Available online at www.sciencedirect.com
ScienceDirect
Journal of Mathematical Psychology 51 (2007) 319–324
Journal of Mathematical Psychology
www.elsevier.com/locate/jmp

On the existence of extremal cones and comparative probability orderings

Simon Marshall

Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544, USA

Received 1 May 2006; received in revised form 2 February 2007
Available online 10 July 2007

Abstract

We study the recently discovered phenomenon [Conder, M. D. E., & Slinko, A. M. (2004). A counterexample to Fishburn's conjecture. *Journal of Mathematical Psychology*, *48*(6), 425–431] of existence of comparative probability orderings on finite sets that violate the Fishburn hypothesis [Fishburn, P. C. (1996). Finite linear qualitative probability. *Journal of Mathematical Psychology*, *40*, 64–77; Fishburn, P. C. (1997). Failure of cancellation conditions for additive linear orders. *Journal of Combinatorial Designs*, *5*, 353–365]—we call such orderings and the discrete cones associated with them extremal. Conder and Slinko constructed an extremal discrete cone on a set of $n = 7$ elements and showed that no extremal cones exist on a set of $n \leqslant 6$ 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 1725 of the 1842 primes between 132 and 16,000, hence for all these primes extremal cones exist.
© 2007 Elsevier Inc. All rights reserved.

Keywords: Comparative probability ordering; Discrete cones; Quadratic residues

1. Introduction

A comparative probability ordering on a finite set X of cardinality n is an order (any reflexive, complete and transitive binary relation) on the power set 2^X satisfying the following de Finetti's axiom (deFinetti, 1931): for any $A, B, C \subseteq X$

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

Without loss of generality, the set X can be assumed to be $\{1, 2, \ldots, n\}$ with $1 \succ 2 \succ \cdots \succ n$.

Comparative probability orderings are normally studied in terms of combinatorial objects associated with them called discrete cones (Conder & Slinko, 2004; Fishburn, 1996, 1997). We may represent a subset $A \subseteq X$ by an n-dimensional characteristic vector $\mathbf{v}_A$ whose ith 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 the following hold:

(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) $\{\mathbf{e}_1 - \mathbf{e}_2, \ldots, \mathbf{e}_{n-1} - \mathbf{e}_n, \mathbf{e}_n\} \subseteq C$, where $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ 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 $\mathbf{x} \in C \Longrightarrow \mathbf{x} \cdot \mathbf{n} \geqslant 0$, and representable if, in addition, $\mathbf{x} \cdot \mathbf{n} = 0 \Longleftrightarrow \mathbf{x} = \mathbf{0}$. 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. The concept of an

E-mail address: slm@math.princeton.edu

0022-2496/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jmp.2007.05.003

almost representable ordering was introduced in Kraft, Pratt, and Seidenberg (1959).

A central problem in the study of comparative probability orderings is deciding 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 $C_1, \ldots, C_k, \ldots$, developed by Kraft et al. (1959). A discrete cone C (and the corresponding comparative probability ordering) satisfies the mth cancellation condition C_m if there are no m non-zero vectors $\mathbf{x}_1, \ldots, \mathbf{x}_m \in C$ and positive integers $a_1, \ldots, a_m$ 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, Fishburn, (1996, 1997) defined a function $f(n)$ as the smallest number k such that the cancellation conditions $C_4, \ldots, C_k$ ensure that a probability ordering on an n element set is representable. Conder and Slinko (2004) introduced a similar function $g(n)$ which is the smallest number k such that the cancellation conditions $C_4, \ldots, C_k$ ensure that an almost representable order is representable. It is clear that $g(n) \leqslant f(n)$ and it is easy to show that $f(n) \leqslant n+1$ and $g(n) \leqslant n$. Fishburn proved that $f(5) = 4$ and $f(n) \geqslant n-1$. He conjectured that $f(n) = n-1$ for all $n \geqslant 5$. Conder and Slinko (2004) confirmed for $n = 6$ that $f(6) = g(6) = 5$, but also they disproved the hypothesis for $n = 7$ by showing that $g(7) = 7$.

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 $C_1, \ldots, C_{n-1}$ 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 $g(n) = n$, when n is a prime satisfying a certain condition. More exactly, we prove

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

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

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 *optimus* primes. The first few non-optimus primes are

$$3, 23, 31, 137, 191, 239, 277, 359, \ldots .$$

Our calculations show that 1725 of the 1842 primes between 132 and 16,000 are optimus 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 $\mathbf{p} = (p_1, \ldots, p_n)$ on the set $[n] = \{1, 2, \ldots, n\}$ with all p_i positive and distinct, such that the corresponding ordering of the power set $P[n]$ 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 3. The non-representable comparative probability ordering $\succeq$ on $P[5]$ constructed by Kraft et al. (1959) does not satisfy the condition C_4, since it contains the following comparisons:

$$\{1,3\} \succ \{2,4,5\},\ \{2,4\} \succ \{1,5\},\ \{2,5\} \succ \{3,4\},\ \{4,5\} \succ \{2\}. \tag{2}$$

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

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

This can be obtained from a representable but non-strict 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 (2004) clarified the conditions under which such a construction would work. Interchanging rows and columns in their theorem, we have the following:

Theorem 2 (*Conder and Slinko, 2004*). *Let $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_m\}$, $m \geqslant 4$, 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 $a_1, \ldots, a_m$, 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 $\mathbf{x}_1, \ldots, \mathbf{x}_m$ as its columns has the property that $\mathbf{p}U = \mathbf{0}$ for some positive integer-valued vector $\mathbf{p} = (p_1, \ldots, p_n)$ such that $p_1 > p_2 > \cdots > p_n > 0$ and $\sum_{i=1}^{n} p_i = 1$. Moreover,*

$$span\{\mathbf{x}_1, \ldots, \mathbf{x}_m\} \cap T^n = \{\pm\mathbf{x}_1, \ldots, \pm\mathbf{x}_m, \mathbf{0}\}. \tag{3}$$

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

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

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 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 $\mathbf{u}_1, \ldots, \mathbf{u}_p$ which has the following properties:

(i) The only dependence between the columns $\mathbf{u}_i$ is $\sum_{i=1}^{p} \mathbf{u}_i = \mathbf{0}$ (and its scalar multiples).
(ii) The only vectors in $\mathrm{col}(U) \cap T^p$ are $\pm\mathbf{u}_i$ and $\mathbf{0}$, where $\mathrm{col}(U)$ is the column space of U.
(iii) None of the $\mathbf{u}_k$ are 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 a 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 the columns of U we know that neither $\mathbf{e}_i$ nor $\pm\mathbf{e}_i \pm \mathbf{e}_j$ belongs to $\mathrm{Col}(U)$ for and i and j. This implies that $p_i \neq 0$ and $|p_i| \neq |p_j|$ for all $i \neq j$. If any of the 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, and so by permuting the rows of U we may assume that $p_1 > p_2 > \cdots > p_n > 0$. Finally $\mathbf{p}$ can be normalised so that $\sum_{i=1}^{n} p_i = 1$. Summarising we have the following:

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

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

in the first two co-ordinates as follows:

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

and then form a circulant matrix

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

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 non-trivial 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

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

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

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

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

Because Q and R are circulant, they lie in the one-generated subalgebra of the matrix algebra generated by S. Being in a one-generator subalgebra, any two circulant matrices commute. If A is a circulant matrix with first column $(a_0, a_1, \ldots, a_{p-1})^T$ then $A = \sum_{k=0}^{p-1} a_k S^k$. Let the pth roots of unity over $\mathbb{Q}$ be $1, \omega, \omega^2, \ldots, \omega^{p-1}$. Then these roots of unity are exactly the eigenvalues of S and, hence, the eigenvalues of A will be

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

(see also Ortega, 1987). We then know that the eigenvalues of Q are given by

$$\lambda_i = 1 - \omega^i + \sum_{k=0}^{p-1} \omega^{ki} \left(\frac{k}{p}\right) \quad (i = 1, \ldots, p).$$

These eigenvalues can be rewritten as

$$\begin{aligned} \lambda_i &= 1 - \omega^i + \left(\frac{i^{-1}}{p}\right) \sum_{k=0}^{p-1} \omega^{ki} \left(\frac{ki}{p}\right) \\ &= 1 - \omega^i + \left(\frac{i^{-1}}{p}\right) \sum_{k=0}^{p-1} \omega^{k} \left(\frac{k}{p}\right). \end{aligned}$$

Denote by τ the Gauss sum $\sum_{k=1}^{p-1} (\frac{k}{p}) \omega^k$. It is known (Ribenboim, 2001) that $\tau^2 = (\frac{-1}{p})p$, so if $i \neq p$ (as $\lambda_p = 0$) 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 Q has rank $p-1$. Denote by W the space spanned by the eigenvectors corresponding to non-zero eigenvalues of Q. Since these eigenvectors are of the form

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

where ω is a pth root of the unity, we have $W = \mathbf{n}^{\perp}$, where $\mathbf{n} = (1, \ldots, 1)$ is the eigenvector belonging to 0.

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

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

We will now prove that U satisfies properties (i)–(iii) given in Section 2. 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 other than $\pm\mathbf{u}_1,\ldots,\pm\mathbf{u}_n$ and $\mathbf{0}$. They will be proved in the following two lemmata.

Lemma 1. *If the condition of Theorem* 1 *is satisfied,*

$$col(U)\cap T^p \subset intspan\{\mathbf{u}_1,\ldots,\mathbf{u}_p\}.$$

Proof. We will make use here of the natural homomorphism

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

for a given prime q, 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 of the lemma, there must be some $a_i, b_i \in \mathbb{Z}$, for $i = 1,2,\ldots,p$, such that

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

Since $\mathbf{u}_1+\cdots+\mathbf{u}_p = \mathbf{0}$ 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 $\gcd(n_1,\ldots,n_p)$ is relatively prime to n, we may assume that it is not true that $n_1 = \cdots = n_p$ (otherwise $\mathbf{u} = \mathbf{0}$). As $n>1$, 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, since $\gcd(n_1,\ldots,n_p)$ is relatively prime 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 $\{\bar{\mathbf{u}}_1,\ldots,\bar{\mathbf{u}}_p\}$ 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 Q has row sum and column sum both equal to the zero vector, the formula describing how the determinant changes under row and column operations implies that all principal minors of Q 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, $\bar{Q}$ must have nullity at least 2, and because the sum of the rows of $\bar{Q}$ 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. Because any two circulant matrices commute, $R(I-S) = (I-S)R$ and $W = R^2-(I-S)^2$.

We may now calculate R^2 by expanding the identity $\tau^2 = (\frac{-1}{p})p$, where τ is the Gauss sum mentioned previously. We have

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

where the congruence in the subscript is modulo p. Since

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

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

$$\sum_{i+j\equiv n}\left(\frac{i}{p}\right)\left(\frac{j}{p}\right) = -\left(\frac{-1}{p}\right) \tag{7}$$

for all $n\neq 0$.

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

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

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

Because $W = -(\frac{-1}{p})J + (\frac{-1}{p})pI - I + 2S - S^2$ is circulant, we may calculate the eigenvalues of $\bar{W}$ in the algebraic closure $\bar{\mathbb{Z}}_q$ 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 $1, \pi, \pi^2, \ldots, \pi^{p-1}$ denote the solutions to $x^p = 1$ in $\bar{\mathbb{Z}}_q$ we find that the eigenvalues of the circulant matrix with first column $(a_0, a_1, \ldots, a_{p-1})^T$ will be

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

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

$$\theta^2 - 2\theta - \left(\frac{-1}{p}\right)p + 1 = 0. \tag{8}$$

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 from here on that q is odd. Suppose that some $p - 2$ columns of $\bar{W}$ have a linear dependence. Write the dependency in the form $\sum_{i=1}^{p} n_i \bar{\mathbf{w}}_i = \mathbf{0}$ where $n_i \in \mathbb{Z}_q$ and two of the n_i are 0. The ith row of $\bar{W}$ gives the following equation between the $n_1, \ldots, n_p$

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

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

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

We may consider the pth 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 $\bar{\mathbb{Z}}_q$ 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, θ 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 $\beta^2 = \overline{(\frac{-1}{p})p}$. Raising both of these equations to the power of p we obtain

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

Expanding these numbers as $c \pm d\beta$ with $c, d \in \mathbb{Z}_q$, the fact β is non-zero 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

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

defined by

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

This may be routinely verified to be a homomorphism.

Due to (11) we must have

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

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 non-trivial.

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

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

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 $q=p$. □

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

Lemma 2. *For $p>131$ satisfying the conditions of Theorem 1,*

$intspan\{\mathbf{u}_1,\ldots,\mathbf{u}_p\}\cap T^p=\{\pm\mathbf{u}_1,\ldots,\pm\mathbf{u}_p,\mathbf{0}\}$.

Proof. Recall that λ_i are the eigenvalues of Q, and $W=(1,\ldots,1)^{\perp}$ is the subspace spanned by eigenvectors of Q corresponding to non-zero eigenvalues. Because $|\lambda_i|\geqslant\sqrt{p}-2$ for $i\neq p$, all $\mathbf{v}\in W$ satisfy $\|Q\mathbf{v}\|\geqslant(\sqrt{p}-2)\|\mathbf{v}\|$. In general we may estimate $\|Q\mathbf{v}\|$ from below as

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

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

If some $\mathbf{k}=(k_1,\ldots,k_p)\in\mathbb{Z}^p$ satisfies $U\mathbf{k}\in T^p$ we have $\|U\mathbf{k}\|\leqslant\sqrt{p}$. Denote $\mathrm{proj}_W(\mathbf{k})$ by $\mathbf{s}=(s_1,\ldots,s_p)$. 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

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

The first and pth 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 $s_1^2+s_p^2\geqslant\frac{1}{2}|k_1-k_p|^2$, and

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

Combining this with 14 gives

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

or

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

For $p>131$ this implies $|k_1-k_p|\leqslant1$. We may use a similar argument to show that $\|\mathrm{proj}_N(\mathbf{k})\|\geqslant\frac{1}{\sqrt{2}}|k_i-k_j|$ for any i and j, so

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

(the 1 here arising from the estimate $|k_1-k_p|\leqslant1$). For $p>100$ this implies $|k_i-k_j|\leqslant1$ 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 $\frac{-l}{p}$ 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 $p-1$ we obtain vectors of the form $\pm\mathbf{u}_i$, we may assume that $2\leqslant m\leqslant p-2$. The minimum value of $\|\mathbf{s}\|^2$ will be at $m=2$ and $p-2$, where it is $\frac{2(p-2)}{p}$. Therefore, if there is to be a non-trivial vector in T^p, which is a linear combination of the $\mathbf{u}_i$'s, by (14) we must have

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

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. □

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 non-zero 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 (2004) conjectured that $g(n)=n$ for all $n\geqslant7$ 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 non-optimus primes it is likely that we may find a matrix of the desired type. Second, we think that with some work our ideas could be extended to numbers with no small prime factors. Third, computational checking of the matrices used here in cases where the primes are non-optimus has verified that the construction works for all primes between 7 and 23, and so we believe that this construction works for all primes. More general computational investigation has in fact proven that $g(n)=n$ for all n between 7 and 12.

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

Acknowledgment

We would like to thank Sam McCall for conducting a computational check of the condition for primes up to 16,000, and Marston Conder for checking that the matrices work for primes between 7 and 23, and that $g(n)=n$ for $7\leqslant n\leqslant12$, as detailed above.

References

Conder, M. D. E., & Slinko, A. M. (2004). A counterexample to Fishburn's conjecture. *Journal of Mathematical Psychology*, *48*(6), 425–431.

de Finetti, B. (1931). Sul significato soggetivo della probabilitiá. *Fundamenta Mathematicae*, *17*, 298–329.

Fishburn, P. C. (1996). Finite linear qualitative probability. *Journal of Mathematical Psychology*, *40*, 64–77.

Fishburn, P. C. (1997). Failure of cancellation conditions for additive linear orders. *Journal of Combinatorial Designs*, *5*, 353–365.

Kraft, C. H., Pratt, J. W., & Seidenberg, A. (1959). Intuitive Probability on Finite Sets. *Annals of Mathematical Statistics*, *30*, 408–419.

Ortega, J.M. (1987). Matrix theory: A second course pp. 242–245, New York: Plenum Press.

Ribenboim, P. (2001) Classical theory of algebraic numbers. pp. 70–72, New York: Springer.