposition 4.2 depends on Proposition 4.3 below. Let $\mathbb{N}$ denote the nonnegative integers and for $a, b \in \mathbb{N}$ let $[a, b] = \{a, \ldots, b\}$. Let

$$\mathbb{N}_k = \{(\mu_1, \ldots, \mu_k) \in \mathbb{N}^k \ : \ \mu_i \neq \mu_j \ \text{ if } \ i \neq j\}.$$

For $\mu = (\mu_1, \ldots, \mu_k)$, $\nu = (\nu_1, \ldots, \nu_k) \in \mathbb{N}_k$ write $\mu \preceq \nu$ if $\{\mu_1, \ldots, \mu_k\}$ precedes $\{\nu_1, \ldots, \nu_k\}$ in the lexicographic order on k-subsets of $\mathbb{N}$, i.e. if

$$\sum_{i=1}^{k} 2^{-\mu_i} \geq \sum_{i=1}^{k} 2^{-\nu_i}.$$

Fix an $\mu = (\mu_1, \ldots, \mu_k) \in \mathbb{N}_k$ such that $\mu_1 < \cdots < \mu_k$ and let

$$L = \{1 \leq i \leq k-1 : \mu_i + 1 < \mu_{i+1}\}.$$

Write $L = \{\ell_1 < \ldots < \ell_{t-1}\}$ and let $\ell_0 = 0$, $\ell_t = k$. For $1 \leq i \leq t$ let $K_i = [\ell_{i-1} + 1, \ell_i]$. Let

$$\mathcal{G}_1(\mu) = \{(\gamma, \sigma) \in \mathbb{N}_k \times S_k \ : \ \gamma \preceq \mu \text{ and } \gamma_j - \sigma(j) = \mu_j - j \ \text{ for all } \ j\}.$$

We'll need the following characterization of $\mathcal{G}_1(\mu)$. Let S_K denote the symmetric group on a set K. Let $T = S_{K_1} \times \cdots \times S_{K_t}$ be the Young subgroup of S_k corresponding to the partition $[k] = \cup_{i=1}^t K_i$. Let

$$\mathcal{G}_2(\mu) = \{(\gamma, \sigma) \in \mathbb{N}_k \times T \ : \ \gamma_j = \mu_{\sigma(j)} \ \text{ for all } \ j\}.$$

Proposition 4.3. $\mathcal{G}_1(\mu) = \mathcal{G}_2(\mu)$

Proof: We first show that $\mathcal{G}_2(\mu) \subset \mathcal{G}_1(\mu)$. Let $(\gamma, \sigma) \in \mathcal{G}_2(\mu)$ and let $1 \leq j \leq k$. If $j \in K_i$ then $\sigma(j) \in K_i$ and hence $\mu_{\sigma(j)} - \mu_j = \sigma(j) - j$. Therefore

$$\gamma_j - \sigma(j) = \mu_{\sigma(j)} - \sigma(j) = \mu_j - j$$

and so $(\gamma, \sigma) \in \mathcal{G}_1(\mu)$. For the other direction let $(\gamma, \sigma) \in \mathcal{G}_1(\mu)$. Write $\gamma = (\gamma_1, \ldots, \gamma_k)$ and let $\pi \in S_k$ such that $\gamma_{\pi(1)} < \cdots < \gamma_{\pi(k)}$.

Claim 4.4. *For $1 \leq i \leq t$ and $j \in K_i$*
(a) $\sigma(\pi(j)) = j$.
(b) $\gamma_{\pi(j)} = \mu_j$.
(c) $\pi(j) \in K_i$.

Proof: We argue by induction on j. Suppose (a),(b) and (c) hold for all $j' < j$. (a) implies that $\{\sigma(\pi(j')) : j' < j\} = [j-1]$ and hence $\sigma(\pi(j)) \geq j$. Therefore

$$\mu_j - j \geq \mu_j - \sigma(\pi(j)). \tag{14}$$

Next note that by (b) $\gamma_{\pi(j')} = \mu_{j'}$ for all $j' < j$. As $\gamma \preceq \mu$ it follows that $\mu_j \geq \gamma_{\pi(j)}$ and therefore

$$\mu_j - \sigma(\pi(j)) \geq \gamma_{\pi(j)} - \sigma(\pi(j)) = \mu_{\pi(j)} - \pi(j). \tag{15}$$

Finally (c) implies that $\{\pi(j') : 1 \leq j' \leq \ell_{i-1}\} = [1, \ell_{i-1}]$ and therefore $\pi(j) \geq \ell_{i-1} + 1$. Together with the assumption $j \in K_i$ it follows that

$$\mu_{\pi(j)} - \pi(j) \geq \mu_{\ell_{i-1}+1} - (\ell_{i-1} + 1) = \mu_j - j. \tag{16}$$

It follows that the three inequalities in (14),(15),(16) are in fact equalities. Therefore $\sigma(\pi(j)) = j$, $\gamma_{\pi(j)} = \mu_j$ and $\mu_{\pi(j)} = \mu_j + (\pi(j) - j)$ respectively establishing (a),(b),(c) for j.

□

Claim 4.4 implies that $\sigma = \pi^{-1} \in T$ and that $\gamma_j = \mu_{\sigma(j)}$ for all $1 \leq j \leq k$. Therefore $(\gamma, \sigma) \in \mathcal{G}_2(\mu)$.

□

Proof of Proposition 4.2: Let $s \in \mathcal{S}$ such that $D_0(x)s = 0$. We have to show that $s = 0$. For $\gamma = (\gamma_1, \ldots, \gamma_k) \in \mathbb{F}_p^k$ we abbreviate $x^\gamma = \prod_{j=1}^k x_j^{\gamma_j} = (z^{\gamma_1}, \ldots, z^{\gamma_k}) \in C_p^k$. Note that this notation is unambiguous since $x_j^p = 1$. By assumption

$$\begin{aligned} 0 = D_0(x)s &= \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) \prod_{j=1}^k x_j^{k-\sigma(j)} \sum_{\gamma=(\gamma_1,\ldots,\gamma_k)\in\mathbb{F}_p^k} s(x^\gamma) \prod_{j=1}^k x_j^{\gamma_j} \\ &= \sum_{\gamma=(\gamma_1,\ldots,\gamma_k)\in\mathbb{F}_p^k} \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) s(x^\gamma) \prod_{j=1}^k x_j^{\gamma_j + k - \sigma(j)}. \end{aligned} \tag{17}$$

Suppose for contradiction that $s \neq 0$ and let

$$\mu = (\mu_1, \ldots, \mu_k) = \max\{\gamma \in \mathcal{B}_k \ : \ s(x^\gamma) \neq 0\}$$

where the maximum is taken with respect to $\preceq$. Let $\lambda \in \mathbb{F}_p$ denote the coefficient of $\prod_{j=1}^k x_j^{\mu_j+k-j}$ in the expansion of $D_0(x)s$ in the standard basis $\{x^\beta : \beta \in \mathbb{F}_p^k\}$ of $\mathbb{F}_p[C_p^k]$. Note that if

$$\prod_{j=1}^k x_j^{\mu_j+k-j} = \prod_{j=1}^k x_j^{\gamma_j+k-\sigma(j)}$$

then for all $1 \leq j \leq k$

$$\mu_j - j = \gamma_j - \sigma(j) \pmod p.$$

Since

$$-1 \leq \mu_j - j \leq p-1-k$$

and

$$-k \leq \gamma_j - \sigma(j) \leq p-2$$

it follows that

$$\mu_j - j = \gamma_j - \sigma(j).$$

Hence, Eq. (17) and Proposition 4.3 imply that

$$\begin{aligned}\lambda = \sum_{(\gamma,\sigma)\in\mathcal{G}_1(\mu)} \operatorname{sgn}(\sigma)s(x^\gamma) &= \sum_{(\gamma,\sigma)\in\mathcal{G}_2(\mu)} \operatorname{sgn}(\sigma)s(x^\gamma)\\ &= \sum_{(\gamma,\sigma)\in\mathcal{G}_2(\mu)} \operatorname{sgn}(\sigma)s(z^{\gamma_1}, \ldots, z^{\gamma_k})\\ &= \sum_{\sigma\in S_{K_1}\times\cdots\times S_{K_t}} \operatorname{sgn}(\sigma)s(z^{\mu_{\sigma(1)}}, \ldots, z^{\mu_{\sigma(k)}})\\ &= |S_{K_1}\times\cdots\times S_{K_t}|\, s(z^{\mu_1}, \ldots, z^{\mu_k}) = \prod_{i=1}^t (\ell_i - \ell_{i-1})!\, s(x^\mu).\end{aligned}$$

Since $\ell_t = k < p$ it follows that $\prod_{i=1}^t (\ell_i - \ell_{i-1})! \neq 0 (\bmod p)$ and so $\lambda \neq 0$. Therefore $D_0(x)s \neq 0$, a contradiction.

□

Remark: Proposition 4.2 does not hold for $k = p$. Indeed, in this case $s = D_0(x) = \prod_{1\leq i<j\leq p}(x_i - x_j)$ is a nonzero skew symmetric element of $\mathbb{F}_p[C_p^p]$ and it can be checked that $D_0(x)s = D_0(x)^2 = 0$.

4.3 Homology of $\mathbf{X_{A,k}}$ over $\mathbb{F}_\mathbf{p}$

In this subsection we prove Theorem 1.3. We first consider the case $m = k$. **Theorem 4.5.** *If $|A| = k$ then $\tilde{H}_{k-1}(X_{A,k}; \mathbb{F}_p) = 0$.*

Proof: As already noted the case $k = p$ is trivial so we assume $k < p$. Let $A = \{a_1, \ldots, a_k\}$ where $a_i = z^{\alpha_i}$ and $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathcal{B}_k$. Let $s \in \tilde{H}_{k-1}(X_{A,k}; \mathbb{F}_p)$ then by Claim 2.1

$$N_\alpha \begin{bmatrix} \rho_{a_1}(s) \\ \vdots \\ \rho_{a_k}(s) \end{bmatrix} = \begin{bmatrix} x_1^{-\alpha_1} & \cdots & x_1^{-\alpha_k} \\ \vdots & \ddots & \vdots \\ x_k^{-\alpha_1} & \cdots & x_k^{-\alpha_k} \end{bmatrix} \begin{bmatrix} \rho_{a_1}(s) \\ \vdots \\ \rho_{a_k}(s) \end{bmatrix}$$
$$= \begin{bmatrix} e_1(a_1^{-1}) & \cdots & e_1(a_k^{-1}) \\ \vdots & \ddots & \vdots \\ e_k(a_1^{-1}) & \cdots & e_k(a_k^{-1}) \end{bmatrix} \begin{bmatrix} \rho_{a_1}(s) \\ \vdots \\ \rho_{a_k}(s) \end{bmatrix} = 0.$$

Therefore $\det N_\alpha \cdot \rho_{a_j}(s) = 0$ for all $1 \le j \le k$. Proposition 4.1 then implies that $D_0(x)\rho_{a_j}(s) = 0$. Hence $\rho_{a_j}(s) = 0$ by Proposition 4.2. It follows that $s = 0$ and so $\tilde{H}_{k-1}(X_{A,k}; \mathbb{F}_p) = 0$.

□

Proof of Theorem 1.3: Let $|A| = m \ge k$ and let A' be an arbitrary subset of A of cardinality k. Theorem 4.5 and Eq. (6) imply that $\tilde{H}_*(X_{A',k}; \mathbb{F}_p) = 0$. Hence by the exact sequence

$$0 = \tilde{H}_{k-1}(X_{A',k}; \mathbb{F}_p) \to \tilde{H}_{k-1}(X_{A,k}; \mathbb{F}_p) \to$$
$$\to \tilde{H}_{k-1}(X_{A,k}, X_{A',k}; \mathbb{F}_p) \to \tilde{H}_{k-2}(X_{A',k}; \mathbb{F}_p) = 0$$

it follows that

$$\dim \tilde{H}_{k-1}(X_{A,k}; \mathbb{F}_p) = \dim \tilde{H}_{k-1}(X_{A,k}, X_{A',k}; \mathbb{F}_p)$$
$$= f_{k-1}(X_{A,k}) - f_{k-1}(X_{A',k}) = (\frac{m}{k} - 1)\binom{p-1}{k-1}.$$

□

5 Uncertainty Numbers and Homology

Proof of Theorem 1.1: Recall that $A = \{z^{\alpha_1}, \ldots, z^{\alpha_m}\} \subset C_p$. Let $\mathbb{F}$ be an algebraically closed field with $\operatorname{char} \mathbb{F} = \ell$. We consider two cases:

(i) **The semisimple case** $\ell \neq p$. Here it suffices to show that for any fixed $1 \leq k \leq p$ the following three conditions are equivalent:

(C1) $\tilde{H}_{k-1}(X_{A,k}; \mathbb{F}) \neq 0$.

(C2) There exists a $\beta \in \mathcal{B}_k$ such that $\operatorname{rank} M_{\beta,\alpha} < m$.

(C3) $u_{\mathbb{F}}(A) \leq p - k$.

First note that Theorem 1.2 implies that $\tilde{H}_{k-1}(X_{A,k}; \mathbb{F}) \neq 0$ iff

$$\frac{m}{p}\binom{p}{k} > \frac{1}{p}\sum_{\beta \in \mathcal{B}_k} \operatorname{rank} M_{\beta,\alpha}.$$

This proves the equivalence of (C1) and (C2). Next let $\lambda = (\lambda_1, \ldots, \lambda_m) \in \mathbb{F}^m$ and let $f_\lambda = \sum_{j=1}^m \lambda_j z^{\alpha_j} \in \mathbb{F}[C_p]$. Then $\operatorname{supp}(f_\lambda) \subset A$ and for $\beta = (\beta_1, \ldots, \beta_k) \in \mathbb{F}_p^k$

$$M_{\beta,\alpha}\lambda = (\sum_{j=1}^m \lambda_j \omega^{\beta_i \alpha_j})_{i=1}^k = \left(\widehat{f_\lambda}(\eta_{-\beta_i})\right)_{i=1}^k .$$

It follows that if $\beta = (\beta_1, \ldots, \beta_k) \in \mathcal{B}_k$ then $\operatorname{rank} M_{\beta,\alpha} < m$ iff there exists a nonzero $f = f_\lambda \in \mathbb{F}[C_p]$ such that $\operatorname{supp}(f) \subset A$ and $\operatorname{supp}(\widehat{f}) \cap \{\eta_{-\beta_i}\}_{i=1}^k = \emptyset$. This proves the equivalence of (C2) and (C3).

(ii) **The modular case** $\ell = p$. Let $\mathbb{F}$ be a field of characteristic p. By Theorem 1.3

$$p - \max\{k : \tilde{H}_{k-1}(X_{A,k}; \mathbb{F}) \neq 0\} = p - m + 1.$$

It thus suffices to show that $u_{\mathbb{F}}(A) = p - m + 1$. Let $0 \neq f = \sum_{j=1}^m \lambda_j z^{\alpha_j} \in \mathbb{F}[C_p]$. Regarding $f = f(z)$ as an element of the polynomial ring $\mathbb{F}[z]$, the rank of T_f is given by

$$\begin{aligned} \operatorname{rank} T_f &= p - \deg \gcd(f(z), z^p - 1) \\ &= p - \deg \gcd(f(z), (z-1)^p) = p - \mu(f) \end{aligned} \qquad (18)$$

where $\mu(f)$ is the multiplicity of 1 as a root of $f(z)$. By a simple well known result (see e.g. Lemma 2 in [4]), $\mu(f) \leq m-1$ and hence $u_{\mathbb{F}}(A) \geq p-m+1$. For the other direction note that the $\mathbb{F}$-linear space

$$\mathcal{P} = \{f(z) \in \mathbb{F}[C_p] : \ \mu(f) \geq m-1\}$$

satisfies $\dim_{\mathbb{F}} \mathcal{P} = p-m+1$ and hence must contain a nonzero f of the form $f(z) = \sum_{j=1}^{m} \lambda_j z^{\alpha_j}$. It follows by (18) that f satisfies $\operatorname{rank} T_f \leq p-m+1$. Therefore $u_{\mathbb{F}}(A) \leq p-m+1$.

□

6 Concluding Remarks

We mention two problems related to the results of this paper.

1. Let $k \geq 2$ and let X be a $(k-1)$-dimensional complex X with $N = f_{k-1}(X)$ facets. It was observed by G. Kalai, S. Weinberger and the author that the torsion subgroup $H_{k-2}(X)_{tor}$ satisfies $|H_{k-2}(X)_{tor}| \leq \sqrt{k}^N$. Kalai on the other hand showed [5] that there exist X's with $|H_{k-2}(X)_{tor}| \geq \sqrt{k/e}^N$. Computer experiments indicate that the $\mathbb{Q}$-acyclic sum complexes obtained by taking $|A| = k$ often have large torsion. For example, $A = \{1, z, z^{19}\} \subset C_{83}$ satisfies $|H_1(X_{A,3})| > 1.17^N$ where $N = f_2(X_{A,3}) = \binom{82}{2}$. Note that the base of the exponent 1.17 is slightly bigger than the constant $\sqrt{3/e} \doteq 1.05$ in Kalai's lower bound. In view of this it would be interesting to determine (or estimate) the maximum torsion of sum complexes.

2. Theorem 1.1 characterizes the uncertainty number $u_{\mathbb{F}}(A)$ with $A \subset G = C_p$ and $\mathbb{F}$ algebraically closed, in terms of the homology of $X_{A,k}$ over $\mathbb{F}$. It would be useful to find appropriate extensions of this characterization to general finite groups G and arbitrary fields $\mathbb{F}$.

References

[1] D.L. Donoho and P.B. Stark, Uncertainty principles and signal recovery, *SIAM J. Applied Math.* **49**(1989) 906-931.

[2] P. Etingof, Introduction to Representation Theory, Student Mathematical Library Vol. 59, AMS, 2011.

[3] G. Folland and A. Sitaram, The uncertainty principle: a mathematical survey, *J. Fourier Anal. Appl.* **3**(1997) 207-238.

[4] P. E. Frenkel, Simple proof of Chebotarev's theorem on roots of unity, arXiv:math/0312398.

[5] G. Kalai, Enumeration of $\mathbb{Q}$-acyclic simplicial complexes, *Israel J. Math.* **45**(1983) 337–351.

[6] N. Linial, R. Meshulam and M. Rosenthal, Sum complexes - a new family of hypertrees, *Discrete Comput. Geom.*, **44**(2010) 622–636.

[7] R. Meshulam, An uncertainty inequality for finite abelian groups, *European J. of Combinatorics*, **27**(2006) 63-67.

[8] P. Stevenhagen and H. W. Lenstra, Chebotarëv and his density theorem, *Math. Intelligencer* **18**(1996) 26–37.

[9] T. Tao, An uncertainty principle for cyclic groups of prime order, *Math. Res. Lett.* **12**(2005)121-127.