Proving a conjecture of V. Strehl on necklaces

Proving a conjecture of V. Strehl on necklaces

N.G. de Bruijn

Technological University Eindhoven
Department of Mathematics and Computing Science
PO Box 513, 5600MB Eindhoven, The Netherlands

1. Introduction

With a fixed positive integer n we consider the set B_n of all 2^n binary sequences, i.e., the sequences of n digits which are all 0 or 1.

We introduce the mapping $C : B_n \to B_n$ defined by

$$C\ (\varepsilon_{n-1} \cdots \varepsilon_0)\ =\ (\varepsilon_{n-2} \cdots \varepsilon_0 \varepsilon_{n-1}).$$

The powers C^j provide the cyclic permutations of the sequences.

Moreover we consider the operation T that replaces zeros by ones and vice versa:

$$T\ (\varepsilon_{n-1} \cdots \varepsilon_0)\ =\ (\delta_{n-1} \cdots \delta_0),$$

where

$$\delta_{n-1}\ =\ 1 - \varepsilon_{n-1},\ \ \cdots\ , \delta_0\ =\ 1 - \varepsilon_0.$$

Two elements of B_n are called *equivalent* if we get from the one to the other by some C^j or by some $C^j\ T$ (in both cases with $0 \le j < n$). For example, if $n = 8$ then 10110111, 01111011, 10000100 and 00100100 are pairwise equivalent. The equivalence classes are sometimes called *necklaces*.

In each equivalence class we take the lowest representative, where the word "lowest" refers to the standard order in B_n, i.e., the lexicographic order we get by considering the sequences as binary numbers. And we make a list of these lowest representatives, arranged in standard order.

Volker Strehl studied these ordered lists of lowest representatives for various values of n, always omitting the lowest case $0 \cdots 0$. In Appendix 1 these lists are displayed for $n = 2, \ldots, 9$.

It is trivial that in each one of the lists the first column consists of 0's only (if a sequence starts with 1 then the operation T will lead to a lower one), and the last column consists of 1's only (if a sequence ends with 0 then the operation C^{n-1} leads to a lower one, unless the sequence was $0\cdots 0$). But Strehl made (in 1987) a more surprising observation that is by no means easy to explain: the entries in the $(n-1)$-st column are 0 and 1 in strict alternation! With today's desk computers it is not hard to investigate this for values of n up to 24 or a little more, and no exceptions are found. Strehl conjectured that it remains true for all n. He also noted that the last entry in the $(n-1)$-st column is always 0.

At first sight the conjecture seems to be weird and difficult to attack, since we can think of no simple relation between consecutive sequences of the list. But we get a better insight if, instead of concentrating on the sequences of the list, we study the sequences that have *not* been admitted. In order to express this, we introduce the notion of good and bad sequences, and of the badness index.

If a sequence is the lowest representative of its equivalence class, it will be called *good*, otherwise *bad*.

If a sequence σ is bad, the *badness index* is defined as the least value of j that establishes the badness. If $T\sigma < \sigma$ the badness index is zero, and otherwise it is the smallest positive j such that $C^j\sigma < \sigma$ or $C^jT\sigma < \sigma$.

Finally we shall use the term *odd sequence* for any sequence that ends with 1 (which means that the binary number represented by the sequence is an odd integer).

We get the ordered list of lowest representatives if we start from the list of *all* odd 2^{n-1} sequences of length n, and delete the bad sequences. Between two good sequences there can occur a set of consecutive bad ones. We shall call such sets *blocks*. Strehl's conjecture can now be expressed by saying that every block consists of an *even number* of bad sequences. Omitting blocks of even length from the full list will not disturb the perfect alteration of 0's and 1's in the $(n-1)$-st column. Note that we do not mind that the number of bad sequences at the *end* of the list might be odd. They do not lie *between* a pair of good sequences.

In Appendix 2 the full lists are displayed for some values of n. If the sequence is bad, the badness index is printed on the right. In order to save space, the second half of the list is omitted from $n = 5$ onwards. The sequences of the second half all start with 1, and therefore they have index 0. There is not much to observe in the cases $n = 3, 4, 5$. The first time we have something *between* two good sequences is at $n = 6$ with a block of 4 sequences with index 2. With $n = 7$ we have a block consisting of 2 bad sequences with index 3 between the good sequences 0001101 and 0010011.

In all cases that can be handled experimentally we note that the blocks have even length. And for a long time we think to observe that all the bad sequences in a block have the same badness index. But that is *not* generally true. In Appendix 3 there is a counterexample, provided by a fragment of the full list with $n = 17$. It shows a block consisting of 546 consecutive bad sequences between two good ones. In that block the badness index is *not* constant. First we have 2 sequences with index 12, then 30 sequences with index 8, and finally 514 sequences with index 4.

We note that these numbers 2, 30, 514 are all even. Strehl's conjecture indicates only that the *sum* of them is even. Wherever we look we note that the separate numbers are all even themselves, so we have discovered something stronger than Strehl's conjecture. And this stronger statement can actually be proved. We have as a theorem:

Theorem 1.1. For any natural number n the ordered list of all 2^{n-1} odd sequences has the property that for every pair σ_1, σ_2 of good sequences the set of bad sequences lying between σ_1 and σ_2 can be dissected into a number of disjoint subsets $G_1, \dots, G_h$, where

(i) each G_i is a set of an even number of consecutive sequences from the list,
(ii) in each G_i all sequences have the same badness index.

For the proof we refer to section 4.

2. Reformulation of badness

The sequences of B_n can be considered as the binary representations of the integers x in the set I_n, which is the set of all integers in the interval $0 \le x < 2^n$.

From now on we shall express ourselves in terms of those integers. In particular the notions of badness and badness index (with respect to n) will be used for those x. The operations C and T lead directly to mappings $f_C : I_n \to I_n$ and $f_T : I_n \to I_n$, where we agree that $y = f_C(x)$ means that C maps the binary representation of x into the one of y, and similarly for f_T.

The action of f_T is simply $f_T(x) = 2^n - 1 - x$ for all $x \in I_n$. f_T and f_C obviously commute.

If j is any integer with $1 \le j < n$, we can represent any $x \in I_n$ as $x = 2^{n-j}q + r$ with $0 \le q < 2^j$ and $0 \le r < 2^{n-j}$. The action of f_C^j can now be described by

$$f_C^j(2^{n-j}q + r) = 2^j r + q,$$

and the one of $f_T f_C^j$ by

$$f_T f_C^j(2^{n-j}q + r) = 2^n - 1 - 2^j r - q.$$

As remarked before, the integers x with $x \ge 2^{n-1}$ are all bad, just because of $f_T(x) < x$. So we do not loose anything of any interest if we assume that $x < 2^{n-1}$.

If x is bad and $0 < x < 2^{n-1}$, then there is an integer j with $1 \le j < n$ such that condition $P_{n,j}(x)$ holds, where $P_{n,j}(x)$ stands for the statement that at least one of $f_C^j(x)$ and $f_T f_C^j(x)$ is less than x. This condition can be reformulated in two ways:

Theorem 2.1. If x is an integer with $0 < x < 2^{n-1}$, then the condition that $P_{n,j}(x)$ does not hold is equivalent to

$$x \le y \le 2^n - 1 - x,$$

where y is the uniquely determined integer with

$$0 < y < 2^n - 1, \; y \equiv 2^j x \pmod{2^n - 1}.$$

Proof. Trivial.

Theorem 2.2. If x is an integer with $0 < x < 2^{n-1}$ and $1 \le j < n$, then $P_{n,j}(x)$ holds if and only if there is an integer q with $0 < q < 2^j$ such that

$$q(2^n - 1)/(2^j + 1) < x < q(2^n - 1)/(2^j - 1). \tag{2.1}$$

Proof. Throughout the proof we assume $1 \le j < n$, $0 < x < 2^{n-1}$.

We note that $f_C^j(x)$ is the integer uniquely determined by

$$0 < f_C^j(x) < 2^n - 1, \quad f_C^j(x) \equiv 2^j x \pmod{2^n - 1}.$$

Now first assume $f_C^j(x) < x$. We write $2^j x = Q(2^n - 1) + R$ with $0 \le R < 2^n - 1$. So $f_C^j(x) = R$, and therefore $0 \le R < x$. This means $Q(2^n - 1) \le 2^j x$ and $(2^j - 1)x < Q(2^n - 1)$. We have $Q > 0$ since $R < x \le 2^j x$, and $Q < 2^j$ since $Q(2^n - 1) \le 2^j x < 2^j(2^n - 1)$. So we have proved the existence of an integer q with

$$0 < q < 2^j, \quad (2^n - 1)q/2^j \le x < (2^n - 1)q/(2^j - 1). \tag{2.2}$$

Conversely assume the existence of an integer q with (2.2). Then we have $2^j x \ge (2^n - 1)q$ and $2^j x < (2^n - 1)q + x < (2^n - 1)(q + 1)$ (note that $x < 2^n - 1$). So $0 \le 2^j x - (2^n - 1)q < 2^n - 1$, whence $f_C^j(x) = 2^j x - (2^n - 1)q$ and therefore $f_C^j(x) < x$.

Secondly assume $f_C^j(x) > 2^n - 1 - x$. Again we write $2^j x = Q(2^n - 1) + R$ with $0 \le R < 2^n - 1$, whence $f_C^j(x) = R$ and $R > 2^n - 1 - x$.

From $2^j x - (2^n - 1)Q = R < 2^n - 1$ we infer that $x < (2^n - 1)(Q + 1)/2^j$. On the other hand we derive from $R > 2^n - 1 - x$ that $(2^n - 1)(Q + 1)/(2^j + 1) < x$.

We have $Q \ge 0$, so $Q + 1 > 0$. On the other hand $(2^n - 1)Q \le 2^j x$, $x < 2^n - 1$ whence $Q < 2^j$.

It takes some trouble to show that even $Q + 1 < 2^j$. We have

$$(2^n - 1)(Q + 1) < (2^n - 1)Q + R + x = (2^j + 1)x \le (2^j + 1)(2^{n-1} - 1).$$

Now the assumption $Q + 1 \ge 2^j$ would lead to $(2^n - 1)2^j < (2^j + 1)(2^{n-1} - 1)$, so $2^{n+j-1} < 2^{n-1} - 1$, which is absurd.

Thus we have proved the existence of an integer q such that

$$0 < q < 2^j, \quad (2^n - 1)q/(2^j + 1) < x < (2^n - 1)q/2^j. \tag{2.3}$$

Conversely assume the existence of an integer q with (2.2). Putting $Q = q - 1$, $R = 2^j x - (2^n - 1)Q$ we find $R + x = (2^j + 1)x - (2^n - 1)Q > (2^n - 1)(Q + 1) - (2^n - 1) = 2^n - 1$, whence $R > 2^n - 1 - x$ and $R > 0$. On the other hand it follows from $x < (2^n - 1)q/2^j$ that $R < 2^n - 1$. Since also $R \equiv 2^j x \pmod{2^n - 1}$ we infer $f_C^j(x) > 2^n - 1 - x$.

So we have proved that $f_C^j(x) < x$ is equivalent to the existence of an integer q with $0 < q < 2^j$ that satisfies (2.1), and $f_T f_C^j(x) < x$ is equivalent to the existence of such a q with (2.3). Since $P_{n,j}(x)$ is the disjunction of the two conditions, the theorem follows.

As a simple application of Theorem 2.2 we can take $j = 1$, $q = 1$, which shows that all x with $(2^n - 1)/3 < x < 2^n - 1$ are bad. The boundary case $x = (2^n - 1)/3$ (which occurs if n is even) is good. If $n > 2$ it is also a boundary point of the open interval from $(2^n - 1)/5$ to $(2^n - 1)/3$, which contains bad numbers only (take $j = 2$, $q = 1$ in (2.1)).

Another application is the case that x is even. There we can take $q = x/2$, $j = n - 1$.

3. A perfectly dominated set of intervals on the real line

We develop some terminology about sets of intervals on the real line, although the same words might be used about sets of sets in general.

If Λ is a set of intervals then an element $I \in \Lambda$ is called a *dominant* if all $J \in \Lambda$ that have a non-empty intersection with I are entirely contained in I.

We say that Λ is *perfectly dominated* if for every $J \in \Lambda$ there is a dominant $I \in \Lambda$ with $I \supset J$.

If Λ is perfectly dominated then its dominants are obviously pairwise disjoint.

A trivial example of a perfectly dominated set is the set of all intervals on the real line that do not contain any integers. Its dominants are the open intervals between consecutive integers.

A non-trivial perfectly dominated set Ω is suggested by Theorem 2.2. The elements of Ω are $V_{j,q}$, where j is a positive integer and q is an integer restricted by $0 < q \leq (2^j - 1)/3$. Each $V_{j,q}$ is an open interval on the positive real axis:

$$V_{j,q} \ = \ (\ q/(2^j + 1) \ , \ q/(2^j - 1) \ ).$$

(We use the notation (a, b) for the set of all reals between a and b.)

The connection with Theorem 2.2 is that $P_{n,j}(x)$ means that there is some q with $0 \leq q < 2^j$ such that $x(2^n - 1)^{-1} \in V_{j,q}$. This statement contains the letter n, but in the study of Ω in the present section the n will play no role.

Some of the $V_{j,q}$ will turn out to be dominants. If $V_{j,q}$ is a dominant, we will say that (j, q) is a *dominant pair*.

Theorem 3.1. If j and q are positive integers with $0 < q \leq (2^j - 1)/3$, then the condition for the pair (j, q) to be dominant can be expressed as $E_{j,q}$, where

$E_{j,q} \equiv$ there do not exist integers i and s with $i \geq 0$ and $-q < s < q$ such that $2^i q - s$ is divisible by either $2^j - 1$ or $2^j + 1$.

Proof. Since we have open intervals only, the condition that $V_{j,q}$ is a dominant is equivalent to the condition that no $V_{i,r} \in \Omega$ contains an end-point of $V_{j,q}$.

The formula

$$r/(2^i+1) < q/(2^j+1) < r/(2^i-1)$$

is equivalent to

$$2^iq - q < (2^j+1)r < 2^iq + q,$$

and similarly for (2^j-1) instead of (2^j+1). It follows that $V_{j,q}$ being a dominant is equivalent to $F_{j,q}$, where

$F_{j,q} \equiv$ for all positive integers i and all integers r with $0 < r \leq (2^i-1)/3$ both $(2^j-1)r$ and $(2^j+1)r$ lie outside the open interval $(2^iq-q, 2^iq+q)$.

Now first assume that $V_{j,q}$ is a dominant. Both $(2^j-1)r$ and $(2^j+1)r$ lie outside the open interval $(2^iq-q, 2^iq+q)$, not just for the r with $0 < r \leq (2^i-1)/3$ but for all integers r. If $r \leq 0$ this holds since 2^iq-q is positive, and if $r > (2^i-1)/3$ we have $3r \geq 2^i+1$ ($3r$ cannot be a power of 2) so both $(2^j-1)r$ and $(2^j+1)r$ are at least $(2^j-1)(2^i+1)/3$, which is at least 2^iq+q.

We conclude that there do not exist integers i and s with $i > j$ and $-q < s < q$ such that 2^iq-s is divisible by either 2^j-1 or 2^j+1. So we have proved $E_{j,q}$.

Conversely, assume $E_{j,q}$. It follows that for all positive integers i and all integers r both $(2^j-1)r$ and $(2^j+1)r$ lie outside the open interval $(2^iq-q, 2^iq+q)$. In particular this holds if we add the restriction $0 < r \leq (2^i-1)/3$, so we have $F_{j,q}$, and therefore $V_{j,q}$ is a dominant. This finishes the proof of Theorem 3.1.

Theorem 3.3. Ω is perfectly dominated, i.e., for every $V_{j,q} \in \Omega$ there is a dominant $I \in \Omega$ with $I \supset V_{j,q}$.

Proof. We proceed by induction with respect to j. If $V_{j,q}$ is a dominant itself, there is nothing to prove. So assume that $V_{j,q}$ is not a dominant. By Theorem 3.1 there exist integers i and s with $i \geq 0$ and $-q < s < q$ such that 2^iq-s is divisible by either 2^j-1 or 2^j+1. Let $i = kj+h$, where $k \geq 0$ and $0 \leq h < j$. Since $2^j \equiv 1 \pmod{2^j-1}$, $2^j \equiv -1 \pmod{2^j+1}$ we have an integer v such that $-q < v < q$ and 2^hq-v is divisible by either 2^j-1 or 2^j+1.

With some integer w we have $2^iq - v = w(2^j+c)$, where c is either -1 or 1. So $q/(2^j+c) = w/(2^i - v/q)$. Since v/q lies between -1 and 1, we conclude that one of the end-points of $V_{j,q}$ is an interior point of the interval $(w/(2^i+1), w/(2^i-1))$.

We shall show that $0 < w \leq (2^i-1)/3$. From $q/(2^j+c) = w/(2^i-v/q)$ we see that $w > 0$ and $3w < 3q(2^i+1)/(2^j-1) \leq 2^i+1$. Since $3w$ cannot be a power of 2 we infer that $3w \leq 2^i-1$ indeed. So $V_{i,w}$ belongs to Ω. Since $i < j$ this $V_{i,w}$ is contained in some dominant I, according to the induction hypothesis.

Some interior point of $V_{i,w}$ is an end-point of $V_{j,q}$, and therefore $V_{i,w}$ and $V_{j,q}$ have a point in common. That point belongs to I. So $V_{i,w}$ has a point in common with I. The fact that I is a dominant entails that $I \supset V_{i,w}$, which completes the proof.

The dominant pairs (j,q) with $2 \leq j \leq 12$ are listed In Appendix 4.

In material of this kind many regularities can be observed, some of which can be proved. We postpone these things to Section 6; here we only prove Theorem 3.3 since we need it in the proof of Strehl's conjecture.

Theorem 3.3. If (j, q) is a dominant pair then q is odd.

Proof. If q is even the definition of the V's shows at once that $V_{j,q}$ is a proper subset of $V_{j-1,q/2}$. So $V_{j,q}$ cannot satisfy the definition of dominants.

Theorem 3.4. If ξ is a real number such that there exists an $I \in \Omega$ with $\xi \in I$, and if j is the smallest number such that there exists a q with $0 < q \le (2^j - 1)/3$ and $\xi \in V_{j,q}$, then $V_{j,q}$ is a dominant.

Proof. It follows from the definition of the intervals V that if $V_{j,q} \in \Omega$, $V_{i,r} \in \Omega$ and $V_{j,q} \subset V_{i,r}$ then $i < j$ unless both $i = j$ and $q = r$. Now Theorem 3.4 follows from Theorem 3.3.

The following theorem is a decisive step to the proof of Theorem 1.1:

Theorem 3.5. If $V_{j,q}$ is a dominant, n any positive integer, and if $N_{j,q,n}$ stands for the number of odd integers m such that $m/(2^n - 1) \in V_{j,q}$ then $N_{j,q,n}$ is even.

Proof. As a preparation we remark that if X and Y are integers with $X < Y$, and either $Y - X \equiv 1 \pmod 4$ or $Y + X \equiv 0 \pmod 4$ then the number of odd integers m with $X < m < Y$ is even:

$$2\lfloor (Y - X)/4 \rfloor. \tag{3.1}$$

Here we use the standard notation for floor and ceiling: the *floor* $\lfloor x \rfloor$ of a real number ξ is the largest integer $\le \xi$, and the ceiling $\lceil \xi \rceil$ is the smallest integer $\ge \xi$.

We also remark that if ξ and η are real numbers and m is an integer, the condition $\xi < m < \eta$ is equivalent to $\lfloor \xi \rfloor < m < \lceil \eta \rceil$. So $N_{j,q,n}$ is the number of odd integers m with $X < m < Y$, where

$$X = \lfloor q(2^n - 1)/(2^j + 1) \rfloor, \quad Y = \lceil q(2^n - 1)/(2^j - 1) \rceil.$$

We shall prove the theorem by showing that $Y - X \equiv 1 \pmod 4$ or $Y + X \equiv 0 \pmod 4$.

We begin by reducing n, defining k and b by $n = kj + b$, $0 \le b < j$. This results in

$$X = M - K + \lfloor q((-1)^k 2^b - 1)/(2^j + 1) \rfloor, \quad Y = M + \lceil q(2^b - 1)/(2^j - 1) \rceil, \tag{3.2}$$

where

$$M = 2^b q \sum_{i=0}^{k-1} 2^{(k-1-i)j}, \quad K = 2 \cdot 2^b q \sum_{i} 2^{(k-1-i)j},$$

and in the second sum the summation is restricted to the *odd* values of i in the interval $0 \le i \le k - 1$.

In order to investigate the floors and ceilings we write

$$2^b q \;=\; A(2^j+1)+R, \tag{3.2}$$

$$2^b q \;=\; A(2^j-1)+2A+R, \tag{3.4}$$

with $0 \le R < 2^j+1$. Since $V_{j,q}$ is a dominant we infer from Theorem 3.1 that

$$q \le R \le 2^j+1-q. \tag{3.5}$$

By (3.2) we have $0 \le A < 2^b q/(2^j+1)$, so from $b < j$ we conclude that $0 \le A < q/2$.

We first deal with Y. Trivially $Y = M$ if $b = 0$. If $b > 0$ we shall show that $Y = M + A + 1$.

We write $(2^b-1)q = A(2^j-1)+2A+R-q$ and have to show that $0 < 2A+R-q \le 2^j-1$. Since $2A < q$ we have $2A+R-q < R$. By (3.5) R is at most 2^j, $2A+R-q \le 2^j-1$. For a lower estimate we use $2A+R-q \ge R-q \ge 0$, and we shall show that $2A+R-q = 0$ is impossible.

Suppose $2A+R-q = 0$. We have $A \ge 0$, and $R-q \ge 0$ by (3.5), and therefore both $R-q$ and $2A$ are equal to 0. Now (3.4) gives $(2^b-1)q = 0$, which contradicts the assumption that $b > 0$. Thus we have proved that $2A+R-q$ is strictly positive and $\le 2^j-1$. which leads to $Y = M+A+1$.

Next we treat X, dealing separately with the cases that k is odd or even.

First assume that k is even. If $b = 0$ we have simply $X = M-K$. If $b > 0$ we note that (3.5) gives $0 \le R-q < 2^j+1$,which leads to $\lfloor q(2^b-1)/(2^j+1)\rfloor = A$. Therefore $X = M-K+A$.

Next we turn to the case that k is odd. If k is odd and $b = 0$ we have $X = M-K+\lfloor -2q/(2^j+1)\rfloor$. The definition of Ω implies $0 < q \le (2^j-1)/3$, whence $2q < 2^j+1$. Therefore $X = M-K-1$.

If k odd and $b > 0$ we only have to note that (3.2) and (3.5) lead to $-A-1 \le q(2^b+1)/((2^j-1) < -A$. It follows that $X = M-K-A-1$.

Having determined X and Y in all cases, we can finish the proof. First we note that $j > 1$ (this follows from the definition of Ω). And b and k can not be both equal to 0 (since $n > 0$). Therefore $M \equiv 2^b q \pmod 4$, $K \equiv 2\cdot 2^b q \pmod 4$.

If k is even and $b = 0$ we have $X = M-K$, $Y = M$ whence $X+Y \equiv 0 \pmod 4$.

If k is even and $b > 0$ we have $X = M-K+A$, $Y = M+A+1$ and $K \equiv 0 \pmod 4$, whence $Y - X \equiv \pmod 4$.

If k is odd and $b = 0$ we have $X = M-K-1$, $Y = M$ and $xK \equiv 0 \pmod 4$, whence $Y - X \equiv \pmod 4$.

If k is odd and $b > 0$ we have $X = M-K-A-1$, $Y = M+A+1$, and $K \equiv 2M \equiv \pmod 4$, whence $X+Y \equiv 0 \pmod 4$.

The proof of Theorem 3.5 is now complete.

Remark. Our proof provides the following value for $N_{j,q,n}$:

$$N_{j,q,n} \;=\; (1-(-1)^k)\lfloor (A+1)/2\rfloor + 2\lfloor K/4\rfloor, \tag{3.6}$$

where $n \geq 1$, $j \geq 1$, $0 < q \leq (2^j-1)/3$, $n = kj+b$, $A = \lfloor q2^b/(2^j+1)\rfloor$, and K is given by (3.2) ($K = 0$ if $k = 0$).

4. Proof of Theorem 1.1

We shall show that Theorem 1.1 is an easy consequence of what we have done thus far.

We take a fixed value of n and first get rid of the x with $x > (2^n-1)/3$. If $x = 2^n-1$ then x is bad because of $f_T(x) = 0 < x$. If $(2^n-1)/3 < x < 2^n-1$ we have (2.1) with $j = 1$, $q = 1$, so x is bad by Theorem 2.2.

From now on we assume $0 < x \leq (2^n-1)/3$. If q satisfies (2.1) with some j ($1 \leq j < n$) we have $q(2^n-1) < (2^j+1)x$, whence $3q < 2^j+1$. Since $3q$ cannot be a power of 2 it follows that $3q \leq 2^j-1$. Therefore x is bad if and only if x lies in some interval belonging to Ω. Its badness index is the smallest value of j such that there is a $V_{j,q}$ containing $x/(2^n-1)$. By Theorem 3.4 this $V_{j,q}$ is a dominant.

Let us write V_n for the union of all dominants $V_{j,q}$ with $j < n$. Then for the integers x in the interval $0 < x \leq (2^j-1)/3$ we can say that x is bad if and only if $x/(2^n-1) \in V_n$, and if x is bad, its badness index is the j with $x/(2^n-1) \in V_{j,q}$.

Restricting ourselves to the odd values of x in $0 < x \leq (2^j-1)/3$, we get directly to what is expressed in Theorem 1.1. The bad values of x are those for which $x/(2^n-1)$ falls in V_n, and in each one of the intervals $V_{j,q}$ contributing to V_n we have an even number of such x (according to Theorem 3.5), all with the same badness index j. The remaining odd values of x, those for which $x/(2^n-1)$ lies outside V_n, are all good.

5. Further properties of the dominant pairs

From computer generated material we can observe a number of regularities that can lead to conjectures or theorems.

First we note:

(i) If (j,q) is dominant then $(j+1,q)$ is dominant.
This is not hard to prove by means of Theorem 3.1. More generally it looks as if we also have

(ii) If (j,q) is dominant and i a non-negative integer, then $(j+2^i, 2^iq+2^i-1)$ is dominant,
but that seems to be less simple.

(iii) For every positive odd number q the pair (j,q) is dominant for all sufficiently large j.

This can be proved by means of Theorem 3.1, but also from Theorem 5.1.

Next we can observe the relation between Strehl's lists of good sequences (minimal representatives) and the lists of q's. Let us denote by R_n the set of all good sequences of length n, this time *not* excluding the all-zero sequence. And ρ_n stands for the number of elements of R_n. So

$$\rho_1 = 1,\ \rho_2 = 2,\ \rho_3 = 2,\ \rho_4 = 4,\ \rho_5 = 4,\ \rho_6 = 8,\ \rho_7 = 10,$$

$$\rho_8 = 20,\ \rho_9 = 30,\ \rho_{10} = 56,\ \rho_{11} = 94,\ \rho_{12} = 180,\ \cdots.$$

For every $j > 1$ the set of q with $0 < q \leq (2^j - 1)/3$ and such that $V_{j,q}$ is a dominant will be denoted by T_n. We also define T_1 as consisting of the number 1 only. The number of elements of T_n is called τ_n. So

$$\tau_1 = 1,\ \tau_2 = 1,\ \tau_3 = 1,\ \tau_4 = 2,\ \tau_5 = 3,\ \tau_6 = 5,\ \tau_7 = 9,$$

$$\tau_8 = 16,\ \tau_9 = 28,\ \tau_{10} = 51,\ \tau_{11} = 93,\ \tau_{12} = 170, \cdots.$$

We observe that for every n we have

$$\rho_n = \sum_{d|n} \tau_d \tag{5.1}$$

(the sum runs over all divisors d of n). This can be proved indeed as a direct consequence of Theorem 5.1 below.

The number ρ_n is the number of equivalence classes under the group of $2n$ elements generated by the C^j and T (see Section 1), and can be found by means of the Cauchy-Frobenius lemma (also called Burnside's lemma), with the result

$$\rho_n \ = \ (2n)^{-1} \sum_{d|n} 2^d \psi(n/d), \tag{5.2}$$

where $\psi(n) = \phi(n)$ if n is odd, $\psi(k) = 2\phi(k)$ if k is even, and ϕ is Euler's function. In combination with (5.1) this gives a simple expression for τ_n:

$$\tau_n \ = \ (2n)^{-1} \sum_{d|n,\ d \text{ odd}} \mu(d) 2^{n/d} \tag{5.3}$$

(the sum runs over all odd divisors d of n). Here μ is the Möbius function.

In order to compare the R_n's and T_n's we introduce the sets W_n. For every $q \in T_n$ we take its n-bit binary representation (which is a sequence of zeros and ones that may start with a number of zeros), and W_n is the set of all those sequences. For example

$$T_6 \ = \ \{1, 3, 5, 7, 11\},\ W_6 \ = \ \{000000, 000001, 000011, 000101, 000111, 001011\}.$$

A sequence of n zeros and ones will be called *repetitive* if it is obtained by t-fold repetition of a sequence of d zeros and ones, where d and t are integers with $td = n$, $t > 1$. Example: 010110101101011 is repetitive ($d = 5$, $t = 3$).

It is easy to see that by t-fold repetition of an element of R_d we get an element of R_{td}, and, conversely, if by t-fold repetition of an arbitrary d-bit sequence σ we get an element of R_n then $\sigma \in R_d$.

If we compare W_6 with

$$R_6 \;=\; \{000000, 000001, 000011, 000101, 000111, 001001, 001011, 010101\}$$

we note that W_6 is exactly the set of all non-repetitive elements of R_6 (the repetitives are 001001 and 010101). This is generally expressed in Theorem 5.1.

A consequence is that R_n can be obtained from the sets W_d where d runs through the divisors of n, just by (n/d)-fold repetition of each element of W_d. This can be demonstrated in the example with $n = 6$ with the divisors 1, 2, 3 and 6. The elements of W_6 need no repetition at all. The element 001 of W_3 produces 001001 by repetition, the element 01 of W_2 produces 010101 and the element 0 of W_1 produces 000000.

Theorem 5.1. For any positive integer n the set W_n is the set of all non-repetitive elements of R_n.

Proof. We have to show (i), (ii), (iii), where

(i) $W_n \subset R_n$.

(ii) W_n does not contain any repetitive elements.

(iii) If σ is an element of R_n that does not belong to W_n, then σ is repetitive.

First we prove (i). If $q \in T_n$ we know from Theorem 3.2 that there do not exist integers i and s with $i \geq 0$ and $-q < s < q$ such that $2^i q - s$ is divisible by either $2^j - 1$ or $2^j + 1$. According to Theorem 2.1 the weaker statement with divisibility by $2^j - 1$ alone guarantees that the binary representation of q belongs to R_n.

In order to prove (ii) we assume that a number $q \in T_n$ has a repetitive binary representation. Since the cases $q = 0$ and $q = 2n - 1$ are excluded, there are numbers r and A with $1 < r < n$ and $0 < A < 2^r$ such that $2^r q = A(2^n - 1) + q$. Since $2(2^r - 1) < 2^n - 1$ we infer that $2A < q$.

So in $2^r q = A(2^n + 1) + q - 2A$ we have $0 < q - 2A < q$. Now Theorem 3.1, applied with $s = q - 2A$, establishes a contradiction.

Finally we deal with (iii). Let $\varepsilon_{n-1} \cdots \varepsilon_0$ be an element of R_n that does not belong to W_n, and let q be the number that has $\varepsilon_{n-1} \cdots \varepsilon_0$ as its binary representation. We can assume that $q > 0$ since $0 \cdots 0$ is repetitive. It follows from Theorems 2.1 and 3.1 that there are numbers i and s with $i \geq 0$ and $-q < s < q$ such that $2^i q - s$ is divisible by $2^n + 1$. Since $2^n \equiv -1 \pmod{2^n + 1}$ we can assume that $0 < i < n$. We write $q = 2^{n-i} u + v$ with $0 \leq v < 2^{n-i}$, $0 \leq u < 2^i$. Putting $y = 2^i v + u$ we have $0 \leq y < 2^{n-1}$ and $y \equiv 2^i q \pmod{2^n - 1}$. Since $\varepsilon_{n-1} \cdots \varepsilon_0 \in R_n$ Theorem 2.1 shows that $q \leq y \leq 2^n - 1 - q$ (the case $y = 0$ is trivial here).

Since $2^i q \equiv 2^n u + 2^i v \equiv 2^i v - u \pmod{2^n + 1}$ we have $2^i v - u \equiv s \pmod{2^n + 1}$. Moreover $2^i v - u \leq 2^i v + u = y \leq 2^{n-1} - q$ and $2^i v - u \geq -u > -q$. So $2^i v - u$ and s are both $> -q$ and $\leq 2^{n-1} - q$. Therefore $2^i v - u \equiv s \pmod{2^n + 1}$ leads to $2^i v - u = s$, whence $2^i v - u < q$. This can be written as

$$\varepsilon_{n-i-1} \cdots \varepsilon_0 \, 0 \cdots 0 - \varepsilon_{n-1} \cdots \varepsilon_{n-i} \;<\; \varepsilon_{n-1} \cdots \varepsilon_0 .$$

Since $q \leq y$ we also have

$$(5.4) \qquad \varepsilon_{n-i-1} \cdots \varepsilon_0 \, 0 \cdots 0 + \varepsilon_{n-1} \cdots \varepsilon_{n-i} \;\geq\; \varepsilon_{n-1} \cdots \varepsilon_0,$$

and we conclude that

$$(5.5) \qquad \varepsilon_{n-i-1} \cdots \varepsilon_0 \;=\; \varepsilon_{n-1} \cdots \varepsilon_i.$$

From (5.4) it follows that

$$(5.6) \qquad \varepsilon_{n-1} \cdots \varepsilon_{n-i} \;\geq\; \varepsilon_{i-1} \cdots \varepsilon_0.$$

A second application of the fact that $\varepsilon_{n-1} \cdots \varepsilon_0$ belongs to R_n leads to

$$\varepsilon_{n-1} \cdots \varepsilon_0 \;\leq\; \varepsilon_{i-1} \cdots \varepsilon_0 \varepsilon_{n-1} \cdots \varepsilon_i.$$

So we have (5.6) with $\leq$ instead of $\geq$. It follows that

$$(5.7) \qquad \varepsilon_{n-1} \cdots \varepsilon_{n-i} \;=\; \varepsilon_{i-1} \cdots \varepsilon_0.$$

From (5.5) and (5.7) we conclude that

$$\varepsilon_{(k+i) \bmod n} \;=\; \varepsilon_k$$

for $0 \leq k < n$ ($(k+i) \bmod n$ is the residue when dividing $k+i$ by n). If d is the greatest common divisor of i and n we find that also $\varepsilon_{(k+d) \bmod n} = \varepsilon_k$ for all those k, and, moreover, d is less than n and a divisor of n, which means that $\varepsilon_{n-1} \cdots \varepsilon_0$ is repetitive.

This completes the proof of Theorem 5.1.

6. Final remarks

1. Let V be the union of all intervals I with $I \in \Omega$. This V covers a considerable part of the interval $(0, 1/3)$. In particular all fractions $q/2^k$ in that interval (where q and k are positive integers) belong to V, just because $q/2^k \in V_{k,q}$.

By Theorem 3.2 the set V is the disjoint union of all dominants.

The complement U of V (i.e., the set $(0, 1/3) \setminus V$) is nowhere dense (every interval contains a sub-interval that has nothing in common with U). It can also be shown to have Lebesgue measure zero. We sketch a proof here.

If j and q are positive integers, an ξ is a real number, the condition $\xi \in V_{j,q}$ is equivalent to $2^j \xi \in (q - \xi, q + \xi)$. Therefore U is the set of all real numbers ξ with $0 < \xi < 1/3$ such that for all positive integers j we have

$$\xi \leq 2^j \xi - \lfloor 2^j \xi \rfloor \leq 1 - \xi.$$

Let r be any positive integer, put $M = 2^r$ and let W be the set of all numbers ξ with $0 \leq x \leq 1$ such that for all j we have $2^{-r} \leq 2^j \xi - \lfloor 2^j \xi \rfloor$. This W is a subset of the set of real numbers in the unit interval with the property that in the M-ary number system the digit 0 does not occur, and therefore W has measure zero. Since $U \subset (0, 2^{-r}) \cap W$ the measure of U is at most $2-r$. Since this holds for all r, the measure of U is zero.

2. For technical reasons we have introduced the restriction $0 < q \leq (2^j - 1)/3$ in the definition of Ω, but it is not essential. If we replace that restriction by $0 < q \leq (2^j - 1)$ we get just one more dominant, viz. the interval $(1/3, 1)$ (the case $i = 1$, $q = 1$), and almost all of section 3 remains true, in particular Theorem 3.5. It is easy to show that the number of odd numbers m with $2^n - 1 < 3m < 3(2^n - 1)$ is an even number (just check the values of $2^n \pmod 6$), and therefore $N_{1,1,n}$ is even. In connection with Theorem 2.2 it was remarked already that all x with $1/3 < (x/(2^n - 1)) < 1$ are bad.

3. Applying this to Strehl's lists we can show that the last entry in each list of lowest representatives ends with the digits 01. The last entry of the list of *all* binary n-digit numbers is $11 \cdots 11$, but that one does not belong to the set of x with $1/3 < (x/(2^n - 1)) < 1$. The number of bad cases *between* the last one of the lowest representatives and this $11 \cdots 11$ is even. Therefore that last lowest representative ends with 01.

A different proof for the same statement depends on the fact that once we know the correctness of Strehl's conjecture it suffices to show that for every n Strehl's list has an odd number of sequences, which means that the last entry has the same pair of digits at the end as the first one. It is not hard to show this by means of (5.2).

A third proof can be given by remarking that the last item of Strehl's list is $010101 \cdots 01$ if n is even and $0010101 \cdots 01$ if n is odd. It is not hard to show by simple combinatorial reasoning, without any use of algebra, that these sequences are good, and that there are no good sequences beyond them.

We indicate an argument for the latter statement in the case that n is odd. It shows that all sequences beyond $0010101 \cdots 01$ are bad, because every sequence is equivalent to a sequend that is *not* beyond $0010101 \cdots 01$.

If in a necklace there is a sub-sequence of more than two equal bits, these can be shifted to the beginning and turned into zeros, whence we have something less than $0010101 \cdots 01$. So we assume that there are no sub-sequences of more than two equal bits. Since n is odd, there should be at least one pair of equal bits. If there is just one such pair, the necklace is equivalent to $0010101 \cdots 01$ itself. If there are more than one, there are at least two of them with an odd number of bits in between. If the first pair is 00, the bits in between are a sub-sequence of the form $1010 \cdots 101$, and the second pair is again 00. If the first pair is 11 the situation is similar. Therefore the necklace is equivalent to a sequence of the form $001010 \cdots 10100 \cdots$, and that is less than $0010101 \cdots 01$.

APPENDIX 1

Lists of all good sequences (without the all-zero sequences):

n = 2	3	4	5	6	7	8	9
01	001	0001	00001	000001	0000001	00000001	000000001
		0011	00011	000011	0000011	00000011	000000011
		0101	00101	000101	0000101	00000101	000000101
				000111	0000111	00000111	000000111
				001001	0001001	00001001	000001001
				001011	0001011	00001011	000001011
				010101	0001101	00001101	000001101
					0010011	00001111	000001111
					0010101	00010001	000010001
						00010011	000010011
						00010101	000010101
						00010111	000010111
						00011001	000011001
						00011011	000011011
						00100101	000011101
						00101011	000100011
						00101101	000100101
						00110011	000100111
						01010101	000101001
							000101011
							000101101
							000110011
							000110101
							000110111
							001001001
							001001011
							001001101
							001010011
							001010101

APPENDIX 2

Full lists with indication of badness index (for n>4 the second half of the list, consisting of the sequences starting with 1, is omitted; they are all bad, with index 1):

n=3		n=4		n=5	
001		0001		00001	
011	1	0011		00011	
101	0	0101		00101	
111	0	0111	1	00111	2
		1001	0	01001	2
		1011	0	01011	1
		1101	0	01101	1
		1111	0	01111	1

n=6

000001		001001		010001	2	011001	1
000011		001011		010011	2	011011	1
000101		001101	2	010101		011101	1
000111		001111	2	010111	1	011111	1

n=7

0000001		0010001	3	0100001	2	0110001	1
0000011		0010011		0100011	2	0110011	1
0000101		0010101		0100101	2	0110101	1
0000111		0010111	4	0100111	2	0110111	1
0001001		0011001	4	0101001	2	0111001	1
0001011		0011011	2	0101011	1	0111011	1
0001101		0011101	2	0101101	1	0111101	1
0001111	3	0011111	2	0101111	1	0111111	1

APPENDIX 3

A fragment of the full list with n=17:

```
00001110111011011
00001110111011101
00001110111011111  12
00001110111100001  12
00001110111100011   8
00001110111100101   8
***************** (26 further sequences with index 8)
00001111000011011   8
00001111000011101   8
00001111000011111   4
00001111000100001   4
***************** (510 further sequences with index 4)
00010001000011111   4
00010001000100001   4
00010001000100011
00010001000100101
```

APPENDIX 4

Dominant pairs.

```
j= 2.  List of values for q:
 1

j= 3.  List of values for q:
 1

j= 4.  List of values for q:
 1 3

j= 5.  List of values for q:
 1 3 5

j= 6.  List of values for q:
 1 3 5 7 11
```

```
j= 7.  List of values for q:
 1 3 5 7 9 11 13 19 21

j= 8.  List of values for q:
 1 3 5 7 9 11 13 15 19 21 23 25 27 37 43 45

j= 9.  List of values for q:
 1  3  5  7  9 11 13 15 17 19 21 23 25 27
29 35 37 39 41 43 45 51 53 55 75 77 83 85

j= 10.  List of values for q:
   1   3   5   7   9  11  13  15  17  19  21  23  25  27  29
  31  35  37  39  41  43  45  47  49  51  53  55  57  59  69
  71  73  75  77  83  85  87  89  91  93 101 103 105 107 109
 147 149 155 171 173 179

j= 11.  List of values for q:
  1   3   5   7   9  11  13  15  17  19  21  23  25  27  29  31
 33  35  37  39  41  43  45  47  49  51  53  55  57  59  61  67
 69  71  73  75  77  79  81  83  85  87  89  91  93  99 101 103
105 107 109 111 113 115 117 119 137 139 141 147 149 151 153 155
157 163 165 167 169 171 173 179 181 183 185 199 201 203 205 211
213 215 217 219 293 299 301 307 309 331 333 339 341

j= 12.  List of values for q:
  1   3   5   7   9  11  13  15  17  19  21  23  25  27  29  31
 33  35  37  39  41  43  45  47  49  51  53  55  57  59  61  63
 67  69  71  73  75  77  79  81  83  85  87  89  91  93  95  97
 99 101 103 105 107 109 111 113 115 117 119 121 123 133 135 137
139 141 143 145 147 149 151 153 155 157 163 165 167 169 171 173
175 177 179 181 183 185 187 189 197 199 201 203 205 207 209 211
213 215 217 219 221 227 229 231 233 235 237 239 275 277 279 281
283 285 291 293 295 297 299 301 307 309 311 313 315 327 329 331
333 339 341 343 345 347 349 355 357 359 361 363 365 371 397 403
405 407 409 411 421 423 425 427 429 435 437 439 441 587 589 595
597 603 613 619 661 683 685 691 693 717
```