Laced Boolean functions and subset sum problems in finite fields

David Canright[1], Sugata Gangopadhyay[2]
Subhamoy Maitra[3], Pantelimon Stănică[1]

[1] Department of Applied Mathematics, Naval Postgraduate School
Monterey, CA 93943–5216, USA; {dcanright,pstanica}@nps.edu

[2] Department of Mathematics, Indian Institute of Technology
Roorkee 247667 INDIA; gsugata@gmail.com

[3] Applied Statistics Unit, Indian Statistical Institute
203 B. T. Road, Calcutta 700 108, INDIA; subho@isical.ac.in

March 13, 2011

Abstract

In this paper, we investigate some algebraic and combinatorial properties of a special Boolean function on n variables, defined using weighted sums in the residue ring modulo the least prime $p \geq n$. We also give further evidence to a question raised by Shparlinski regarding this function, by computing accurately the Boolean sensitivity, thus settling the question for prime number values $p = n$. Finally, we propose a generalization of these functions, which we call *laced functions*, and compute the weight of one such, for *every* value of n.

Mathematics Subject Classification: 06E30,11B65,11D45,11D72
Key Words: Boolean functions; Hamming weight; Subset sum problems; residues modulo primes.

1 Introduction

Being interested in read-once branching programs, Savicky and Zak [7] were led to the definition and investigation, from a complexity point of view, of a special Boolean function based on weighted sums in the residue ring modulo a prime p. Later on, a modification of the same function was used by Sauerhoff [6] to show that quantum read-once branching programs are exponentially more powerful than classical read-once branching programs. Shparlinski [8] used exponential sums methods to find bounds on the Fourier coefficients, and he posed several open questions, which are the motivation of this work.

Let n be a positive integer and p the smallest prime with $p \geq n$. Let $\mathbb{V}_n := \mathbb{Z}_2^n$. Given a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{V}_n$, we define $wt(\mathbf{x}) = \sum_{i=1}^n x_i$ to be the Hamming weight of $\mathbf{x}$, and we let

$$s_+(\mathbf{x}) = \sum_{k=1}^{n} k x_k \pmod{p}, \quad 1 \leq s_+(\mathbf{x}) \leq p, \tag{1}$$

and define the x_1–*laced Boolean function* (or simply, *laced function*) $L_{n,+}$ on $\mathbb{V}_n$ by

$$L_{n,+}(\mathbf{x}) = \begin{cases} x_{s_+(\mathbf{x})} & \text{if } 1 \leq s_+(\mathbf{x}) \leq n; \\ x_1 & \text{otherwise.} \end{cases} \tag{2}$$

Note: this $L_{n,+}$ function is the function f_n of [7] and f of [8].

We remark that we can alternatively define a function

$$s_0(\mathbf{x}) = \sum_{k=1}^{n} k x_k \pmod{p}, \quad \text{with } 0 \leq s_0(\mathbf{x}) \leq p-1. \tag{3}$$

Let $L_{n,0}$ be the laced function corresponding to s_0, namely

$$L_{n,0}(\mathbf{x}) = \begin{cases} x_{s_0(\mathbf{x})} & \text{if } 1 \leq s_0(\mathbf{x}) \leq n; \\ x_1 & \text{otherwise.} \end{cases} \tag{4}$$

It is immediate that if $n \neq p$ then $L_{n,0}$ is the same as $L_{n,+}$.

Throughout this paper, we use the Landau symbols O and o with their usual meanings. We denote by $e_i = (0, \ldots, 1, 0, \ldots, 0)$ the basis vector with the only nonzero component in position i, in a vector space over the binary field, of dimension that will be apparent from the context.

2 The weight of $L_{n,+}$

We recall that the weight, denoted by $wt(f)$, of a Boolean function f is the weight of its truth table, namely the number of 1's in that binary string.

It is not very difficult to show that $L_{p,0}$ (p prime) does not depend on x_p. In fact, the following theorem holds.

Theorem 1. *If p is prime, then*

$$L_{p,0}(x_1, \ldots, x_p) = L_{p-1,+}(x_1, \ldots, x_{p-1})$$

and so, $wt(L_{p,0}) = 2\, wt(L_{p-1,+})$. Furthermore, if $n \neq 2$, then

$$wt(L_{n,0}) = wt(L_{n,+}).$$

Proof. When n is prime, the function $L_{n,0}$ is degenerate and the first half of the truth table is the same as the second half. That is because when n is prime, then $k\, x_k \pmod p$ will always be zero when $k = n$, for either bit value x_k. The first half of the truth table will have $x_n = 0$, and the second half will have $x_n = 1$. The output will be the same in both the cases. Only in the case that $p-1$ is also prime is the $L_{p-1,+}$ function needed on the right-hand side, otherwise $L_{p-1,0}$ is equivalent. Since the weight of a function, whose value does not depend on one of its variables, is twice the weight of the function after removing this variable we have $wt(L_{p,0}) = 2wt(L_{p-1,+})$.

When $n = p$ is prime then $L_{n,0}$ and $L_{n,+}$ may differ. In that case, when $L_{p,+}(\mathbf{x}) = x_p$, then $L_{p,0}(\mathbf{x}) = x_1$. The argument for the first part of our theorem implies that $L_{p,0}(\mathbf{x})$ is independent of the value of x_p. Moreover, note that $\sum_{k=1}^{p-1} k = \frac{p(p-1)}{2}$ is divisible by p if p is *odd*. Consider those values of $\mathbf{x}$ whose weighted sums are divisible by p, where $L_{p,+}(\mathbf{x})$ and $L_{p,0}(\mathbf{x})$ may differ. For each such choice of the first $p-1$ bits, the bitwise complement of those $p-1$ bits also gives a weighted sum divisible by p, and x_p can take either value. So these cases can be partitioned into groups of four, each group having two with $x_1 = 1$ and two with $x_p = 1$. Hence $wt(L_{p,0}) = wt(L_{p,+})$. Finally, it is easy to check that $wt(L_{2,0}) = 2 \neq wt(L_{2,+}) = 3$. □

Suppose $D \subseteq \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ and $b \in \mathbb{Z}_p$. Define as in [3]

$$N(k, b, D) = \#\{\{x_1, \ldots, x_k\} \subseteq D \,|\, x_1 + x_2 + \cdots + x_k \equiv b \bmod p\}.$$

Let $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. From Theorem 1.2 in [3] we obtain

$$N(k, b, \mathbb{Z}_p^*) = \frac{1}{p}\binom{p-1}{k} + (-1)^k \frac{v(b)}{p}$$

where $v(b) = p-1$ if $b = 0$ and $v(b) = -1$ if $b \neq 0$. In this section we use the results on the subset sum problem proved in [3] to put the computation of the weight of $L_{n,0}$ in a recursive framework. First we prove the following lemma.

Lemma 2. *For any $a, b \in \mathbb{Z}_p$ and $a \neq 0$,*

$$N(k, b, \mathbb{Z}_p \setminus \{0, a\}) = \frac{1}{p}\left(\binom{p-2}{k} + (-1)^k (wp - k - 1)\right), \tag{5}$$

where $w = 1$ if $b/a \in \{0, \ldots, k\}$ and $w = 0$ otherwise.

Proof. From the proof of Theorem 1.3 of [3, p. 920] we infer that

$$N(k,b,\mathbb{Z}_p\setminus\{0,a\})=\frac{1}{p}\left(\binom{p-2}{k}-(-1)^k\sum_{j=0}^{k}v(b-ka+ja)R_j^1\right),$$

where $R_j^1=(-1)^{\lfloor j/p\rfloor+1}=-1$ (if $j<p$). In the case under consideration $R_j^1=-1$ and $b-ka+ja=0$ if and only if $b/a=k-j$ where $j\in\{0,1,\dots k\}$. Therefore we obtain

$$N(k,b,\mathbb{Z}_p\setminus\{0,a\})=\frac{1}{p}\left(\binom{p-2}{k}+(-1)^k(wp-k-1)\right),$$

where $w=1$ if $b/a\in\{0,\dots,k\}$ and $w=0$ otherwise. □

Theorem 3. *If $p>3$ is a prime then*

$$wt(L_{p-1,0})=2^{p-2}+\frac{p-1}{2}.$$

Further, the algebraic degree of $L_{p-1,0}$ is $\deg(L_{p-1,0})=p-1$, if $p\equiv 3 \pmod 4$, and $\deg(L_{p-1,0})\le p-2$, if $p\equiv 1 \pmod 4$.

Proof. Suppose $\mathbf{x}=(x_1,\mathbf{x}')\in\mathbb{V}_{p-1}\setminus\{\mathbf{0}\}$. Then $L_{p-1,0}(\mathbf{x})=1$ if and only if any one of the following conditions is satisfied:

1. $s_0(\mathbf{x})=0$ and $x_1=1$; that is, $s_0(0,\mathbf{x}')=p-1$, using indices $k\in\mathbb{Z}_p\setminus\{0,1\}$.
2. $s_0(\mathbf{x})=b\ge 1$ and $x_b=1$; that is, letting $\tilde{\mathbf{x}}$ be $\mathbf{x}$ except $\tilde{x}_b=0$, then $s_0(\tilde{\mathbf{x}})=0$, using indices $k\in\mathbb{Z}_p\setminus\{0,b\}$.

The weight of the function $L_{p-1,0}$ is

$$\begin{aligned}wt(L_{p-1,0})&=\sum_{k=1}^{p-2}N(k,p-1,\mathbb{Z}_p\setminus\{0,1\})+\sum_{k=0}^{p-2}\sum_{b=1}^{p-1}N(k,0,\mathbb{Z}_p\setminus\{0,b\})\\&=\sum_{k=1}^{p-2}\frac{\binom{p-2}{k}+(-1)^{k+1}(k+1)}{p}\\&+\sum_{k=0}^{p-2}\sum_{b=1}^{p-1}\frac{1}{p}\left(\binom{p-2}{k}+(-1)^k(p-k-1)\right)\\&=2^{p-2}+\frac{p-1}{2}.\end{aligned}\tag{6}$$

The above follows from Lemma 2, binomial coefficients manipulation, using the well known $\sum_{s=0}^{N}\binom{N}{s}=2^N$ and the fact that $\sum_{l=0}^{k}(-1)^l(k+1-l)=\left\lfloor\frac{k+2}{2}\right\rfloor$.

We now deal with the last claim. Assume $p\equiv 3 \pmod 4$. By McEliece's Theorem, the weight of a Boolean function of degree d must be divisible by

$2^{\lfloor (n-1)/d \rfloor}$ (see [4, p. 447]). If the degree d of $L_{p-1,0}$ were at most $p-2$, then its weight would be divisible by $2^{\lfloor (p-2)/d \rfloor}$ with $\lfloor (p-2)/d \rfloor \geq 1$. Since in our case $p \equiv 3 \pmod 4$, then 2 cannot divide $(p-1)/2$, and so, 2 cannot divide the weight of $L_{p-1,0}$, therefore the degree of $L_{p-1,0}$ must be $p-1$. Further, assume $p \equiv 1 \pmod 4$. If $\deg(L_{p-1,0})$ were $p-1$, then it is immediate that the weight of $L_{p-1,0}$ must be odd, which is not true under the condition $p \equiv 1 \pmod 4$. Thus, $\deg(L_{p-1,0}) \leq p-2$. (We conjecture that, in fact, $\deg(L_{p-1,0}) = p-2$, if $p \equiv 1 \pmod 4$.) □

In [3, p. 922] the following recursion was obtained, which will be used by us quite often.

Lemma 4. *We have*

$$N(k, b, \mathbb{Z}_p \setminus \{a_1, \ldots, a_c\}) = \sum_{i=0}^{k} (-1)^i N(k-i, b-ia_c, \mathbb{Z}_p \setminus \{a_1, \ldots, a_{c-1}\}). \quad (7)$$

In principle, one can compute the weight of any of $L_{s,0}$ by using a descent method, which we shall display next. Let $\mathbf{x} = (x_1, x_2, \cdots, x_{n-1})$ and $\mathbf{x}' = (x_2, x_3, \cdots, x_{n-1})$. It is easy to see that if $n-1$ is not prime, then

$$L_{n,0}(\mathbf{x}, x_n) = \bar{x}_n L_{n,0}(\mathbf{x}, 0) \oplus x_n L_{n,0}(\mathbf{x}, 1). \quad (8)$$

Further, $L_{n,0}(\mathbf{x}, 0) = L_{n-1,0}(\mathbf{x})$ unless $s_0(\mathbf{x}) = n$ and $x_1 = 1$, therefore, $wt(L_{n,0}(\mathbf{x}, 0)) = wt(L_{n-1,0}(\mathbf{x})) - \#\{\mathbf{x} : s_0(\mathbf{x}) = n \text{ and } x_1 = 1\}$. Thus, if one knows the weight of $L_{n,0}$ (for instance, since we now know the weight of $L_{p-1,0}$ by Theorem 3, we can work our way down), to find the weight of any function $L_{n-1,0}$, we need to find the weight of the second half of $L_{n,0}$, that is, $wt(L_{n,0}(\cdot, 1))$. The problem does not seem to be easy, in general, but we shall display an example.

Let $n = p-1$. From (8) we get

$$wt(L_{n,0}) = wt(L_{n-1,0}) + wt(L_{n,0}(\cdot, 1)) - \sum_{k=1}^{p-3} N(k, p-2, \mathbb{Z}_p \setminus \{0, 1, p-1\}).$$

First, using equation (5) and the well known binomial coefficients identity

$$\sum_{i=0}^{k} (-1)^i \binom{r}{i} = (-1)^k \binom{r-1}{k}. \quad (9)$$

we obtain

$$\begin{aligned} N(k, p-2, \mathbb{Z}_p \setminus \{0, 1, p-1\}) &= \sum_{i=0}^{k} (-1)^i N(k-i, i-2, \mathbb{Z}_p \setminus \{0, 1\}) \\ &= \sum_{i=0}^{k} \frac{(-1)^i}{p} \left(\binom{p-2}{k-i} + (-1)^{k-i} \sum_{j=0}^{k-i} v(2i+j-k-2) \right) \quad (10) \\ &= \frac{1}{p} \binom{p-3}{k} + \frac{(-1)^k}{p} \sum_{i=0}^{k} \sum_{j=0}^{k-i} v(2i+j-k-2). \end{aligned}$$

The computation of the double sum is straightforward, since $v(\cdot)$ is -1 except for one input, when it is $p-1$, but that happens only if $2 \leq i \leq \frac{k+2}{2}$. Ultimately, one obtains

$$\sum_{k=1}^{p-3} N(k, p-2, \mathbb{Z}_p \setminus \{0, 1, p-1\}) = \frac{2^{p-1} + p^2 - 4p - 1}{4p},$$

and so, we get

$$wt(L_{n,0}) = wt(L_{n-1,0}) + wt(L_{n,0}(\cdot, 1)) - \frac{2^{p-1} + p^2 - 4p - 1}{4p} \tag{11}$$

We now concentrate on $L_{n,0}(\mathbf{x}, 1)$, where $n = p-1$. By Theorem 3, we know that the weight $wt(L_{p-1,0}) = 2^{p-2} + \frac{p-1}{2}$. Since $x_n = 1$ in this case, we see that $L_{n,0}(\mathbf{x}, 1) = 1$ if and only if one of the next (independent) conditions is satisfied:

(*i*) $s_0(\mathbf{x}) = 0$; and so, $s_0(\mathbf{x}, x_n) = n$. It follows that $L_{n,0}(\mathbf{x}, 1) = x_n = 1$.

(*ii*) $s_0(\mathbf{x}) = 1$ and $x_1 = 1$; and so, $s_0(\mathbf{x}, x_n) = 0$. Then $L_{n,0}(\mathbf{x}, 1) = x_1 = 1$.

(*iii*) $s_0(\mathbf{x}) = b \geq 2$ and $x_{b-1} = 1$; and so, $1 \leq s_0(\mathbf{x}, x_n) = b - 1 \leq p - 2$. Then $L_{n,0}(\mathbf{x}, 1) = x_{b-1} = 1$.

We now count the number of solutions $\mathbf{x}$ in each of these cases. With the previous notations, by (5) the number of solutions in case (*i*) is

$$\begin{aligned} \sum_{k=0}^{n-1} N(k, 0, \mathbb{Z}_p \setminus \{0, p-1\}) &= \sum_{k=0}^{p-2} \frac{1}{p} \left(\binom{p-2}{k} + (-1)^k (p-k-1) \right) \\ &= \frac{2^{p-2} - 1}{p} + \frac{p+1}{2p} = \frac{2^{p-1} + p - 1}{2p}. \end{aligned} \tag{12}$$

It follows from (7) that the number of solutions in case (*ii*) is

$$\begin{aligned} &\sum_{k=0}^{p-3} N(k, 0, \mathbb{Z}_p \setminus \{0, 1, p-1\}) \\ &= \sum_{k=0}^{p-3} \sum_{i=0}^{k} (-1)^i N(k-i, i, \mathbb{Z}_p \setminus \{0, 1\}) \\ &= \sum_{k=0}^{p-3} \sum_{i=0}^{k} (-1)^i \frac{1}{p} \left(\binom{p-2}{k-i} + (-1)^{k-i} \sum_{j=0}^{k-i} v(2i + j - k) \right) \\ &= \frac{2^{p-3}}{p} + \frac{p^2 - 1}{4p} = \frac{2^{p-1} + p^2 - 1}{4p}. \end{aligned}$$

Similarly, the number of solutions in case (iii) is

$$\begin{aligned}
&\sum_{b=2}^{p-1}\sum_{k=1}^{p-3} N(k,1,\mathbb{Z}_p\setminus\{0,b-1,p-1\})\\
&=\sum_{b=2}^{p-1}\sum_{k=1}^{p-3}\sum_{i=0}^{k}(-1)^i N(k-i,i+1,\mathbb{Z}_p\setminus\{0,b-1\})\\
&=\sum_{b=2}^{p-1}\sum_{k=1}^{p-3}\sum_{i=0}^{k}(-1)^i\frac{1}{p}\left(\binom{p-2}{k-i}+(-1)^{k-i}\sum_{j=0}^{k-i}v(i+1+(j-k+i)(b-1))\right)\\
&=\sum_{b=2}^{p-1}\sum_{k=1}^{p-3}\frac{1}{p}\left(\binom{p-3}{k}-\frac{(-1)^k}{2}(k^2+3k+2)\right)=\frac{2^{p-1}(p-2)-2p+2}{4p}.
\end{aligned}$$

Adding these three counts and using (11), we obtain

$$\begin{aligned}
&2^{p-2}+\frac{p-1}{2}-\frac{2^{p-1}+p-1}{2p}-\frac{2^{p-1}+p^2-1}{4p}-\frac{2^{p-1}(p-2)-2p+2}{4p}\\
&\quad+\frac{p^2-4p+2^{p-1}-1}{4p}=2^{p-3}+\frac{p-3}{2},
\end{aligned}$$

which proves the next theorem.

Theorem 5. *Assuming that $p>3$ is prime and $p-2$ composite, then the weight of $L_{p-2,0}$ is*

$$wt(L_{p-2,0})=2^{p-3}+\frac{p-3}{2}.$$

For easy writing, if p is fixed, let $A(t):=\sum_{k=0}^{t}(-1)^k\binom{k+p-1-t}{k}$. In general, along the same path as before (without attempting to have accurate bounds) one can prove the next result.

Theorem 6. *Let $n>2$ be an integer, p the least prime $\geq n$ and $\mathbb{D}=\mathbb{Z}_p\setminus\{0,n+1,\ldots,p-1\}$. The weights $w_n=wt(L_{n,0})$, $n\leq p-2$, satisfy the recurrence*

$$\begin{aligned}
w_n-w_{n-1} &= \sum_{k=0}^{n-1}N(k,0,\mathbb{D}\setminus\{n\})+\sum_{k=0}^{n-2}N(k,0,\mathbb{D}\setminus\{1,n\})\\
&\quad+\sum_{b=2}^{n}\sum_{k=1}^{n-2}N(k,1,\mathbb{D}\setminus\{b-1,n\})-\sum_{k=1}^{n-2}N(k,n-1,\mathbb{D}\setminus\{1,n\})\\
&\leq \frac{1}{p}\left((n+1)2^{n-2}+n\binom{p-1}{n-2}+\binom{p-1}{n-1}+-\frac{n-1}{p}+2\right)\\
&\quad+\binom{p}{n-1}-1-\frac{1}{p^2}\left(A(n-1)+(p-1)A(n-2)\right).
\end{aligned}$$

Proof. We will motivate only the inequality claim, as the recurrence can be shown by an argument similar to the one of Theorem 5. We use Theorem 1.1 of [3] together with equation (8), to find upper bounds for each count.

First,

$$\begin{aligned}\sum_{k=0}^{n-1} N(k,0,\mathbb{D}\setminus\{n\}) &\leq \sum_{k=0}^{n-1} \frac{\binom{n-1}{k} - \frac{(-1)^k}{p}\binom{k+p-n}{p-n} + \binom{k+p-n-1}{p-n-1}}{p} \\ &= \frac{1}{p}\left(2^{n-1} + \binom{p-1}{n-1}\right) - \frac{1}{p^2}\sum_{k=0}^{n-1}(-1)^k\binom{k+p-n}{p-n} \\ &= \frac{1}{p}\left(2^{n-1} + \binom{p-1}{n-1}\right) - \frac{1}{p^2}A(n-1).\end{aligned}$$

Next,

$$\begin{aligned}\sum_{k=0}^{n-1} N(k,0,\mathbb{D}\setminus\{1,n\}) &\leq \sum_{k=0}^{n-2} \frac{\binom{n-2}{k} - \frac{(-1)^k}{p}\binom{k+p-n+1}{p-n+1} + \binom{k+p-n}{p-n}}{p} \\ &\frac{1}{p}\left(2^{n-2} + \binom{p-1}{n-2}\right) - \frac{1}{p^2}\sum_{k=0}^{n-2}(-1)^k\binom{k+p-n+1}{p-n+1} \\ &\frac{1}{p}\left(2^{n-2} + \binom{p-1}{n-2}\right) - \frac{1}{p^2}A(n-2).\end{aligned}$$

Third,

$$\begin{aligned}\sum_{b=2}^{n}\sum_{k=1}^{n-2} N(k,1,\mathbb{D}\setminus\{b-1,n\}) &\leq (n-1)\sum_{k=1}^{n-2} \frac{\binom{n-2}{k} - \frac{(-1)^k}{p}\binom{k+p-n+1}{p-n+1} + \binom{k+p-n}{p-n}}{p} \\ &= \frac{n-1}{p}\left(2^{n-2} + \binom{p-1}{n-2} - 1\right) - \frac{n-1}{p^2}\sum_{k=1}^{n-2}(-1)^k\binom{k+p-n+1}{p-n+1} \\ &= \frac{n-1}{p}\left(2^{n-2} + \binom{p-1}{n-2} - 1\right) - \frac{n-1}{p^2}\left(A(n-2) - 1\right).\end{aligned}$$

Finally,

$$\begin{aligned}&\sum_{k=1}^{n-2} N(k,n-1,\mathbb{D}\setminus\{1,n\}) \\ &\geq \sum_{k=1}^{n-2}\left(\frac{1}{p}\binom{n-2}{k} - \frac{(-1)^k}{p}\binom{k+p-n+1}{p-n+1} - \binom{k+p-n}{p-n}\right) \\ &= \frac{1}{p}\left(2^{n-2} + p - 1\right) - \binom{p}{n-1} - \frac{1}{p}\sum_{k=1}^{n-2}(-1)^k\binom{k+p-n+1}{p-n+1}.\end{aligned}$$

Putting all these bounds together, we obtain that $w_n - w_{n-1}$ is

$$\begin{aligned}\leq\ & \frac{1}{p}\left((n+1)2^{n-2} + n\binom{p-1}{n-2} + \binom{p-1}{n-1} + -\frac{n-1}{p} + 2\right) \\ &+\binom{p}{n-1} - 1 - \frac{1}{p^2}\left(A(n-1) + (p-1)A(n-2)\right).\end{aligned}$$

□

One can use a computer algebra system to replace $A(t)$ by a hypergeometric expression, but we preferred not to do that, since it is simple enough (as one reviewer suggested). Taking $n = p-2$ in the previous theorem and using the result of Theorem 5, we obtain the following corollary.

Corollary 7. *We have for prime $p > 3$ where $p-2$ is composite*

$$wt(L_{p-3,0}) \geq \frac{p-1}{p} \cdot 2^{p-4} - \frac{4p^5 - 34p^4 + 117p^3 - 215p^2 + 227p - 3}{24p}.$$

3 A generalization

We introduce a generalized version of the x_1–laced Boolean function, say *ϕ–laced function*, where ϕ is an arbitrary, but fixed Boolean function on $\mathbb{V}_n$, which we define by

$$L_n^{\phi}(\mathbf{x}) = \begin{cases} x_{s(\mathbf{x})} & \text{if } 1 \leq s(\mathbf{x}) \leq n; \\ \phi(\mathbf{x}) & \text{otherwise,} \end{cases}$$

where s is either s_0, or s_+. It could be interesting to investigate the properties of this generalized laced function, similar to the ones contained in [8], or in this paper. Below we consider one such function obtained by modifying the x_1–laced Boolean function, and compute its weight for any value of n.

3.1 A modification of the x_1–laced Boolean function

Let the Boolean function L_n be defined as follows.

$$L_n(\mathbf{x}) = \begin{cases} x_{s_+(\mathbf{x})} & \text{if } s_+(\mathbf{x}) \in [1, n]; \\ x_{s_+(\mathbf{x})-n} & \text{if } s_+(\mathbf{x}) \in [n+1, p]. \end{cases} \tag{13}$$

(Note that when $n = p$ or $n = p-1$, this L_n is the same as $L_{n,+}$, which was studied earlier.) Recall the definition of Gauss' hypergeometric function [1, P.1]

$${}_2F_1(a, b; c; z) = \sum_{k=0}^{\infty} \frac{(a)_k (b)_k z^k}{(c)_k k!},$$

where $(x)_k = x(x+1)\cdots(x+k-1)$ is the Pochhammer symbol. We will be using the hypergeometric function ${}_2F_1$ to write in a compact way an alternating sum of binomial coefficients. In the following theorem we obtain the weight of the function L_n, for *every* value of n. Let $w_{b,k} = 1$, if (the least residue of) $n(b-n)^{-1} \pmod p$ is $i \leq k$, otherwise, $w_{b,k} = 0$. Define $\epsilon_n := \sum_{b=n+1}^{p} \sum_{k=1}^{n-1} (-1)^k w_{b,k}$.

Theorem 8. *If $n > 2$ is a positive integer and p is the smallest prime number greater than or equal to n with $p \neq n$ then the weight of the function L_n is*

$$wt(L_n) = 2^{p-2} + \frac{n-p}{p} - \binom{p-2}{n} {}_2F_1(1, n-p+2, n+1, -1) + \epsilon_n \\ + \frac{(2(-1)^n n + (1-(-1)^n)(2p-1)) + (3 + (2n+1)(-1)^n)(p-n)}{4p}.$$

Proof. Suppose $s_+(\mathbf{x}) = b$. $L_n(\mathbf{x}) = 1$ in the following two cases.
Case 1: $b \in [1, n]$, $x_b = 1$. In this case $\sum_{k=1}^{n} kx_k = b \bmod p$, that is $\sum_{k=1, k\neq b}^{n} kx_k = 0 \bmod p$. The number of such points is equal to

$$\sum_{b=1}^{n} \sum_{k=0}^{n-1} N(k, 0, \mathbb{Z} \setminus \{0, b\}).$$

Case 2: $b \in [n+1, p]$, $x_{b-n} = 1$. In this case $\sum_{k=1, k\neq n-b}^{n} kx_k + b - n = b \bmod p$, that is $\sum_{k=1, k\neq n-b}^{n} kx_k = n \bmod p$. The number of such points is equal to

$$\sum_{b=n+1}^{p} \sum_{k=1}^{n-1} N(k, n, \mathbb{Z} \setminus \{0, b-n\}).$$

Thus the total number of points at which the function L_n is equal to 1 is

$$wt(L_n) = \sum_{b=1}^{n} \sum_{k=0}^{n-1} N(k, 0, \mathbb{Z} \setminus \{0, b\}) + \sum_{b=n+1}^{p} \sum_{k=1}^{n-1} N(k, n, \mathbb{Z} \setminus \{0, b-n\}).$$

Recall that $N(k, b, \mathbb{Z}_p \setminus \{0, a\}) = \frac{1}{p}\left(\binom{p-2}{k} - (-1)^k \sum_{j=0}^{k} v(b - ka + ja) R_j^1\right)$, where $v(b) = p - 1$ if $b = 0$ and $v(b) = -1$ if $b \neq 0$. $R_j^1 = (-1)^{\lfloor \frac{j}{p} \rfloor + 1} = -1$ if $j < p$. Thus

$$\begin{aligned} N(k, 0, \mathbb{Z}_p \setminus \{0, b\}) &= \frac{1}{p}\left(\binom{p-2}{k} + (-1)^k \sum_{j=0}^{k} v(b(j-k))\right) \\ &= \frac{1}{p}\left(\binom{p-2}{k} + (-1)^k (p - k - 1)\right), \end{aligned} \tag{14}$$

since $b < p$ and so $v(b(j-k)) = v(j-k)$. Further,

$$\begin{aligned} N(k, n, \mathbb{Z}_p \setminus \{0, b-n\}) &= \frac{1}{p}\left(\binom{p-2}{k} + (-1)^k \sum_{j=0}^{k} v(n - (b-n)(k-j))\right) \\ &= \frac{1}{p}\left(\binom{p-2}{k} + (-1)^k \sum_{i=0}^{k} v(n - (b-n)i)\right) \\ &= \frac{1}{p}\left(\binom{p-2}{k} + (-1)^k (p\, w_{b,k} - k - 1)\right), \end{aligned} \tag{15}$$

where $w_{b,k} = 1$, if (the least residue of) $n(b-n)^{-1} \pmod p$ is $i \leq k$ (and so, $v(n - (b-n)i) = p - 1$, in that case), otherwise, $w_{b,k} = 0$. Now, we use (14) and (15), together with Mathematica[1], to compute the weight of the

[1] A Trademark of Wolfram Research

function L_n as

$$\begin{aligned}
wt(L_n) &= \sum_{b=1}^{n}\sum_{k=0}^{n-1} N(k,0,\mathbb{Z}\setminus\{0,b\}) + \sum_{b=n+1}^{p}\sum_{k=1}^{n-1} N(k,n,\mathbb{Z}\setminus\{0,b-n\}) \\
&= \frac{1}{p}\sum_{b=1}^{n}\sum_{k=0}^{n-1}\left(\binom{p-2}{k} + (-1)^k(p-k-1)\right) \\
&+ \frac{1}{p}\sum_{b=n+1}^{p}\sum_{k=1}^{n-1}\left(\binom{p-2}{k} + (-1)^k(p\,w_{b,k}-k-1)\right) \\
&= \frac{1}{p}\sum_{b=1}^{p}\sum_{k=0}^{n-1}\binom{p-2}{k} + \frac{n-p}{p} + \frac{1}{p}\sum_{b=1}^{n}\sum_{k=0}^{n-1}(-1)^k(p-k-1) \\
&+ \frac{1}{p}\sum_{b=n+1}^{p}\sum_{k=1}^{n-1}(-1)^k(p\,w_{b,k}-k-1) \\
&= 2^{p-2} + \frac{n-p}{p} - \binom{p-2}{n}{}_2F_1(1,n-p+2,n+1,-1) + \epsilon_n \\
&+ \frac{1}{4p}\left(2(-1)^n n + (1-(-1)^n)(2p-1)\right) + \frac{1}{4p}\left(3+(2n+1)(-1)^n\right)(p-n).
\end{aligned}$$

(Observe that the hypergeometric function ${}_2F_1(a,b;c;z)$ is convergent for $a=1, b=n-p+2, n+1, z=-1$, since $Re(c-a-b) = (n+1)-1-(n-p+2) = p-2 > 0$, cf. [1, P.1].) □

4 The average sensitivity of some laced functions

In [2], Cook et al. introduced the notion of *sensitivity* as a combinatorial complexity measure for Boolean functions providing lower bounds on the time needed by a CREW PRAM (concurrent read, but exclusive write (CREW) parallel random access machine (PRAM)). It was extended by Nisan [5] to block sensitivity. It is still open whether sensitivity and block sensitivity are polynomially related (they are equal for monotone Boolean functions). Here, we will define and work with the notion of sensitivity, only. Although the definition is straightforward, the sensitivity is understood only for a few classes of function. In this section we add one more class (Theorem 10) of Boolean functions for which the sensitivity is known.

Let $\rho = 1 - \frac{2}{\pi \ln 2}\sum_{k=0}^{\infty}\frac{(-1)^k}{(2k+1)^2} \approx 0.1587\ldots$, and let H be the entropy function $H(x) = -x\log x - (1-x)\log(1-x)$, $0 < x < 1$. We define the *average sensitivity* of a Boolean function g on n variables by

$$\sigma_{av}(g) = 2^{-n}\sum_{\mathbf{x}\in\mathbb{V}_n}\sum_{i=1}^{n}|g(\mathbf{x}) - g(\mathbf{x}\oplus e_i)|, \tag{16}$$

where $e_i = (0,\ldots,0,1,0,\ldots)$ (with 1 on the ith position). Shparlinski showed in [8] that $\sigma_{av}(f) \geq (\tau + o(1))n$, where $\tau = 0.0575\ldots$ is the root of the equation $H(\tau) = 2\rho$, and he asked the following question.

Open Question 9 ([8, p. 86])**.** *Is it true that the function $L_{n,+}$ satisfies*

$$\sigma_{av}(L_{n,+}) \geq \left(\frac{1}{2} + o(1)\right) n\,?$$

Below, we give further evidence to this open question (recall that for n prime, $L_n = L_{n,+}$, and so, we get the same result for L_n for free). We would like to point out that the error term in our computation is explicit and always negative, for prime p sufficiently large (more precisely, $p \geq 11$).

Theorem 10. *We have for odd prime p*

$$\begin{aligned}\sigma_{av}(L_{p,+}) &= \frac{(p^2-p+2)2^{p-2} + (p-1)^3 + (p^2-p)(-1)^{\frac{p-1}{2}}}{p\,2^{p-1}} \\ &= \left[\frac{1}{2}\left(1 - \frac{1}{p} + \frac{2}{p^2}\right) + O\left(\frac{p}{2^{p-1}}\right)\right] p.\end{aligned}$$

Consequently, $\sigma_{av}(L_{p,+}) < \frac{p}{2}$, for sufficiently large prime p.

Proof. To find $\sigma_{av}(L_{p,+})$ we count the ways that changing a single bit in $\mathbf{x}$ to get $\tilde{\mathbf{x}}$ results in a change in the function from $L_{p,+}(\mathbf{x}) = 1$ to $L_{p,+}(\tilde{\mathbf{x}}) = 0$; this total gives $2^{p-1}\,\sigma_{av}(L_{p,+})$. (The power is 2^{p-1}, not 2^p, because we only count the changes of $L_{p,+}$ from 1 to 0 and not the reverse cases from 0 to 1.)

Let $a = s_+(\mathbf{x})$, b be the index of the bit x_b we flip to $\tilde{x}_b$, and $c = s_+(\tilde{\mathbf{x}})$. Then the output of $L_{p,+}$ will change from $x_a = 1$ to $\tilde{x}_c = 0$ in the five distinct cases below. In the last case, $x_b = 0$ changes to $\tilde{x}_b = 1$. For the first four cases, $x_b = 1$ changes to $\tilde{x}_b = 0$, so $c = a - b \pmod p$, and we exhaust all cases of equality between a, b, and c; note that we cannot have $a = c \neq b$ because then $\tilde{x}_c = x_a = 1$.

(*i*) $a = b = c = p$ (since $c = a - b \pmod p$) so $\tilde{x}_c = \tilde{x}_b = 0$.

(*ii*) $x_b = 1$ and $a \neq b = c$ (i.e. $a = 2b \pmod p$ but $b \neq p$), so $a \neq p$ and $\tilde{x}_c = \tilde{x}_b = 0$.

(*iii*) $a = b \neq c = p$ (since $c = a - b \pmod p$) and $x_p = 0$, so $\tilde{x}_c = x_p = 0$.

(*iv*) $x_b = 1$ and $x_c = 0$ and a, b, and c are distinct (where $c = a - b \pmod p$), so $a \neq 2b \pmod p$ (since $b \neq c$) and $b \neq p$ (since $a \neq c$) and $c \neq p$ (since $a \neq b$), then $\tilde{x}_c = x_c = 0$.

(*v*) $x_b = 0$ and $x_c = 0$, where $c = a + b \pmod p$, so $a \neq b$ (since $x_a = 1 \neq x_b = 0$), $b \neq c$ and $a \neq p$ (since $\tilde{x}_b = 1 \neq \tilde{x}_c = 0$), $a \neq c$ and $b \neq p$ (since $x_a = 1 \neq x_c = 0$), so again a, b, and c are distinct.

We now count the number of solutions a, b, c in each of these cases. We will extensively use Lemma 4 along with equation (9) and the definition of the function $v(\cdot)$.

With the previous notations, the number of solutions in case (i) is

$$\begin{aligned} S_1 &= \sum_{k=0}^{p-1} N(k,0,\mathbb{Z}_p\setminus\{0\}) \\ &= \sum_{k=0}^{p-1}\frac{1}{p}\left(\binom{p-1}{k}+(-1)^k(p-1)\right) = \frac{2^{p-1}+p-1}{p}. \end{aligned} \tag{17}$$

For case (ii), the number of solutions for the choice $b=1$ (so $a=2$) is

$$\begin{aligned} S_2 &= \sum_{k=1}^{p-3} N(k,-1,\mathbb{Z}_p\setminus\{1,2\}) = \sum_{k=1}^{p-3}\sum_{i=0}^{k}(-1)^i N(k-i,-2i-1,\mathbb{Z}_p\setminus\{1\}) \\ &= \sum_{k=1}^{p-3}\sum_{i=0}^{k}\frac{(-1)^i}{p}\left(\binom{p-1}{k-i}+(-1)^{k-i}v(-k-i-1)\right) \\ &= \frac{2^{p-2}-1}{p}+\frac{(-1)^{(p-1)/2}+1}{2p} = \frac{2^{p-1}-1}{2p}+\frac{(-1)^{\frac{p-1}{2}}}{2}. \end{aligned}$$

Then, since b could take any value in $\mathbb{Z}_p^*$ (with a changing accordingly from 2 above to $2b \pmod p$), the total for case (ii) is $(p-1)\times$ this sum.

The number of solutions in case (iii), for the choice $b=1$, is (as in (6))

$$\begin{aligned} S_3 &= \sum_{k=0}^{p-3} N(k,0,\mathbb{Z}_p\setminus\{0,1\}) = \sum_{k=0}^{p-2}\frac{1}{p}\left(\binom{p-2}{k}+(-1)^k(p-k-1)\right) \\ &= \frac{2^{p-1}+p-1}{2p}. \end{aligned}$$

Again, b could take any value in $\mathbb{Z}_p^*$, so the total for case (iii) is $(p-1)\times$ this sum.

For case (iv), with the choice $b=p-1$ (so $c=a-b=a+1$ and $a\neq 2b=p-2$), by Lemma 4, the number of solutions is

$$\begin{aligned} S_4 &= \sum_{a=0}^{p-3}\sum_{k=1}^{p-3} N(k,1,\mathbb{Z}_p\setminus\{a,a+1,p-1\}) \\ &= \sum_{a=0}^{p-3}\sum_{k=1}^{p-3}\sum_{i=0}^{k}(-1)^i N(k-i,i+1,\mathbb{Z}_p\setminus\{a,a+1\}) \\ &= \sum_{a=0}^{p-3}\sum_{k=1}^{p-3}\sum_{i=0}^{k}\sum_{j=0}^{k-i}(-1)^{i+j} N(k-i-j,i+1-j(a+1),\mathbb{Z}_p\setminus\{a\}) \\ &= \sum_{a=0}^{p-3}\sum_{k=1}^{p-3}\sum_{i=0}^{k}\sum_{j=0}^{k-i}(-1)^{i+j} N(k-i-j,i+1-j(a+1)-(k-i-j)a,\mathbb{Z}_p^*) \\ &= \sum_{a=0}^{p-3}\sum_{k=1}^{p-3}\sum_{i=0}^{k}\sum_{j=0}^{k-i}(-1)^{i+j}\frac{\left(\binom{p-1}{k-i-j}+(-1)^{k-i-j}v(i+1-j+(i-k)a)\right)}{p} \\ &= \frac{(2^{p-3}-1)(p-2)}{p}+\frac{p-3}{2p} = \frac{2^{p-3}(p-2)}{p}-\frac{p-1}{2p}, \end{aligned}$$

using the fact that, for $a \neq 0$, $N(k, b, \mathbb{Z}_p \setminus \{a\}) = N(k, b - ka, \mathbb{Z}_p \setminus \{0\})$. Again, the total is $(p-1)\times$ this sum, since any given choice of $(a, a+1, -1)$ above can be multiplied by any $b \in \mathbb{Z}_p^*$.

Lastly, for case (v), again with the choice $b = p-1$ (so $c = a+b = a-1$ and $a \neq b, p$), the number of solutions is

$$\begin{aligned}
S_5 &= \sum_{c=0}^{p-3}\sum_{k=1}^{p-3} N(k, 0, \mathbb{Z}_p \setminus \{c, c+1, p-1\}) \\
&= \sum_{c=0}^{p-3}\sum_{k=1}^{p-3}\sum_{i=0}^{k}\sum_{j=0}^{k-i}(-1)^{i+j} N(k-i-j, i-j(c+1), \mathbb{Z}_p \setminus \{c\}) \\
&= \sum_{c=0}^{p-3}\sum_{k=1}^{p-3}\sum_{i=0}^{k}\sum_{j=0}^{k-i}(-1)^{i+j} N(k-i-j, i-j(c+1)-(k-i-j)c, \mathbb{Z}_p^*) \\
&= \sum_{c=0}^{p-3}\sum_{k=1}^{p-3}\sum_{i=0}^{k}\sum_{j=0}^{k-i}(-1)^{i+j}\frac{1}{p}\left(\binom{p-1}{k-i-j} + (-1)^{k-i-j} v(i-j+(i-k)c)\right) \\
&= \frac{2^{p-3}(p-2)}{p} + p - 2 + \frac{1}{2p} + \frac{(-1)^{\frac{p-1}{2}}}{2}.
\end{aligned}$$

And again, the total is $(p-1)\times$ this sum.

Adding the counts for cases (ii)-(v) (each for a single choice of b) then gives

$$S_2 + S_3 + S_4 + S_5 = 2^{p-2} + p - 2 + (-1)^{\frac{p-1}{2}}$$

So we conclude that

$$\begin{aligned}
\sigma_{av}(L_{p,+}) &= \frac{S_1 + (p-1)\times[S_2 + S_3 + S_4 + S_5]}{2^{p-1}} \\
&= \frac{(p^2 - p + 2)2^{p-2} + (p-1)^3 + (p^2-p)(-1)^{\frac{p-1}{2}}}{p\,2^{p-1}} \\
&= \left[\frac{1}{2}\left(1 - \frac{1}{p} + \frac{2}{p^2}\right) + O\left(\frac{p}{2^{p-1}}\right)\right] p.
\end{aligned}$$

Therefore, $\sigma_{av}(L_{p,+})/p < \frac{1}{2}$ for p sufficiently large. □

We wrote a computer program to directly calculate the sensitivity per bit $\sigma_{av}(L_{n,+})/n$ for values $2 \leq n \leq 32$, and similarly for $L_{n,0}$ and L_n. Figure 1 shows our findings (values at integers n are connected by lines for visual clarity); these results are also listed in the Appendix. Note: for $n \neq p$, then $L_{n,0} = L_{n,+}$; for $n = p$ or $n = p-1$, then $L_n = L_{n,+}$.

The analysis for the sensitivity of L_{n+} may be done for other values of n, as the reader can suspect, however, the general case does not seem too simple since the bounds for the N counts used in our analysis are not strong enough to give the tight bounds for the sensitivity.

Certainly, other cryptographic properties can be investigated. We wrote a program which computes the (Hamming) nonlinearity (that is, the minimum Hamming distance to the set of all affine functions [9]) of the x_1–laced functions and we report here some preliminary observations. We found that

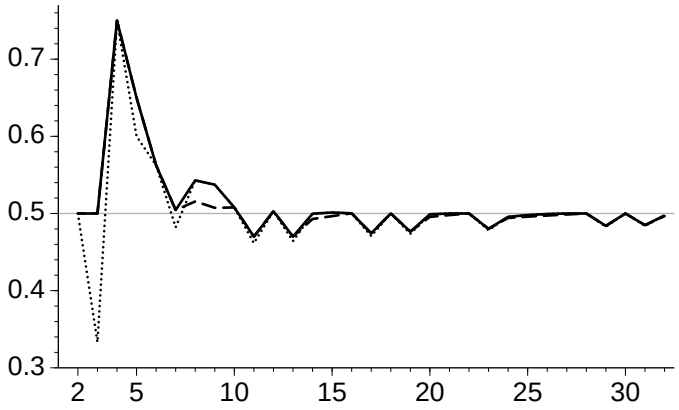

Figure 1: Sensitivity per bit of $L_{n,+}$ (solid), $L_{n,0}$ (dotted), L_n (dashed), for $n \leq 32$

for $n \geq 10$, x_1 seems to be the closest function whose corresponding distance gives the nonlinearity (this is natural as in many cases we force L_n to equal x_1). If that were to be proved, then the nonlinearity can certainly be computed since we know that the truth table of the function x_1 is simply the concatenation of the pattern 01, 2^{n-1} number of times. That can be accomplished by a method not too different than the one contained in this paper. Moreover, we observed that the nonlinearity seems to increase as the distance between n and the next prime increases.

Acknowledgement

We gratefully thank the reviewers for the detailed and excellent comments, which improved the quality of the paper.

References

[1] George Gasper and Mizan Rahman, *Basic Hypergeometric Series*, 2nd Edition, (2004), Encyclopedia of Mathematics and Its Applications, 96, Cambridge University Press, Cambridge.

[2] S.A. Cook, C. Dwork, and R. Reischuk, "Upper and lower time bounds for parallel random access machines without simultaneous writes", *SIAM J. Comp.* 15 (1986), 87–97.

[3] J. Li, D. Wan, "On the subset sum problem over finite fields", *Finite Fields & Applic.* 14 (2008), 911–929.

[4] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, New York, Oxford, 1977.

[5] N. Nisan,"CREW PRAMs and decision trees", *SIAM J. Comput.* 20 (1991), no. 6, 999–1070.

[6] M. Sauerhoff, "Quantum vs. classical read-once branching programs", preprint 2005, 1–35; see http://arxiv.org/abs/quant-ph/0504198.

[7] P. Savický, S. Žák, "A read-once lower bound and a $(1, +k)$-hierarchy for branching programs", *Theoret. Comput. Sci.* 238 (2000), 347–362.

[8] I. Shparlinski, "Bounds on the Fourier coefficients of the weighted sum function", *Inform. Process. Lett.* 103 (2007), 83–87.

[9] Y. Zheng, X.-M. Zhang, H. Imai, "Restriction, terms and nonlinearity of Boolean functions", *Theoret. Comput. Sci.* 226 (1999), 207–223.

Appendix

Table 1: Sensitivity of the Laced Boolean Functions.
Note: for $n \neq p$, then $L_{n,0} = L_{n,+}$; for $n = p$ or $n = p - 1$, then $L_n = L_{n,+}$.

		Laced Function		
n	p	$L_{n,0}$	$L_{n,+}$	L_n
1	2	$\Longrightarrow$	1.000000	$\Longleftarrow$
2	2	0.500000	0.500000	$\Longleftarrow$
3	3	0.333333	0.500000	$\Longleftarrow$
4	5	$\Longrightarrow$	0.750000	$\Longleftarrow$
5	5	0.600000	0.650000	$\Longleftarrow$
6	7	$\Longrightarrow$	0.562500	$\Longleftarrow$
7	7	0.482143	0.504464	$\Longleftarrow$
8	11	$\Longrightarrow$	0.542969	0.515625
9	11	$\Longrightarrow$	0.537326	0.507378
10	11	$\Longrightarrow$	0.507812	$\Longleftarrow$
11	11	0.461648	0.469993	$\Longleftarrow$
12	13	$\Longrightarrow$	0.502930	$\Longleftarrow$
13	13	0.464243	0.470177	$\Longleftarrow$
14	17	$\Longrightarrow$	0.499721	0.492868
15	17	$\Longrightarrow$	0.501274	0.496570
16	17	$\Longrightarrow$	0.500244	$\Longleftarrow$
17	17	0.470818	0.474279	$\Longleftarrow$
18	19	$\Longrightarrow$	0.500061	$\Longleftarrow$
19	19	0.473742	0.476512	$\Longleftarrow$
20	23	$\Longrightarrow$	0.498964	0.495687
21	23	$\Longrightarrow$	0.500033	0.497941
22	23	$\Longrightarrow$	0.500005	$\Longleftarrow$
23	23	0.478265	0.480156	$\Longleftarrow$
24	29	$\Longrightarrow$	0.495695	0.494256
25	29	$\Longrightarrow$	0.497934	0.495863
26	29	$\Longrightarrow$	0.499338	0.497348
27	29	$\Longrightarrow$	0.500001	0.498723
28	29	$\Longrightarrow$	0.500000	$\Longleftarrow$
29	29	0.482759	0.483948	$\Longleftarrow$
30	31	$\Longrightarrow$	0.500000	$\Longleftarrow$
31	31	0.483871	0.484912	$\Longleftarrow$
32	37	$\Longrightarrow$	0.497466	0.496622