DIMACS Technical Report 99-40

Camel Sequences and Quadratic Residues

by

V. Gurvich[1]
DIMACS and RUTCOR, Rutgers University, NJ
(gurvich@rutcor.rutgers.edu)
on leave from the International Institute of
Earthquake Prediction Theory and Mathematical Geophysics,
Russian Academy of Sciences

Li Sheng
Dept. of Mathematics and Computer Science
Drexel University, PA, (lsheng@mcs.drexel.edu)

[1]The first author gratefully acknowledge the support of DIMACS and Office of Naval Research (Grant N00014-92-J-1375)

ABSTRACT

Given an even cyclic $(+1,-1)$ sequence $s=(s_0,...,s_{2n-1})$ which consists of n plus ones and n minus ones, let us compute $i+j$ $(mod\ 2n)$ for all n^2 $(+1,-1)$-pairs (s_i,s_j) and distribute obtained n^2 numbers between $2n$ "boxes" $1,2,...,2n-1,2n=0$ $(mod\ 2n)$. The average cardinality of a box is $\frac{n^2}{2n}=\frac{n}{2}$. Some sequences have quite remarkable box-distributions, "almost average everywhere with two big humps". For example,

$n=5,\ s=(+1+1-1-1+1-1+1-1-1+1),\ B=(3333133330)=(3^4 1\, 3^4 0)$;

$n=7,\ s=(+1+1+1-1+1-1-1-1+1+1-1+1-1-1),\ B=(33333363333337)=(3^6 6\, 3^6 7)$. In general, given an *odd* n, the box-distributions $(\lfloor\frac{n}{2}\rfloor^{n-1}\ (n-1)\ \lfloor\frac{n}{2}\rfloor^{n-1}\ n)$ and $(\lceil\frac{n}{2}\rceil^{n-1}\ 1\ \lceil\frac{n}{2}\rceil^{n-1}\ 0)$ as well as the sequences, which generate them, will be called the *camel distributions* and *camel sequences*, respectively *up-camel* and *down-camel.* For example, the first sequence above is down-camel, and the second one is up-camel. Camel sequences have applications in extremal graph theory. Here we prove that there are infinitely many 'camels' of both types. More precisely, for every prime $n=4j-1$ we construct an up-camel sequence and for every prime $n=4j+1$ a down-camel one. In both cases these sequences are related to quadratic residues and non-residues modulo n. We conjecture that there are no other camel sequences.

Key Words: *quadratic residues, camel sequences, maximin, minimax, extremal graph theory, vertex-enumerated graphs.*

1 Introduction

Given an even cyclic $(+1,-1)$-sequence $s=(s_0,...,s_{2n-1})$ which consists of n plus ones and n minus ones, let us compute $i+j \ (mod\, 2n)$ for all n^2 $(+1,-1)$-pairs (s_i,s_j) and distribute obtained n^2 numbers between $2n$ "boxes" $1,2,...,2n-1,2n=0 \ (mod\, 2n)$. Obviously, the average cardinality of a box is $\frac{n^2}{2n}=\frac{n}{2}$. Some sequences have quite remarkable box-distributions, "almost average everywhere with two big humps". For example,

$n=3,\ s=(+\ +\ -\ -\ +-),\ B=(112113)=(1^2 2\ 1^2 3),$

$n=7,\ s=(+\ ++-\ +--\ -\ ++-\ +--),\ B=(33333363333337)=(3^6 6\ 3^6 7),$

$n=11,\ s=(+\ +-+++---+-\ -\ +-+++---+-),\ B=(5^{10}10\ 5^{10}11);$

$n=5,\ s=(+\ +--+\ -\ +-\ -+),\ B=(3333133330)=(3^4 1\ 3^4 0),$

$n=13,\ s=(+\ +-++--\ --++-+\ -\ +-++--\ --++-+),\ B=(7^{12}1\ 7^{12}0),$

$n=17,\ s=(+\ ++-+---+\ +---+-++\ -\ ++-+---+\ +---+-++),\ B=(9^{16}1\ 9^{16}0).$

For simplicity we write just $(+)$ instead of $(+1)$ and $(-)$ instead of (-1). In general, given an *odd* n, the box-distributions $(\lfloor\frac{n}{2}\rfloor^{n-1}\ (n-1)\ \lfloor\frac{n}{2}\rfloor^{n-1}\ n)$ and $(\lceil\frac{n}{2}\rceil^{n-1}\ 1\ \lceil\frac{n}{2}\rceil^{n-1}\ 0)$ as well as the generating sequences will be called the *camel distributions* and *camel sequences*, respectively *up-camel* and *down-camel*. In the examples above the first three sequences are up-camel and the last three are down-camel. We will prove that there are infinitely many camel sequences of each type. More precisely, for every prime $n=4k-1$ we construct an up-camel sequence and for every prime $n=4k+1$ a down-camel one. It is known that there exist infinitely many primes of each type. In both cases the camel sequences are related to quadratic residues and non-residues modulo n. In section 2 we recall some basic properties of quadratic residues we will need, for more details see for example [4], chapter 5. In section 3 we define camel sequences related to quadratic residues and in sections 4,5,6 we consider applications of camel sequences in extremal graph theory.

2 Quadratic residues

Given an odd prime p and an $a \neq 0\ (mod\ p)$, the number a is a *quadratic residue modulo* p if $a = b^2\ (mod\ p)$ for some b, otherwise a is called a *quadratic non-residue.* By the definition, the *Legendre symbol* $(a|p) = +1$ in the first case, $(a|p) = -1$ in the second one and $(a|p) = 0$ for $a = 0\ (mod\ p)$. The Legendre symbol is multiplicative: $(ab|p) = (a|p)(b|p)$. Further, $(a|p) = a^{\frac{p-1}{2}}\ (mod\ p)$. In particular, $(-1|p) = (-1)^{\frac{p-1}{2}}\ (mod\ p)$. In other words, if $p = 1\ (mod\ 4)$ then $(-1|p) = 1$ and $(a|p) = (p-a|p)$ (*symmetric*) for all a, that is a is a quadratic residue iff $p - a$ is a quadratic residue; if $p = -1\ (mod\ 4)$ then $(-1|p) = -1$ and $(a|p) = -(p-a|p)$ (*skew symmetric*) for all a, that is a is a residue iff $p-a$ is a non-residue. For every odd prime p there are exactly $\frac{p-1}{2}$ residues and the same number of non-residues between the numbers $\{1, ..., p-1\}$. For $p = 3, 5, 7, 11, 13, 17$ the corresponding $(+1, -1)$-sequences are $(+\,-), (+-\ \ -+), (++-\ \ +--), (+-+++\ \ ---+-), (+-++--\ \ --++-+), (++-+---+\ \ +---+-++)$.

Lemma 1 *The following equalities hold*

$$\sum_{i=1}^{p-1}(i(k+i)|p) = \begin{cases} -1 & \textit{if } k \neq 0\ (mod\ p), \\ p-1 & \textit{if } k = 0\ (mod\ p). \end{cases} \tag{1}$$

$$\sum_{i=1}^{p-1}(i(k-i)|p) = \begin{cases} -(-1|p) & \text{if } k \neq 0\ (mod\ p), \\ (p-1)(-1|p) & \text{if } k = 0\ (mod\ p) \end{cases} = \begin{cases} +1 & \text{if } p = -1\ (mod\ 4),\ k \neq 0\ (mod\ p), \\ -1 & \text{if } p = +1\ (mod\ 4),\ k \neq 0\ (mod\ p), \\ p-1 & \text{if } p = +1\ (mod\ 4),\ k = 0\ (mod\ p), \\ 1-p & \text{if } p = -1\ (mod\ 4),\ k = 0\ (mod\ p). \end{cases} \tag{2}$$

Proof of the first equality can be found in [4], see problem 8a of chapter 5. In case $k \neq 0\ (mod\ p)$ let us multiply each term $(i(k+i)|p) = (i|p)(k+i|p)$ by $(i'^2|p) = (i'|p)^2 = 1$, where i' is defined by equality $ii' = 1\ (mod\ p)$. We get $(i'^2|p)(i|p)(k+i|p) = (ii'|p)(ki'+ii'|p) = (ki'+1|p)$. Obviously, $ki'+1$ takes all the values $1, ..., p-1\ (mod\ p)$ except 1, because $k \neq 0\ (mod\ p)$. Thus in this case the first sum equals (-1). If $k = 0\ (mod\ p)$ then each term of the sum equals $(i^2|p) = 1$ by the definition, and the sum equals $p - 1$.

The second equality of the Lemma can be proved analogously but it is even simpler to derive the second one from the first one by just multiplying both parts of the latter by $(-1|p)$. □

3 Camel sequences related to quadratic residues

Fixed an odd prime p, let us consider circular sequence $s = ((1|p), (2|p), ..., (p-1|p), (p|p))$ of length p which contains $\frac{p-1}{2}$ plus ones (residues), $\frac{p-1}{2}$ minus ones (non-residues) and 1 zero $(p|p)$. And let $B = B(s)$ be the box-distribution of $\frac{(p-1)^2}{4}$ $(+1,-1)$-pairs of s between p boxes: $1, 2, ..., p-1, p = 0\ (mod\ p)$.

Proposition 1 *The box-distribution of s is given by formula:*

$$B = \begin{cases} (\frac{p-1}{4})^{p-1}\ 0 & \textit{if } p = +1\ (mod\ 4), \\ (\frac{p-3}{4})^{p-1}\ \frac{p-1}{2} & \textit{if } p = -1\ (mod\ 4). \end{cases}$$

In both cases the sum is $\frac{(p-1)^2}{4}$. For example, if $p = 11$ then $s = (+-+++---+-\ 0)$ and $B = (2^{10}\ 5)$; if $p = 13$ then $s = (+-++--\ --++-+\ 0)$ and $B = (3^{12}\ 0)$. We will call such sequences and distributions "one-hump camel", respectively up- and down-.

Proof immediately follows from the second formula of Lemma 1. Indeed, cardinality b_k in B equals $(\frac{1}{2})\sum_{i=0}^{p-1} f(i(k-i)|p)$ where $f(0) = f(+1) = 0$ and $f(-1) = 1$. □

For example if $p = 13, k = 5$ then the pairs $(i,(k-i))$ take values $(1,4), (0,5), (12,6), (11,7), (10,8), (9,9)$ and $f(9 \times 9|13) = f(+1) = 0$.

However, 'one-hump camel sequence' $((1|p), (2|p), ..., (p-1|p), (p|p))$ contains a zero, the last element $(p|p) = 0$. To get rid of this 0 let us consider a longer sequence $s = ((+1)r(-1)r)$ where $r = ((1|p), (2|p), ..., (p-1|p))$. As usual, p is an odd prime, and r is the sequence of residues and non-residues modulo p. r contains $\frac{p-1}{2}$ plus ones and $\frac{p-1}{2}$ minus ones, thus sequence s contains p plus ones and p minus ones.

Theorem 1 *Box-distribution of sequence $s = ((+1)r(-1)r)$ is given by formulae:*

$$B = \begin{cases} (\frac{p+1}{2})^{p-1}\ 1(\frac{p+1}{2})^{p-1}\ 0 & \text{if } p = +1\ (mod\ 4), \\ (\frac{p-1}{2})^{p-1}\ (p-1)(\frac{p-1}{2})^{p-1}\ p & \text{if } p = -1\ (mod\ 4), \end{cases}$$

which defines the down-camel and up-camel distributions, respectively.

In both cases the sum is p^2, because the total number of $(+,-)$ pairs is p^2. For example, if $p = 5$ then $s = (+\ + - \ - + \ - \ + - \ -+)$ and $B = (3^4\ 1\ 3^4\ 0)$; if $p = 7$ then $s = (+\ + + - + - - \ - \ + + - + --)$ and $B = (3^6\ 6\ 3^6\ 7)$.

Proof . We will need a few definitions and simple Lemmas for the proof of this theorem.

An *edge* is an unordered pair (i, j), and it is *degenerated* if $i = j$. We assume that the edges are undirected, respectively the pairs are unordered, that is $(i, j) = (j, i)$. Two edges (which may be degenerated) $e = (i, j)$ and $e' = (i', j')$ are called *parallel* if $i+j = i'+j'\ (mod\, 2p)$. Let us note that if two different edges $e = (i, j)$ and $e' = (i', j')$ are parallel then $\{i, j\} \cap \{i', j'\} = \emptyset$. Let U_k be the set of all edges (i, j) such that $i, j \in [0, 2p)$ and $i + j = k\ (mod\ 2p)$, and let B_k (box k) be the set of all non-degenerated edges in U_k. We want to compute b_k, which is the number of non-degenerated edges (i, j) in box k, such that $s_i \cdot s_j = -1$, that is $(s_i, s_j) = (+,-)$ *or* $(-,+)$. Let us first solve the system

$$U_k = \{(i, j) \in [0, 2p) : i + j = k\ (mod\ 2p)\}$$

We will often use the inequalities:

$$\lfloor \frac{k}{2} \rfloor \le p - 1\ \ for\ \ k \in [0, 2p) \tag{3}$$

$$0 < \lfloor \frac{k}{2} \rfloor + 1 \le p \le \lfloor \frac{k}{2} \rfloor + p \le 2p - 1\ \ for\ \ k \in [0, 2p) \tag{4}$$

To give one expression for both B_k and U_k let us introduce the notation

$$A_k = \bigcup_{j=\lfloor \frac{k}{2} \rfloor+1}^{\lfloor \frac{k}{2} \rfloor+p} \{(i,j) : i = (k-j)\ (mod\ 2p), i \in [0,2p)\}.$$

Lemma 2 *For any $k \in [0,2p)$*

1. $A_k \subseteq U_k$*, and* $|A_k| = p$.
2. $$A_k = \begin{cases} U_k = B_k & \text{if } k \text{ is odd} \\ U_k - \{(\frac{k}{2}, \frac{k}{2})\} = B_k \bigcup \{(\frac{k}{2}+p, \frac{k}{2}+p)\} & \text{if } k \text{ is even} \end{cases}$$

Proof (1) If $(i,j) \in A_k$ then, by equation (4), $j \in [0,2p)$, and $(i,j) \in U_k$. This means that $A_k \subseteq U_k$. To see that $|A_k| = p$, we need just to note that for each $j \in [0,2p)$ there exists a unique $i \in [0,2p)$, such that $i = k-j\ (mod\ 2p)$.

(2) If (i,j) and (i',j') are two different edges from B_k then they are parallel, and all four numbers i,j,i',j' are different, because B_k has no degenerated edges. Let m be the number of edges in B_k.

If k is odd then U_k has no degenerated edges and $B_k = U_k$. In this case the ends of the m non-degenerated edges form a set of $2m$ different numbers from $[0,2p)$. Thus $2m \leq 2p$, which implies $m \leq p$. Now $A_k \subseteq U_k$ and $|A_k| = p$ imply the result.

If k is even, then $(\frac{k}{2}, \frac{k}{2})$ and $(\frac{k}{2}+p, \frac{k}{2}+p)$ are the only two degenerated edges in U_k, hence $B_k = U_k - \{(\frac{k}{2}, \frac{k}{2}), (\frac{k}{2}+p, \frac{k}{2}+p)\}$. Moreover, the end points of the m non-degenerated edges of B_k form a set of $2m$ numbers in $[0,2p) - \{\frac{k}{2}\} - \{\frac{k}{2}+p\}$. Thus $2m \leq 2p-2$, which implies that $m \leq p-1$. Now $A_k \subseteq U_k - \{(\frac{k}{2}, \frac{k}{2})\}$ and $|A_k| = p$ imply the result. $\square$

For any given prime p let us generate the sequence $r = ((1|p), (2|p), \cdots, (p-1|p))$, and represent the cyclic sequence $s = ((+1)r(-1)r)$ of length $2p$ in the vertices of a perfect $2p$-gon; see for example Figure 1 and Figure 2, where B_k consists of all parallel non-degenerated edges perpendicular to the dotted line labeled by k, and A_k is B_k plus one degenerated edge represented by the dashed line, and U_k is B_k plus two degenerated edges.

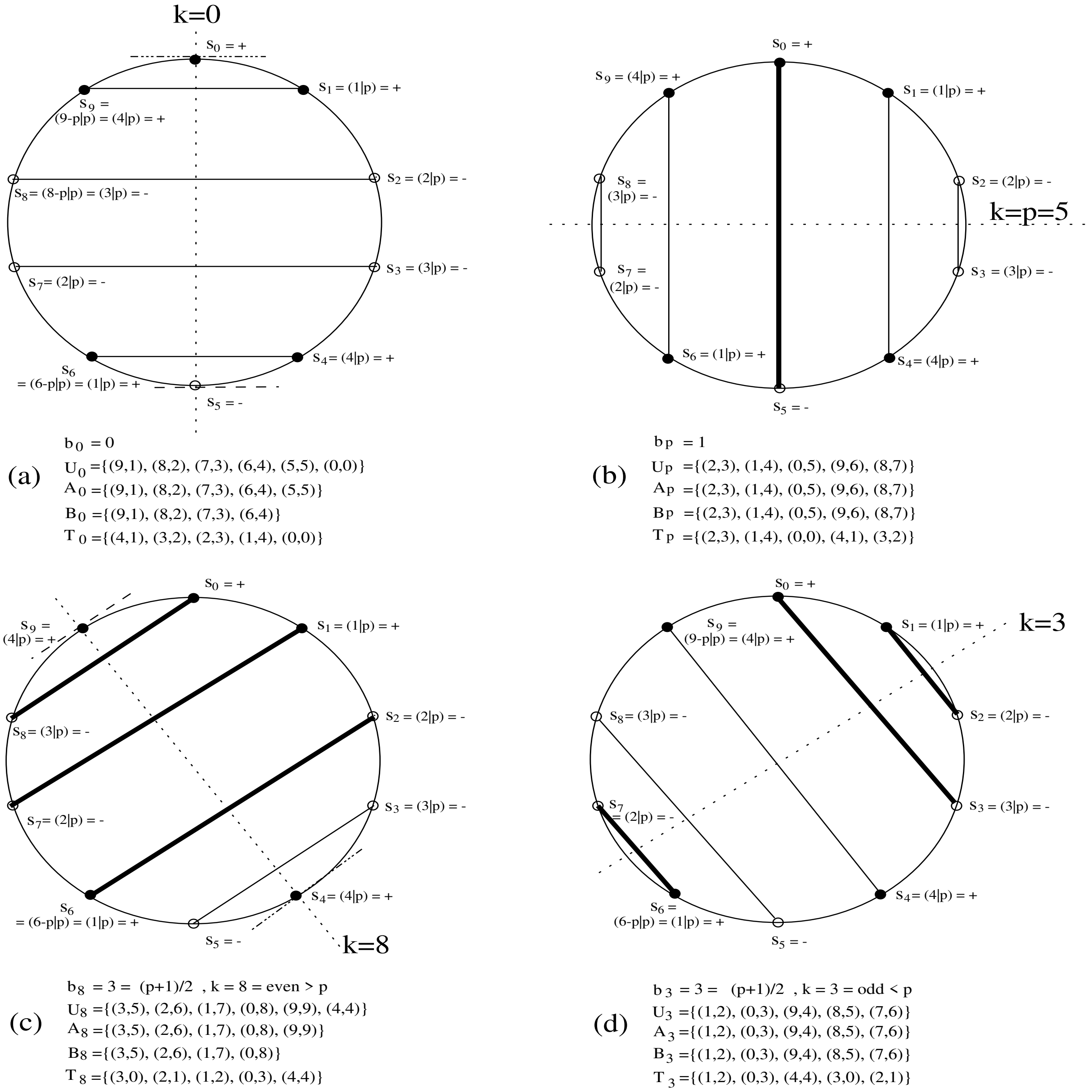


Figure 1: For prime number $p = 5 = 1\ (mod\ 4)$, $r = ((1|p), (2|p), (3|p), (4|p)) = (+--+)$ is symmetric. The box B_k is shown for $k = 0, 5, 3, 8$. The empty circles and the dark ones correspond to $-$ and $+$ respectively. The thick lines represent the $(+,-)$-edges in the box B_k. We get up-camel distribution $(0\ 3^4\ 1\ 3^4)$.

Given sequences $r = ((1|p), (2|p), \cdots, (p-1|p))$ and $s = ((+1)r(-1)r)$, we want to find b_k, the number of edges in B_k for which $s_i \cdot s_j = -1$. For degenerated edges $(i = j)$ and $s_i \cdot s_j = s_i^2 = +1$, thus they do not contribute to b_k. Whence, b_k is the number of pairs (i,j) in A_k for which $s_i \cdot s_j = -1$. In fact, $b_k = -\frac{1}{2}\sum_{(i,j)\in A_k}(s_i s_j - 1) = \frac{p}{2} - \frac{1}{2}\sum_{(i,j)\in A_k} s_i s_j$, and we need to compute $\sum_{(i,j)\in A_k} s_i s_j$.

Let us note that s_i is defined in a peculiar way for $i = 0$ and p. Let A_k^* be the set of all the special edges in A_k for which at least one end being 0 or p. It is easy to see that

Lemma 3 *For any $k \in [0, 2p)$ we obtain*

$$\sum_{(i,j)\in A_k^*} s_i s_j = \begin{cases} s_p^2 = 1 & \textit{if } k = 0 \\ s_0 \cdot s_p = -1 & \textit{if } k = p \\ s_0 s_k + s_p s_k = 0 & \textit{otherwise} \end{cases}$$

Proof All edges in A_k^* are parallel, hence $|A_k^*| \leq 2$. Further, $(0,k) \in A_k^*$ if and only if $k \neq 0$. Inclusions $(k+p, p) \in A_k^*$ if $k < p$ and $(k-p, p) \in A_k^*$ if $k \geq p$ imply

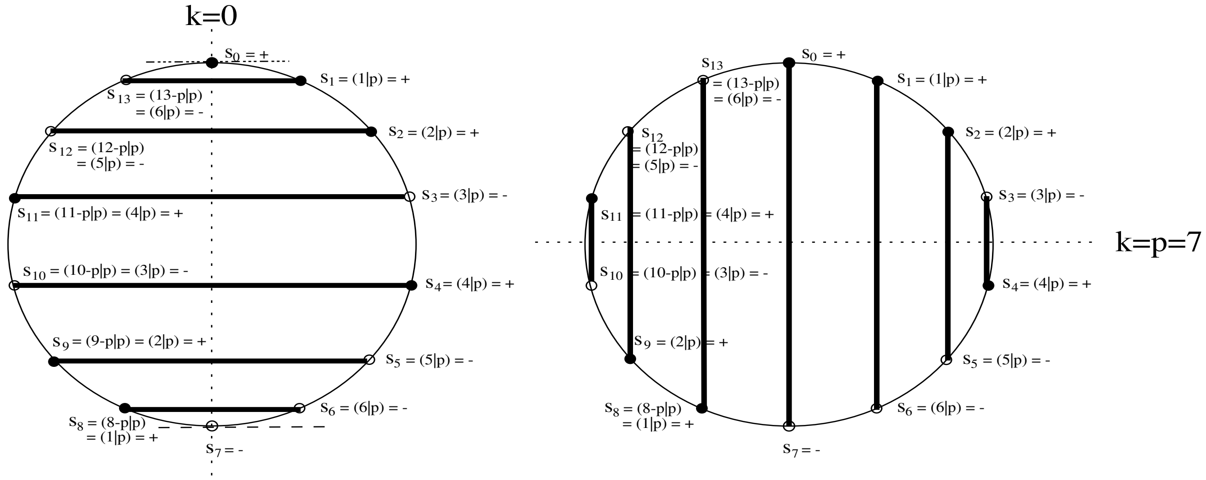
$$A_k^* = \begin{cases} \{(p,p)\} & \text{if } k = 0, \\ \{(0,k), (k+p,p)\} & \text{if } 0 < k < p, \\ \{(0,p)\} & \text{if } k = p, \\ \{(0,k), (k-p,p)\} & \text{if } k > p. \end{cases}$$

Now the equalities $s_{k+p} = s_k = (k|p)$ if $k < p$, $s_{k-p} = s_k = (k-p|p)$ if $k \geq p$ and $s_0 = 1, s_p = -1$ imply the result. □

For any $i \in [0, 2p)$ except for $i = 0$ and $i = p$, we get $s_i = (t_i|p)$, where

$$t_i = i \ (mod\ p) = \begin{cases} i & \text{if } 0 \leq i < p, \\ i - p & \text{if } p \leq i < 2p. \end{cases}$$

Proof of Theorem 1. Any p consecutive numbers from $[0, 2p)$ are all different modulo p. Hence $j \in [\lfloor \frac{k}{2} \rfloor + 1, \lfloor \frac{k}{2} \rfloor + p]$ implies that t_j takes values $0, 1, \cdots, p-1$. Further, for any $i, j \in [0, 2p)$ the implication $i + j = k \ (mod\ 2p) \ \Rightarrow \ t_i + t_j = k \ (mod\ p)$ holds. Hence (t_i, t_j) takes all the values from



(a)

$b_0 = 6 = p-1$

$U_0 = \{(13,1), (12,2), (11,3), (10,4), (9,5), (8,6), (7,7), (0,0)\}$

$A_0 = \{(13,1), (12,2), (11,3), (10,4), (9,5), (8,6), (7,7)\}$

$B_0 = \{(13,1), (12,2), (11,3), (10,4), (9,5), (8,6)\}$

$T_0 = \{(6,1), (5,2), (4,3), (3,4), (2,5), (1,6), (0,0)\}$

(b)

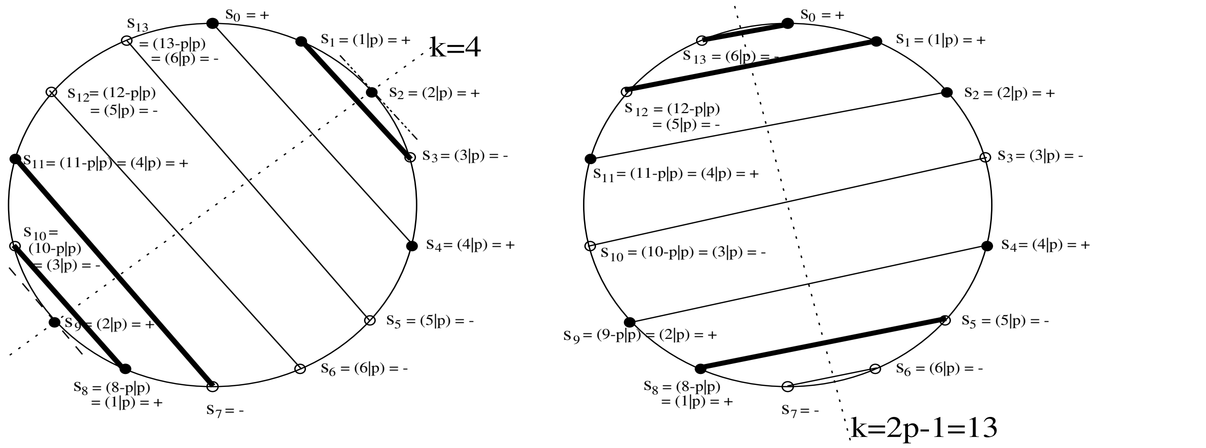
$b_p = 7 = p$

$U_p = \{(3,4), (2,5), (1,6), (0,7), (13,8), (12,9), (11,10)\}$

$A_p = \{(3,4), (2,5), (1,6), (0,7), (13,8), (12,9), (11,10)\}$

$B_p = \{(3,4), (2,5), (1,6), (0,7), (13,8), (12,9), (11,10)\}$

$T_p = \{(3,4), (2,5), (1,6), (0,0), (6,1), (5,2), (4,3)\}$



(c)

$b_4 = 3 = (p-1)/2$, $k = 4 =$ even $< p$

$U_4 = \{(1,3), (0,4), (13,5), (12,6), (11,7), (10,8), (9,9), (2,2)\}$

$A_4 = \{(1,3), (0,4), (13,5), (12,6), (11,7), (10,8), (9,9)\}$

$B_4 = \{(1,3), (0,4), (13,5), (12,6), (11,7), (10,8)\}$

$T_4 = \{(1,3), (0,4), (6,5), (5,6), (4,0), (3,1), (2,2)\}$

(d)

$b_{13} = 3 = (p-1)/2$, $k = 13 =$ odd $> p$

$U_{13} = \{(13,0), (12,1), (11,2), (10,3), (9,4), (8,5), (7,6)\}$

$A_{13} = \{(13,0), (12,1), (11,2), (10,3), (9,4), (8,5), (7,6)\}$

$B_{13} = \{(13,0), (12,1), (11,2), (10,3), (9,4), (8,5), (7,6)\}$

$T_{13} = \{(6,0), (5,1), (4,2), (3,3), (2,4), (1,5), (0,6)\}$

Figure 2: For prime number $p = 7 = 3 \ (mod\ 4)$, $r = ((1|p), (2|p), (3|p), (4|p), (5|p), (6|p)) = (++-+--)$ is skew-symmetric. The box B_k is shown for $k = 0, 7, 4, 13$, where the empty circles and the dark ones correspond to $-$ and $+$ respectively. The thick lines represent the $(+,-)$-edges in the box B_k. We get down-camel distribution $(6\ 3^4\ 7\ 3^4)$.

$$T_k = \bigcup_{j=0}^{p-1} \{(i,j) : i+j = k \ (mod\ p), i \in [0,p)\}$$

while (i,j) run all edges of A_k. Here the pairs (t_i, t_j) and (t_j, t_i) from T_k are different. Thus

$$\begin{aligned}
\textstyle\sum_{(i,j)\in A_k - A_k^*} s_i s_j &= \textstyle\sum_{(i,j)\in A_k - A_k^*} (t_i t_j | p) \\
&= \textstyle\sum_{(i,j)\in A_k} (t_i t_j | p) \quad ((t_i|p)(t_j|p) = 0 \text{ if } (i,j) \in A_k^*) \\
&= \textstyle\sum_{j=0}^{p-1} ((k-j)j|p) = \sum_{j=1}^{p-1} ((k-j)j|p)
\end{aligned}$$

It follows from Lemma 3 and the second formula of Lemma 1 that

$$\begin{aligned}
\textstyle\sum_{(i,j)\in A_k} s_i s_j &= \textstyle\sum_{(i,j)\in A_k - A_k^*} s_i s_j + \sum_{(i,j)\in A_k^*} s_i s_j = \\
&= \begin{cases}
(p-1)+1 = p & \text{if } p = 1\ (mod\ 4),\ k = 0, \\
(p-1)+(-1) = p-2 & \text{if } p = 1\ (mod\ 4),\ k = p, \\
-1 & \text{if } p = 1\ (mod\ 4),\ k \neq 0\ (mod\ p), \\
(1-p)+1 = 2-p & \text{if } p = -1\ (mod\ 4),\ k = 0, \\
(1-p)+(-1) = -p & \text{if } p = -1\ (mod\ 4),\ k = p, \\
1 & \text{if } p = -1\ (mod\ 4),\ k \neq 0\ (mod\ p).
\end{cases}
\end{aligned}$$

$$\begin{aligned}
b_k &= -\tfrac{1}{2} \textstyle\sum_{(i,j)\in A_k} (s_i s_j - 1) = \frac{p}{2} - \frac{1}{2} \sum_{(i,j)\in A_k} s_i s_j = \\
&= \begin{cases}
0 & \text{if } p = 1\ (mod\ 4),\ k = 0, \\
1 & \text{if } p = 1\ (mod\ 4),\ k = p, \\
\frac{p+1}{2} & \text{if } p = 1\ (mod\ 4),\ k \neq 0, p, \\
p-1 & \text{if } p = -1\ (mod\ 4),\ k = 0, \\
p & \text{if } p = -1\ (mod\ 4),\ k = p, \\
\frac{p-1}{2} & \text{if } p = -1\ (mod\ 4),\ k \neq 0, p,
\end{cases}
\end{aligned}$$

$\square$

Remark 1 In fact, b_k can be easily derived for $k = 0$ or p as follows:

If $p = 1\ (mod\ 4)$, then $(j|p) = (p-j|p)$ (symmetric case) and

$$b_k = \begin{cases}
0 & \text{if } k = 0 \text{ (since } s_i = s_j \text{ for each } (i,j) \in B_0) \\
1 & \text{if } k = p \text{ (since } s_i = s_j \text{ for each } (i,j) \neq (0,p) \text{ in } B_p\text{; and } s_0 = -s_p \text{ for } (0,p) \in B_p)
\end{cases}$$

If $p = -1(mod\ 4)$ then $(j|p) = -(p-j|p)$ (skew-symmetric case) and by Lemma 2 we get

$$b_k = \begin{cases} p-1 & \text{if } k=0 \text{ (since } s_i = -s_j \text{ for each } (i,j) \in B_0, \text{ and since 0 is even, } |B_0| = p-1;) \\ p & \text{if } k=p \text{ (since } s_i = -s_j \text{ for each } (i,j) \in B_0, \text{ and since } p \text{ is odd, } |B_p| = p) \end{cases}$$

Using the same arguments as in the proof of Theorem 1 and the second formula of Lemma 1 for any odd prime p we get $\sum_{(i,j)\in A_k - A_k^*} s_i s_j = \sum_{j=1}^{p-1}((k-j)j|p)$ and thus b_k is constant for all k except $k=0$ and $k=p$. Since the total number of edges ($\sum b_k$) in all the $2p$ boxes is p^2, we get

$$b_k = \begin{cases} \frac{p^2-b_0-b_p}{2p-2} = \frac{p^2-0-1}{2p-2} = \frac{p+1}{2} & \text{if } p = 1\ (mod\ 4), \text{ and } k \neq 0, p; \\ \frac{p^2-b_0-b_p}{2p-2} = \frac{p^2-(p-1)-p}{2p-2} = \frac{p-1}{2} & \text{if } p = -1\ (mod\ 4), \text{ and } k \neq 0, p. \end{cases}$$

This is another way to prove Theorem 1.

Figures 1 and 2 show the box distributions for $p = 5 = 1\ (mod\ 4)$ and $p = 7 = -1\ (mod\ 4)$, respectively. In the first case the sequence $r = (+--+)$ is symmetric. Hence $b_0 = 0$, because there are no $(+,-)$ edges in the box $k = 0$, and $b_p = 1$, because there is only one $(+,-)$ edge $(0,p)$ in the box $k = p$. And $b_k = 3 = \frac{p+1}{2}$ for all other $k|k \neq 0, k \neq p$. In the second case the sequence $r = (++-+--)$ is skew symmetric. Hence $b_0 = p - 1 = 6$, because all $p-1$ the edges in the box $k = 0$ are $(+,-)$-edges, and $b_p = p = 7$, because all p edges in box $k = p$ are $(+,-)$-edges. And $b_k = 3 = \frac{p-1}{2}$ for all other $k|k \neq 0, k \neq p$.

4 Applications of camel sequences

Given a graph $G = (V,E)$ without loops and multiple edges ($|V| = n, |E| = m$) and an integer $N \geq n$, let us enumerate the vertices by different numbers from $[N] = \{1, ..., N\}$, or in other words, let us consider an injective mapping $f : V \to [N]$. Given such an f, we will call two different edges $e_1 = v_1v_1', e_2 = v_2v_2' \in E$ *parallel* if $f(v_1)+f(v_1') = f(v_2)+f(v_2')\ (mod\ N)$. All four vertices must be different. There are N sets (bunches) of parallel edges enumerated by $1, 2, ..., N-1, N = 0\ (mod\ N)$. Let us denote by $B(G,N,f) = B = (b_0, ..., b_{N-1})$ the numbers of edges in these bunches. The sum of these N numbers is m, thus the average is $\frac{m}{N}$.

Remark 2 *A geometrical interpretation may be convenient. Let us consider injective embedding of vertices of G into vertices of a perfect N-gon, the edges being the diagonals of N-gon which connect the corresponding pairs of vertices. Clearly, the above notion of parallel edges is in agreement with the standard Euclidean concept. Some 'non-Euclidean concepts' also can be considered. Counting of the corresponding "weakly parallel" edges (i.e. those, which just do not intersect but maybe not parallel) would give rise to some interesting combinatorial problems, too ([2] and Ron Aharoni, private communications). However, we will not consider this approach here.*

We study the following two functions:

$$\alpha(G,N) = \max_{B\in\mathcal{B}} \min_{b\in B} b, \quad \beta(G,N) = \min_{B\in\mathcal{B}} \max_{b\in B} b. \tag{5}$$

where $\mathcal{B} = \mathcal{B}(G,N)$ is the set of the distributions $B = B(G,N,f)$ generated by all the injective mappings $f : V \to [N]$. Obviously,

$$\alpha(G,N) \le \frac{m}{N} \le \beta(G,N) \tag{6}$$

because "minimum $\le$ average $\le$ maximum" for every distribution.

In [1] (see also [3] section 5) we considered the case of a simple cycle, $G = C_n$, $N \ge n \ge 3$. In this case function β can take only two values: 1 and 2 and $\alpha(C_n,N) = 1$ only if $\beta(C_n,N) = 1$ and $N = n$, otherwise $\alpha = 0$. We have proven that $\beta(C_n,N) = 2$ for the case $(n = N = 2i; i = 2,3,...)$, otherwise $\beta(C_n,N) = 1$.

In this paper we restrict ourselves by the case of the complete bipartite graph with equal parts, $G = K_{n,n}$, and $N = 2n$, for which camel sequences are applicable. (In section 6 we consider the case $G = K_{n,n}$, and $N = 2n+1$, for which one-hump camel sequences are applicable.) Let us introduce functions

$$\alpha(n) = \alpha(K_{n,n}, 2n), \quad \beta(n) = \beta(K_{n,n}, 2n). \tag{7}$$

Inequalities (6) can be rewritten as

$$\alpha(n) \leq \frac{n}{2} \leq \beta(n)\ \forall n. \tag{8}$$

Lemma 4 *For any positive integers k and n functions α and β satisfy the inequalities*

$$k\alpha(n) \leq \alpha(kn), \quad gb(kn) \geq \beta(kn). \tag{9}$$

Proof Let us suppose that value $\alpha(n)$ or $\beta(n)$ is realized by a (-1,+1)-sequence $(s_0, ..., s_{2n-1})$ which generates a box-distribution $B(s) = (b_0, ..., b_{2n-1})$. Let us consider the sequence $s^k = (s_0, ..., s_{2n-1})^k$. Obviously, it generates the box-distribution $B(s^k) = (kB(s))^k = (kb_0, ..., kb_{2n-1})^k$, where as usual x^k means: x repeated k times. Thus the maximal and minimal cardinalities of $B(s^k)$ are respectively k times the maximal and minimal cardinalities of $B(s)$. This and the definition of functions α, β by 5,7 prove 9. □

Inequalities (8) and (9) together imply the chain

$$k\alpha(n) \leq \alpha(kn) \leq \frac{n}{2} \leq \beta(kn) \leq k\beta(n). \tag{10}$$

Lemma 5 *Given a prime n, if $n = -1(mod\,4)$ then there exists an up-camel sequence and $\alpha(n) = \lfloor \frac{n}{2} \rfloor$, if $n = +1(mod\,4)$ then there exists a down-camel sequence and $\beta(n) = \lceil \frac{n}{2} \rceil$.*

Proof . The existence of the camel sequences was already proven. Inequalities (8) hold, $\alpha(n)$ and $\beta(n)$ are integer, and n is odd. Thus neither $\alpha(n)$ nor $\beta(n)$ can be equal to $\frac{n}{2}$, and hence they must be equal to $\lfloor \frac{n}{2} \rfloor$ and $\lceil \frac{n}{2} \rceil$ respectively. □

Proposition 2 *Number $\frac{1}{2}$ is a limit point of both sequences $\{\frac{\alpha(n)}{n},\ \frac{\beta(n)}{n};\ n = 1, 2, ...\}$. Moreover, $supLIM\{\frac{\alpha(n)}{n}; n = 1, 2, ...\} = infLIM\{\frac{\beta(n)}{n}; n = 1, 2, ...\} = \frac{1}{2}$, where $LIM(X)$ is the set of all the limit points of a set X.*

Proof . There exist infinitely many prime numbers of both types $n = -1\ (mod\,4)$ and $n = +1\ (mod\,4)$. According to the previous Lemma, for these two cases $\alpha(n) = \lfloor \frac{n}{2} \rfloor$ and $\beta(n) = \lceil \frac{n}{2} \rceil$, respectively, which proves the Proposition. □

Conjecture 1 . *The sequence* $\frac{\alpha(n)}{n}$*, as well as* $\frac{\beta(n)}{n}$*, converge to a limit as* n *tends to* ∞*.*

This would readily imply that their common limit is $\frac{1}{2}$; i.e. $lim_{n\to\infty}\frac{\alpha(n)}{n} = lim_{n\to\infty}\frac{\beta(n)}{n} = \frac{1}{2}$, or in other words, $\alpha(n) = \frac{n}{2} - o(n)$, $\beta(n) = \frac{n}{2} + o(n)$, that is both functions α and β asymptotically equals $\frac{n}{2}$.

5 First few values of functions α and β and some conjectures

According to Theorem 1 and Lemma 5, the camel sequences realize the extremal values $\alpha(n) = \lfloor\frac{n}{2}\rfloor$ and $\beta(n) = \lceil\frac{n}{2}\rceil$. We conjecture that this is a characteristic property of the camel sequences, or we can even say, of the quadratic residues.

Conjecture 2 . *Except for camel sequences, there exist no others, which realize values* $\alpha(n) = \lfloor\frac{n}{2}\rfloor$ *and* $\beta(n) = \lceil\frac{n}{2}\rceil$*. In other words, if* $\alpha(n) = \lfloor\frac{n}{2}\rfloor$ *then* n *is prime,* $n = -1(mod\,4)$ *and this value of* α *is realized by the corresponding up-camel sequence; and if* $\beta(n) = \lceil\frac{n}{2}\rceil$ *then* n *is prime,* $n = +1(mod\,4)$ *and this value of* β *is realized by the corresponding down-camel sequence.*

This conjecture readily, if true, implies that the difference $\beta - \alpha$ is sufficiently large. Indeed, for an even n neither of two equalities $\alpha(n) = n/2$ nor $\beta(n) = n/2$ can hold. Thus in this case $\beta(n) - \alpha(n) \geq 2$. If n is prime then exactly one of the two equalities: $\alpha(n) = \lfloor\frac{n}{2}\rfloor$ or $\beta(n) = \lceil\frac{n}{2}\rceil$ hold. Thus in this case $\beta(n) - \alpha(n) \geq 2$, too. (And we will conjecture that the equality always takes place.) Finally, if n is odd and not prime then neither of two equalities $\alpha(n) = \lfloor\frac{n}{2}\rfloor$ nor $\beta(n) = \lceil\frac{n}{2}\rceil$ hold. In this case $\beta(n) - \alpha(n) \geq 3$. Thus Conjecture 2 implies that

$$\alpha(n) < \frac{n}{2} < \beta(n), \quad \beta(n) - \alpha(n) \geq 2 \;\forall n > 1. \tag{11}$$

Due to a program by A. Tishchenko we get values $\alpha(n)$, $\beta(n)$ up to $n = 20$; see Table 1. We can observe from this table that the sum $\alpha + \beta$ and the difference $\beta - \alpha$ behave in a rather regular way, which gives us a hope to compute both functions exactly.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\alpha(n)$	0	0	1	1	1	2	3	2	3	4	5	4	5	6	6	6	7	8	9	8
$\beta(n)$	1	2	3	3	3	4	5	6	6	6	7	8	7	8	9	10	9	10	11	12

Table 1: The values $\alpha(n)$ and $\beta(n)$ for $n \leq 20$.

Conjecture 3 .

$$\alpha(n)+\beta(n)=\begin{cases} n & \text{if } n \text{ is NOT prime,} \\ n-1=4j & \text{if } n \text{ is prime and } n=4j+1, \\ n+1=4j & \text{if } n \text{ is prime and } n=4j-1. \end{cases}$$

Conjecture 4 . *The difference $\beta(n)-\alpha(n)$ equals 2 if n is prime, otherwise it is a divisor of n. In particular, if $n=pq$ is a product of two primes, then $\beta(n)-\alpha(n)=$* $\min\{p,q\}$.

We know that $\alpha(n)=\lfloor \frac{n}{2} \rfloor$ for $n=4j-1$ and $\beta(n)=\lceil \frac{n}{2} \rceil$ for $n=4j+1$ if n is prime. Thus for primes Conjecture 3 results from Conjecture 4.

6 One-hump camel sequences, the case $G=K_{n,n},\ N=2n+1$

Let us note that 'one-hump camel' sequences provide analogous results for the case $N=2n+1$. In this case we consider sequences which consists of n plus ones, n minus ones and 1 zero. And we distribute n^2 of $(+1,-1)$-pairs between $2n+1$ boxes. Thus the average is $\frac{n^2}{2n+1}$.

Given an odd prime p, the sequence $s=((1|p),(2|p),...,(p-1|p),(p|p))$ contains $\frac{p-1}{2}$ plus ones, $\frac{p-1}{2}$ minus ones and 1 zero, $(p|p)=0$. Thus $n=\frac{p-1}{2}$ and the average of the box-distribution $B=B(s)$ is $\frac{(\frac{p-1}{2})^2}{p}=\frac{(p-1)^2}{4p}$. The box-distribution $B=B(s)$ itself is given by Proposition 1. Obviously,

$$\frac{p-1}{4}=\lceil \frac{(p-1)^2}{4p} \rceil \text{ if } p=1\ (mod\ 4) \text{ and } \frac{p-3}{4}=\lfloor \frac{(p-1)^2}{4p} \rfloor \text{ if } p=-1\ (mod\ 4).$$

Thus for every odd prime p we get a 'one-hump camel' sequence s. If $p = -1\ (mod\ 4)$ then s is up-camel and its box-distribution realizes the maximin, that is $\alpha(K_{n,n}, 2n+1) = \frac{p-3}{4}$; if $p = +1\ (mod\ 4)$ then s is down-camel and its box-distribution realizes the minimax that is $\beta(K_{n,n}, 2n+1) = \frac{p-1}{4}$, where $n = \frac{(p-1)}{2}$.

We also conjecture that the above is a characteristic property of the one-hump camel sequences, or we can say, of the quadratic residues.

The authors are thankful to Alexander Tishchenko and Jiangdong Yang for important computations, the first author also thanks Ron Aharoni for helpful discussions.

References

[1] E.Boros and V.Gurvich, On parallel edges in cycles. DIMACS Technical Report DTR-99-28, Rutgers the State University of NJ, 1999;

[2] A. Dimitrescu and W. Steiger, On a matching problem in the plane, manuscript, Dep. of Computer Science, Rutgers the State University of NJ, 1999;

[3] V. Gurvich and Li Sheng, Camel sequences and their applications, DIMACS Technical Report DTR-99-29, Rutgers the State University of NJ, 1999;

[4] I.M. Vinogradov, An introduction to the theory of numbers, Pergamon Press, London - N.Y., 1955