

On the Existence of Extremal Cones and Comparative Probability Orderings

Simon Marshall*

Department of Mathematics
The University of Auckland
New Zealand

Abstract

We study the recently discovered phenomenon [1] of existence of comparative probability orderings on finite sets that violate Fishburn hypothesis [2, 3] — we call such orderings and the discrete cones associated with them extremal. Conder and Slinko constructed an extremal discrete cone on the set of $n = 7$ elements and showed that no extremal cones exist on the set of $n \leq 6$ elements. In this paper we construct an extremal cone on a finite set of prime cardinality p if p satisfies a certain number theoretical condition. This condition has been computationally checked to hold for 1,725 of the 1,842 primes between 132 and 16,000, hence for all these primes extremal cones exist.

Key words: Comparative probability ordering, Discrete cone, Quadratic residues

AMS classification: 05 B20, 05 B30, 60 A05

*Address for correspondence: Department of Mathematics, The University of Auckland, Private Bag 92019, Auckland New Zealand. Fax: 64-9-3737457, email: smar141@ec.auckland.ac.nz

1 Introduction

A comparative probability ordering on a finite set X of cardinality n is an order¹ on the power set 2^X satisfying the following de Finetti's axiom [4]: for any $A, B, C \subseteq X$

$$A \succeq B \iff A \cup C \succeq B \cup C \text{ whenever } (A \cup B) \cap C = \emptyset.$$

The set X is normally assumed to be $\{1, 2, \dots, n\}$.

Comparative probability orderings are normally studied in terms of combinatorial objects associated with them called discrete cones [1, 2, 3]. We may represent a subset $A \subseteq X$ by an n -dimensional characteristic vector \mathbf{v}_A whose i th coordinate is 1 if $i \in A$ and 0 otherwise. Likewise the comparison $A \succeq B$ can be represented by the vector $\mathbf{v}_A - \mathbf{v}_B$ whose coordinates will now lie in the set $T = \{-1, 0, 1\}$. In this way we may think of comparative probability orderings as subsets of T^n by converting all comparisons to vectors, with de Finetti's axiom ensuring that this correspondence is well defined. The resulting objects, called discrete cones, proved to be a convenient tool for the study of comparative probability orderings.

Definition 1. *A subset C of T^n is a discrete cone if:*

- (i) *if $\mathbf{x} \in C$ and $\mathbf{y} \in C$ then $\mathbf{x} + \mathbf{y} \in C$ provided $\mathbf{x} + \mathbf{y} \in T^n$;*
- (ii) *for $\mathbf{x} \in T^n$, either $\mathbf{x} \in C$ or $-\mathbf{x} \in C$ (not both for $\mathbf{x} \neq \mathbf{0}$);*
- (iii) *$\{\mathbf{e}_1 - \mathbf{e}_2, \dots, \mathbf{e}_{n-1} - \mathbf{e}_n, \mathbf{e}_n\} \subseteq C$, where $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ is the standard basis of \mathbb{R}^n*

We define a discrete cone to be almost representable if there is a vector \mathbf{n} with strictly positive, distinct entries such that $\mathbf{x} \in C \implies \mathbf{x} \cdot \mathbf{n} \geq 0$, and representable if, in addition, $\mathbf{x} \cdot \mathbf{n} = 0 \iff \mathbf{x} = \mathbf{0}$. These two conditions correspond to the existence of a probability measure on X which almost agree or, respectively, agree with the comparative probability ordering to which the cone corresponds [5].

A central question in the study of comparative probability orderings is what conditions are required to ensure that such an ordering is representable. Conditions which are known to be necessary and sufficient are the so-called cancellation conditions C_1, \dots, C_k, \dots developed by Kraft, Pratt and Siedenberg [5]. A discrete cone C (and the corresponding comparative probability

¹any reflexive, complete and transitive binary relation

ordering) satisfies the m th cancellation condition C_m if there are no m vectors $\mathbf{x}_1, \dots, \mathbf{x}_m \in C$ and positive integers a_1, \dots, a_m such that

$$\sum_{i=1}^m a_i \mathbf{x}_i = \mathbf{0}.$$

It is clear that any representable cone satisfies all cancellation conditions.

As conditions C_1, C_2, C_3 are satisfied by any comparative probability ordering [2], Fishburn [2, 3] defined a function $f(n)$ as the smallest number k such that the cancellation conditions C_4, \dots, C_k ensure that a probability ordering on a n element set is representable. Conder and Slinko [1] introduced a similar function $g(n)$ which is the smallest number k such that the cancellation conditions C_4, \dots, C_k ensure that an almost representable order is representable. It is clear that $g(n) \leq f(n)$ and it is easy to show that $f(n) \leq n+1$ and $g(n) \leq n$. Fishburn proved that $f(5) = 4$ and $f(n) \geq n-1$. He conjectured that $f(n) = n-1$ for all $n \geq 5$. Conder and Slinko [1] confirmed it for $n=6$ proving that $f(6) = g(6) = 5$, however they disproved the hypothesis for $n = 7$ by showing that $f(7) \geq g(7) = 7$.

Definition 2. *We will call a discrete cone C in T^n (and the respective comparative probability ordering) extremal if C satisfies the cancellation conditions C_1, \dots, C_{n-1} but is not representable.*

Thus we may say that Conder and Slinko constructed the first extremal almost representable cone in T^7 . The goal of this article is to prove $f(n) \geq g(n) = n$, when n is a prime satisfying a certain condition. More exactly, we prove

Theorem 1. *Let p be a prime greater than 131. If*

$$\left(1 + \sqrt{\left(\frac{-1}{p}\right)^p}\right)^p - 1 = a + b\sqrt{\left(\frac{-1}{p}\right)^p}, \quad (1)$$

where $\gcd(a, b) = p$, then there exists an extremal almost representable discrete cone in T^p and, in particular, $g(p) = p$.

The odd primes satisfying (1) we will call regular because our observations show that the majority of primes satisfy this condition. The first few non-regular primes are

$$3, 23, 31, 137, 191, 239, 277, 359, \dots$$

Our calculations show that 1725 of the 1842 primes between 132 and 16000 are regular primes and Theorem 1 is true for them. At this point, however, we know nothing about the general distribution of such primes, or even if there are an infinite number of them.

2 The Discrete Cones and Matrices

The idea behind all constructions of almost representable but not representable cones is as follows. We choose a probability measure $\mathbf{p} = (p_1, \dots, p_n)$ on $[n]$ with all p_i 's positive and distinct such that the corresponding ordering of subsets in $\mathcal{P}[n]$ is not strict and some subsets are tied having equal probabilities. Then we break ties in a coordinated way and with some luck we may get a comparative probability ordering which is not representable. In the language of cones, a tie means having a pair of vectors $\pm \mathbf{x}$ in the cone, and breaking it means throwing one of them away.

Example 1. *The non-representable comparative probability ordering \succ on $\mathcal{P}[5]$ constructed in [5] does not satisfy the condition C_4 since it contains the following comparisons:*

$$\{1, 3\} \succ \{2, 4, 5\}, \{2, 4\} \succ \{1, 5\}, \{2, 5\} \succ \{3, 4\}, \{4, 5\} \succ \{2\}. \quad (2)$$

These are contradictory which is reflected in the relation $\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 + \mathbf{x}_4 = \mathbf{0}$ for their respective vectors

$$\begin{aligned} \mathbf{x}_1 &= (1, -1, 1, -1, -1)^T, \\ \mathbf{x}_2 &= (-1, 1, 0, 1, -1)^T, \\ \mathbf{x}_3 &= (0, 1, -1, -1, 1)^T, \\ \mathbf{x}_4 &= (0, -1, 0, 1, 1)^T. \end{aligned}$$

This can be obtained from a representable but nonstrict comparative probability ordering with the measure $\mathbf{p} = \frac{1}{24}(8, 7, 4, 3, 2)$ for which all pairs in (2) are tied.

Conder and Slinko [1] in the following theorem clarified the conditions under which such construction would work (in their construction we replaced rows with columns).

Theorem 2 (Conder-Slinko, [1]). *Let $X = \{\mathbf{x}_1, \dots, \mathbf{x}_m\}$, $m \geq 4$, be a system of non-zero vectors from T^n , such that $\sum_{i=1}^m a_i \mathbf{x}_i = \mathbf{0}$ for some positive integers a_1, \dots, a_m , and such that no proper subsystem $X' \subset X$ is linearly dependent with positive coefficients. Suppose further that the $n \times m$ matrix U having the vectors $\mathbf{x}_1, \dots, \mathbf{x}_m$ as its columns has the property that $\mathbf{p}U = \mathbf{0}$ for some positive integer-valued vector $\mathbf{p} = (p_1, \dots, p_m)$ with $p_1 > p_2 > \dots > p_m > 0$, with $\sum_{i=1}^m p_i = 1$, and that*

$$\text{span}\{\mathbf{x}_1, \dots, \mathbf{x}_m\} \cap T^n = \{\pm \mathbf{x}_1, \dots, \pm \mathbf{x}_m\}. \quad (3)$$

Let $C(\succeq)$ be the discrete cone belonging to the weak comparative probability ordering which arises from the measure \mathbf{p} , that is, $C(\succeq) = \{\mathbf{x} \in T^n \mid \mathbf{p} \cdot \mathbf{x} \geq 0\}$. Then the discrete cone

$$C' = C(\succeq) \setminus \{-\mathbf{x}_1, \dots, -\mathbf{x}_m\}$$

corresponds to an almost representable comparative probability ordering which almost agrees with \mathbf{p} , and satisfies C_i for all $i < m$, but does not satisfy C_m .

It should be noted that the condition (3) is most demanding and very difficult to achieve.

For our construction of extremal cones we will use the above theorem. We will construct a $p \times p$ matrix U with columns $\mathbf{u}_1, \dots, \mathbf{u}_p$ which has the following properties:

- (i) The only dependence between the columns \mathbf{u}_i is $\sum_{i=1}^p \mathbf{u}_i = \mathbf{0}$.
- (ii) The only vectors in $\text{col}(U) \cap T^p$ are $\pm \mathbf{u}_i$.
- (iii) None of the \mathbf{u} 's is of the form \mathbf{e}_i or $\pm \mathbf{e}_i \pm \mathbf{e}_j$, for $i \neq j$.

We claim that the conditions of the Theorem 2 will then be possible to satisfy. Indeed, the only thing to check is the existence of a positive integer-valued vector \mathbf{p} with the property $\mathbf{p}U = \mathbf{0}$. Since U has rank $p - 1$ such vector \mathbf{p} satisfying $\mathbf{p}U = \mathbf{0}$ is unique up to a scalar multiple and has rational co-ordinates. From the conditions on columns of U we know that neither \mathbf{e}_i nor $\pm \mathbf{e}_i \pm \mathbf{e}_j$ belongs to $\text{Col}(U)$. This implies that $p_i \neq 0$ and $|p_i| \neq |p_j|$ for all $i \neq j$. If one or more co-ordinates of \mathbf{p} are negative, we change U multiplying the respective rows by -1 . We then know that all co-ordinates of \mathbf{p} are distinct, so by permuting the rows of U we may assume that $p_1 > p_2 > \dots > p_n > 0$. At last \mathbf{p} can be normalised so that $\sum_{i=1}^n p_i = 1$. Summarising we state

Theorem 3. *If a $p \times p$ matrix U satisfying properties (i)–(iii) exists, then there exists an extremal discrete cone in T^p .*

3 The Construction of U

Our construction is based on the distribution of quadratic residues modulo a prime $p > 3$. We use the Legendre quadratic residue symbol $\left(\frac{i}{p}\right)$, $i =$

$0, 1, 2, \dots, p-1$, where for convenience we take $\left(\frac{0}{p}\right)$ to be 0. The idea is to alter the vector of quadratic residue symbols

$$\mathbf{r} = \left(0, \left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots, \left(\frac{p-1}{p}\right)\right)^T$$

in the first two co-ordinates as follows

$$\mathbf{q} = \left(1, \left(\frac{1}{p}\right) - 1, \left(\frac{2}{p}\right), \dots, \left(\frac{p-1}{p}\right)\right)^T,$$

and then form a circulant matrix

$$Q = [\mathbf{q}, S\mathbf{q}, S^2\mathbf{q}, \dots, S^{p-1}\mathbf{q}]$$

from \mathbf{q} , where S is the standard matrix of the circular shift operator which translates all coordinates one place down, with the last co-ordinate being placed at the top. The quadratic residue nature of these vectors means that 1's and -1 's are evenly distributed, making it hard for any nontrivial linear combination to have co-ordinates all from T , while at the same time the matrix still has enough structure that we may effectively prove that the desired conditions hold.

Further we will also need the matrix

$$R = [\mathbf{r}, S\mathbf{r}, S^2\mathbf{r}, \dots, S^{p-1}\mathbf{r}],$$

and we note that $Q = R + I - S$, where I is the identity matrix.

Now finally we form U from Q by subtracting 1 from q_{11} and adding 1 to q_{1p} , and denote its columns by $\mathbf{u}_1, \dots, \mathbf{u}_p$. We note that $\mathbf{u}_i \in T^p$ for all $i = 1, 2, \dots, p$. Here is an example of such construction for $p = 5$:

$$U = \begin{bmatrix} 0 & 1 & -1 & -1 & 1 \\ 0 & 1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 1 & -1 \\ -1 & -1 & 0 & 1 & 1 \\ 1 & -1 & -1 & 0 & 1 \end{bmatrix}.$$

Let us define the integer span of the columns of U as follows:

$$\text{intspan}\{\mathbf{u}_1, \dots, \mathbf{u}_p\} = \left\{ \sum_{i=1}^p n_i \mathbf{u}_i \mid n_i \in \mathbb{Z} \right\}.$$

We will now prove that U satisfies properties (i)-(iii). We wish to split the proof of (ii) into two smaller statements, the first that the only integer vectors in $\text{col}(U) \cap T^p$ are those of the form $\sum_{i=1}^p n_i \mathbf{u}_i$ with $n_i \in \mathbb{Z}$, and the second that there are no vectors of this form in T^p . They will be proved in the following two lemmata.

Lemma 1. $\text{col}(U) \cap T^p = \text{intspan}\{\mathbf{u}_1, \dots, \mathbf{u}_p\}$.

Proof. We will make use here of the canonical homomorphism

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z},$$

where q is a prime, and denote the image of a under ϕ by \bar{a} . This mapping can be extended in an obvious way to a mapping of integer vectors, or integer matrices, and the image of a vector \mathbf{u} or matrix M under this mapping will be similarly denoted $\bar{\mathbf{u}}$ or \bar{M} , respectively.

Assuming the contrary to the lemma, there must be some $a_i, b_i \in \mathbb{Z}$, $i = 1, 2, \dots, p$ such that

$$\sum_{i=1}^p \frac{a_i}{b_i} \mathbf{u}_i \in T^p \quad \text{and} \quad \mathbf{u} = \sum_{i=1}^p \frac{a_i}{b_i} \mathbf{u}_i \notin \text{intspan}\{\mathbf{u}_1, \dots, \mathbf{u}_p\} \quad (4)$$

Since $\mathbf{u}_1 + \dots + \mathbf{u}_p = \mathbf{0}$ we may always obtain a relation (4) with $a_i = 0$ for an arbitrary i . It is clear that $\mathbf{u} \neq \mathbf{0}$ and after representing \mathbf{u} in the form

$$\mathbf{u} = \sum_{i=1}^p \frac{n_i}{n} \mathbf{u}_i$$

where $\text{gcd}(n_1, \dots, n_p)$ is relatively prime to n , we may assume that it is not true that $n_1 = \dots = n_p$ (otherwise $\mathbf{u} = \mathbf{0}$). As $n \geq 1$, let q be any prime divisor of n . Then

$$\sum_{i=1}^p n_i \mathbf{u}_i \in q\mathbb{Z}^p$$

where at least one n_i is not divisible by q due to the relative primeness of $\text{gcd}(n_1, \dots, n_p)$ to n . Hence

$$\sum_{i=1}^p \bar{n}_i \bar{\mathbf{u}}_i = \mathbf{0},$$

and such relations may be obtained with $\bar{n}_i = 0$ for arbitrary i . Therefore any $p - 1$ element subset of $\{\mathbf{u}_1, \dots, \mathbf{u}_p\}$ must have a linear dependency. As a result, the determinant of any principal minor of \bar{U} is 0, or equivalently the determinant of any principal minor of U is divisible by q .

Because the rows and columns of Q add to the zero vector, all principal minors of this matrix must have determinant $\pm D$ for some D . If q is a prime dividing the determinants of all principal minors of U , it must also divide D as Q and U share some principal minors. The determinant of the $(i, 1)$ st principal minor of U will be the determinant of the corresponding principal

minor of Q plus the determinant of the matrix V_i obtained by removing from Q rows 1 and i , and columns 1 and p . This implies that q divides $\det(V_i)$ for all i . Therefore \overline{Q} must have nullity 2, and because the sum of the rows of \overline{Q} is $\mathbf{0}$ it will also have a set of $p - 2$ dependent columns. We will now show that this leads to a contradiction.

To show that Q has no $p - 2$ columns with a dependency modulo any prime dividing D , let us write $Q = R + I - S$, where I is the identity matrix and S is the standard matrix of the shift as before. We wish to show that $W = (R - I + S)(R + I - S)$ has no $p - 2$ dependent columns, and, hence, $Q = R + I - S$ does not have them either.

Let us note now that all circulant matrices lie in the one-generated subalgebra of the matrix algebra generated by S . If A is a circulant matrix with first column $(a_0, a_1, \dots, a_{p-1})^T$ then $A = \sum_{k=0}^{p-1} a_k S^k$. Let the p th roots of unity over \mathbb{Q} be $1, \omega, \omega^2, \dots, \omega^{p-1}$. Then these roots of unity are exactly the eigenvalues of S and, hence, the eigenvalues of A will be

$$\lambda_i = \sum_{k=0}^{p-1} a_k \omega^{ki}, \quad (i = 1, \dots, p)$$

(see also [6]). Being in one-generated subalgebra, any two circulant matrices commute, hence $R(I - S) = (I - S)R$ and $W = R^2 - (I - S)^2$.

Denote by τ the Gauss sum $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \omega^i$. It is known [7] that $\tau^2 = \left(\frac{-1}{p}\right) p$, and expanding this sum fully allows us to calculate R^2 . We have

$$\left(\frac{-1}{p}\right) p = \tau^2 = \left(\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \omega^i\right)^2 = \sum_{n=0}^{p-1} \omega^n \sum_{i+j \equiv n} \left(\frac{i}{p}\right) \left(\frac{j}{p}\right), \quad (5)$$

where the congruence in the subscript is modulo p . Since

$$\sum_{i \equiv -j} \left(\frac{i}{p}\right) \left(\frac{j}{p}\right) = \sum_{i=1}^{p-1} \left(\frac{-i^2}{p}\right) = \left(\frac{-1}{p}\right) (p-1), \quad (6)$$

the formula (5) implies

$$\left(\frac{-1}{p}\right) = \sum_{n=1}^{p-1} \omega^n \sum_{i+j \equiv n} \left(\frac{i}{p}\right) \left(\frac{j}{p}\right)$$

or

$$-\left(\frac{-1}{p}\right) \sum_{n=1}^{p-1} \omega^n = \left(\frac{-1}{p}\right) = \sum_{n=1}^{p-1} \omega^n \sum_{i+j \equiv n} \left(\frac{i}{p}\right) \left(\frac{j}{p}\right).$$

Because $\{\omega^n\}_{n=1}^{p-1}$ is linearly independent over \mathbb{Q} , we must have

$$\sum_{i+j \equiv n} \binom{i}{p} \binom{j}{p} = - \binom{-1}{p} \quad (7)$$

for all $n \neq 0$.

The (ij) th entry of R^2 is equal to

$$\sum_{k=1}^p \binom{i-k}{p} \binom{k-j}{p} = \sum_{m+n \equiv i-j} \binom{m}{p} \binom{n}{p},$$

Therefore, due to (6) and (7), R^2 has entries $-\binom{-1}{p}$ everywhere except for $\binom{-1}{p}(p-1)$ on the main diagonal. Therefore $R^2 = -\binom{-1}{p}J + \binom{-1}{p}pI$, where I is the identity matrix and J is the matrix whose entries are all 1.

Because $W = -\binom{-1}{p}J + \binom{-1}{p}pI - I + 2S - S^2$ is circulant, we may calculate the eigenvalues of \overline{W} in the algebraic closure $\overline{\mathbb{Z}_q}$ of \mathbb{Z}_q in a similar way as for circulant matrices in \mathbb{Q} . We first assume that q is different from p . Then if we let $1, \pi, \pi^2, \dots, \pi^{p-1}$ denote the solutions to $x^p = 1$ in $\overline{\mathbb{Z}_q}$ we find that the eigenvalues of the circulant matrix with first column $(a_0, a_1, \dots, a_{p-1})^T$ will be

$$\lambda_i = \sum_{k=0}^{p-1} a_k \pi_q^{ki}, \quad (i = 1, \dots, p)$$

The eigenvalues of \overline{W} are therefore $\lambda_i = -\binom{-1}{p} \sum_{k=0}^{p-1} \pi^{ki} + \binom{-1}{p} p - 1 + 2\pi^i - \pi^{2i}$, which when $i \neq p$ can be rewritten as $\lambda_i = \binom{-1}{p} p - 1 + 2\pi^i - \pi^{2i}$ (as we know the sum of all solutions to $x^p - 1 = 0$ is 0). We know that the matrix \overline{W} has nullity at least 2 so $\lambda_i = 0$ for some $i \leq p$, i.e. there must be some $\theta = \pi^j$ such that

$$\theta^2 - 2\theta - \binom{-1}{p} p + 1 = 0. \quad (8)$$

We first consider the case $q = 2$. Because we assumed that $p \neq q$ we know that p is odd, so (8) reduces to

$$\theta^2 = 0,$$

which contradicts our assumption that θ satisfied $\theta^p = 1$. We assume herein that q is odd. Suppose that some $p-2$ columns of \overline{W} have a linear dependence. Write the dependency in the form $\sum_{i=1}^p n_i \overline{w}_i = \mathbf{0}$ where $n_i \in \mathbb{Z}_q$ and

two of the n_i are 0. The i th row of \overline{W} gives the following equation between the n_1, \dots, n_p

$$-\left(\frac{-1}{p}\right) \sum_{i=1}^p n_i + \left(\frac{-1}{p}\right) p n_i - n_i + 2n_{i+1} - n_{i+2} = 0, \quad (9)$$

and by taking the difference of the equations corresponding to two consecutive rows we have the equation

$$n_i - 3n_{i-1} + \left(3 - \left(\frac{-1}{p}\right)p\right) n_{i-2} + \left(\left(\frac{-1}{p}\right)p - 1\right) n_{i-3} = 0. \quad (10)$$

We may consider the p th row and 1st row as consecutive rows as well and in the recurrence relation (10) we can consider indices mod p , if we define $n_{i+p} = n_i$. When we consider this as a recurrence relation, the characteristic polynomial of the relation factors in $\overline{\mathbb{Z}_q}$ as

$$(x-1)(x^2 - 2x - \left(\frac{-1}{p}\right)p + 1) = (x-1)(x-\theta)(x-\alpha),$$

where θ is as in (8). We recap that $\theta^p = 1$. Then $n_i = A\alpha^i + B\theta^i + C$, as it may be easily shown that $1, \theta$ and α are all different. If we suppose $A \neq 0$, the requirement that $n_{i+p} = n_i$ forces $\alpha^p = 1$. Assume that both α and θ are of the form π^i and π^j respectively. Completing the square in (8) we have

$$\pi^i = 1 + \beta \quad \text{and} \quad \pi^j = 1 - \beta.$$

Where β satisfies $\beta^2 = \overline{\left(\frac{-1}{p}\right)p}$. Raising both of these equations to the power of p we obtain

$$(1 + \beta)^p - 1 = 0 \quad \text{and} \quad (1 - \beta)^p - 1 = 0. \quad (11)$$

Expanding these numbers as $c \pm d\beta$ with $c, d \in \mathbb{Z}_q$, the fact β is nonzero implies c and d are both 0. It should be noted that if β is not in \mathbb{Z}_q we have $c = d = 0$ from only one of these equations. In general, however, β may lie in \mathbb{Z}_q so the equation $c + d\beta = 0$ does not imply $c = d = 0$, and we need both equations to ensure this.

We may now construct a homomorphism

$$\varphi: \mathbb{Z} \left(\sqrt{\overline{\left(\frac{-1}{p}\right)p}} \right) \longrightarrow \mathbb{Z}_q(\beta)$$

defined by

$$\varphi: x + y\sqrt{\left(\frac{-1}{p}\right)} \mapsto \bar{x} + \bar{y}\beta$$

This may be routinely verified to be a homomorphism.

Due to (11) we must have

$$\varphi\left(\left(1 + \sqrt{\left(\frac{-1}{p}\right)} - 1\right)^p\right) = \bar{a} + \bar{b}\beta = 0,$$

from which, as noted above, both a and b in (1) must be divisible by q , which contradicts $\gcd(a, b) = p$.

In the case $A = 0$ we have $n_i = B\theta^i + C$. If $n_i = n_j = 0$ for some distinct i and j we have $B + C\theta^i = B + C\theta^j = 0$ which implies $B = C = 0$. However this contradicts the assumption that the dependence was nontrivial.

We now consider the case $q = p$. The recurrence relation (9) becomes

$$-\left(\frac{-1}{p}\right) \sum_{k=1}^p n_i - n_i + 2n_{i+1} - n_{i+2} = 0, \quad (12)$$

and the recurrence relation (10) in this case has characteristic polynomial $(x - 1)^3$. The latter has solution $n_i = A + Bi + Ci^2$. Firstly, we note that

$$\sum_{k=1}^p n_i = \sum_{k=1}^p (A + Bk + Ck^2) = 0.$$

Indeed, since $p \neq 2$, we have $\sum_{k=1}^p (A + Bk) = pA + \frac{1}{2}p(p+1)B = 0$. Also if β is any primitive element of \mathbb{Z}_p , then $\beta^{p-1} = 1$, and

$$\sum_{k=1}^p Ck^2 = C \sum_{i=0}^{p-2} \beta^{2i} = C \frac{\beta^{2p-2} - 1}{\beta^2 - 1} = 0,$$

where $\beta^2 \neq 1$, because $p > 3$. Therefore (12) becomes

$$n_i - 2n_{i+1} + n_{i+2} = 0,$$

and, substituting here $n_i = A + Bi + Ci^2$, we have $2C = 0$.

Therefore $n_i = A + Bi$, and so if n_i takes the value 0 twice we must have $A = B = 0$, and n_i must be identically 0, which implies the dependence is trivial. Therefore there are no $p - 2$ dependent columns of Q modulo q for any $q|D$, including $q = p$. \square

This gives us (ii) when combined with the following:

Lemma 2. For $p > 131$,

$$\text{intspan}\{\mathbf{u}_1, \dots, \mathbf{u}_p\} \cap T^p = \{\pm\mathbf{u}_1, \dots, \pm\mathbf{u}_p\}.$$

Proof. We know that the eigenvalues of Q are given by

$$\lambda_i = 1 - \omega^i + \sum_{k=0}^{p-1} \omega^{ki} \binom{k}{p} \quad (i = 1, \dots, p),$$

and because the sum here is just the Gauss sum τ , if $i \neq p$ (in which case $\lambda_p = 0$) we have

$$\lambda_i = 1 - \omega^i \pm \sqrt{\left(\frac{-1}{p}\right)p}.$$

It should be noted that $\lambda_i \neq 0$ for $i \neq p$, so so Q has rank $p - 1$. Denote by W the space spanned by the eigenvectors corresponding to nonzero eigenvalues of Q . Since these eigenvectors are of the form

$$\mu_i = (1, \omega^i, \omega^{2i}, \dots, \omega^{(p-1)i})^T, \quad i = 1, 2, \dots, p - 1,$$

where ω is a p th root of the unity, we have $W = \mathbf{n}^\perp$, where $\mathbf{n} = (1, \dots, 1)$ is the eigenvector belonging to 0. Because $|\lambda_i| \geq \sqrt{p} - 2$ for $i \neq p$, all $\mathbf{v} \in W$ satisfy

$$\|Q\mathbf{v}\| \geq (\sqrt{p} - 2)\|\mathbf{v}\|.$$

In general we may estimate $\|Q\mathbf{v}\|$ from below as

$$\|Q\mathbf{v}\| \geq (\sqrt{p} - 2)\|\mathbf{w}\|, \tag{13}$$

where $\mathbf{w} = \text{proj}_W(\mathbf{v})$.

If some $\mathbf{k} = (k_1, \dots, k_p) \in \mathbb{Z}^p$ satisfies $U\mathbf{k} \in T^p$ we have $\|U\mathbf{k}\| \leq \sqrt{p}$. Denote $\text{proj}_W(\mathbf{k})$ by $\mathbf{s} = (s_1, \dots, s_p)$. Because $\|U\mathbf{k}\|$ and $\|Q\mathbf{k}\|$ differ by at most $|k_1 - k_p|$ by the triangle inequality, we may combine this with (13) to obtain

$$\sqrt{p} + |k_1 - k_p| \geq (\sqrt{p} - 2)\|\mathbf{s}\| \tag{14}$$

The first and p th entries of \mathbf{s} differ by $k_1 - k_p$, so the sum of their absolute values is at least $|k_1 - k_p|$. By the arithmetic mean - quadratic mean inequality this implies $s_1^2 + s_p^2 \geq \frac{1}{2}|k_1 - k_p|^2$, and

$$\|\mathbf{s}\| \geq \frac{1}{\sqrt{2}}|k_1 - k_p|.$$

Combining this with (14) gives

$$\sqrt{p} + |k_1 - k_p| \geq (\sqrt{p} - 2) \frac{1}{\sqrt{2}} |k_1 - k_p|$$

or

$$\frac{\sqrt{2p}}{(\sqrt{p} - 2 - \sqrt{2})} \geq |k_1 - k_p|.$$

For $p > 131$ it may be shown this implies $|k_1 - k_p| \leq 1$. We may use a similar argument to show that $\|\text{proj}_N(\mathbf{k})\| \geq \frac{1}{\sqrt{2}} |k_i - k_j|$ for any i and j , so

$$\sqrt{p} + 1 \geq \frac{1}{\sqrt{2}} (\sqrt{p} - 2) |k_i - k_j|$$

(the 1 here arising from the estimate $|k_1 - k_p| \leq 1$). For $p > 100$ this implies $|k_i - k_j| \leq 1$ as before. We may therefore assume that some of the k_i are 0 and the rest 1. If there are m and ℓ of each, respectively, \mathbf{s} will have m entries equal to $\frac{-\ell}{p}$ and ℓ equal to $\frac{m}{p}$, and, since $m + \ell = p$,

$$\|\mathbf{s}\|^2 = \frac{m^2\ell + \ell^2m}{p^2} = \frac{m\ell}{p} = \frac{m(p-m)}{p}.$$

Since for $m = 1$ and $m = p - 1$ we obtain vectors of the form $\pm \mathbf{u}_i$, we may assume that $2 \leq m \leq p - 2$. The minimum value of $\|\mathbf{s}\|^2$ will be at $m = 2$ and $m = p - 2$, where it is $\frac{2(p-2)}{p}$. Therefore if there is to be a nontrivial vector in T^p , which is a linear combination of \mathbf{u}_i 's, by (14) we must have

$$(\sqrt{p} - 2) \sqrt{\frac{2(p-2)}{p}} \leq \sqrt{p} + 1,$$

which can be shown implies $p < 100$. Therefore for all $p > 131$, no non-trivial integral linear combinations of the \mathbf{u}_i are contained in T^p . \square

We may now check properties (i) and (iii) are satisfied. Because the bottom left principal minor of U is the same as that of Q , and it is known that this minor has nonzero determinant, U has rank $p - 1$. Therefore $\sum_{i=1}^p \mathbf{u}_i = \mathbf{0}$ is the only dependence among the columns of U . As (iii) is trivial, U satisfies all the requirements for the existence of a maximal cone.

4 Conclusion

Conder and Slinko [1] conjectured that $g(n) = n$ for all $n \geq 7$ but this hypothesis remains open. However, we believe that $g(n) = n$ for all sufficiently

large n for a number of reasons. First, the construction used here may be varied in a number of ways, so that even for irregular primes it is likely that we may find a matrix of the desired type. Secondly, we think that with some work our ideas could be extended to numbers with no small prime factors. It also seems reasonable that for large n the existence of such matrices should not depend upon number theoretical properties of n .

We note that it is also not known whether or not $f(n)$ can be greater than $g(n)$.

5 Acknowledgements

We would like to thank Sam McCall for conducting a computational check of the condition for primes as detailed above.

References

- [1] Conder, M.D.E., Slinko, A.M.: "A Counterexample to Fishburn's Conjecture," *Journal of Mathematical Psychology*, to appear.
- [2] Fishburn, P.C.: "Finite Linear Qualitative Probability," *Journal of Mathematical Psychology*, 40 (1996), 64-77.
- [3] Fishburn, P.C.: "Failure of Cancellation Conditions for Additive Linear Orders," *Journal of Combinatorial Design*, 5 (1997), 353-365.
- [4] de Finetti, B.: "Sul significato soggettivo della probabilità," *Fundamenta Mathematicae* 17 (1931), 298-329
- [5] Kraft, C.H., Pratt, J.W., and Siedenberg, A.: Intuitive Probability on Finite Sets," *Annals of Mathematical Statistics* 30 (1959), 408-419.
- [6] Ortega, J.M.: "Matrix Theory: a Second Course," New York, Plenum Press (1987), 242-245.
- [7] Ribenboim, P., "Classical Theory of Algebraic Numbers," New York, Springer-Verlag (2001), 70-72.