6

Binary Periodic Synchronizing Sequences

Marcin Skubiszewski

May 1991

Publication Notes

This article will also appear in *Theoretical Computer Science*, Part A, Volume 99 (October 1992).

Author's electronic address: `skubi@prl.dec.com`

© Digital Equipment Corporation 1991

This work may not be copied or reproduced in whole or in part for any commercial purpose. Permission to copy in whole or in part without payment of fee is granted for non-profit educational and research purposes provided that all such whole or partial copies include the following: a notice that such copying is by permission of the Paris Research Laboratory of Digital Equipment Centre Technique Europe, in Rueil-Malmaison, France; an acknowledgement of the authors and individual contributors to the work; and all applicable portions of the copyright notice. Copying, reproducing, or republishing for any other purpose shall require a license with payment of fee to the Paris Research Laboratory. All rights reserved.

Abstract

In this article, we consider words over $\{0, 1\}$. The *autodistance* of such a word is the lowest among the Hamming distances between the word and its images by circular permutations other than identity; the word's *reverse autodistance* is the highest among these distances. For each $l \geq 2$, we study the words of length l whose autodistance and reverse autodistance are close to $l/2$ (we call such words *synchronizing sequences*).

We establish, for every $l \geq 3$, an upper bound on the autodistance of words of length l. This upper bound, called up (l), is very close to $l/2$.

We briefly describe the maximal period linear recurring sequences, a previously known family of words over $\{0, 1\}$; such words exist for every length of the form $l = 2^n - 1$ and their autodistances achieve the upper bound up (l).

Examples of words whose autodistance and reverse autodistance are both equal or close to up (l) are discussed; we describe the method (based on simulated annealing) which was used to find the examples.

We prove that, for sufficiently large l, an arbitrarily high proportion of words of length l will have both their autodistance and reverse autodistance very close to up (l).

Résumé

Nous considérons dans cet article des mots sur $\{0, 1\}$. Nous appelons *autodistance* d'un tel mot la plus petite des distances de Hamming entre lui-même et ses images par des permutations circulaires non identiques; l'*autodistance inverse* du mot désigne la plus grande de ces distances. Pour tout $l \geq 2$, nous étudions les mots de longueur l dont l'autodistance et l'autodistance inverse sont toutes les deux proches de $l/2$ (de tels mots seront appelés *suites synchronisantes*).

Pour tout $l \geq 3$, nous établissons une borne supérieure sur l'autodistance des mots de longueur l. Cette borne supérieure, notée up (l), est très proche de $l/2$.

Nous présentons brièvement les suites linéairement récurrentes de période maximale, une famille déjà étudiée de mots sur $\{0, 1\}$; de tels mots existent pour toute longueur de forme $l = 2^n - 1$ et leur autodistance atteint la borne up (l).

Nous considérons des exemples de mots dont l'autodistance et l'autodistance inverse sont toutes les deux proches de up (l) ou égales à cette valeur; nous décrivons la méthode (une adaptation du recuit simulé) qui a permis de trouver ces exemples.

Nous prouvons que, pour l suffisamment grand, l'autodistance et l'autodistance inverse sont très proches de up (l) pour une proportion arbitrairement élevée des mots de longueur l.

Keywords

Autocorrelation, autodistance, synchronizing sequences, spread-spectrum communications, multiplexing by code division; linear recurring sequences; simulated annealing.

Contents

1 Introduction

1.1 Subject of the article

Modern radio techniques, including radar and spread-spectrum communications, make use of finite sequences of bits exhibiting various *correlation properties* (*e.g.* [5], [2] chapters 10 and 12, [1]). The correlation properties of a sequence measure how easily it can be distinguished, after a transmission with errors, from other related sequences (the notion of *related sequences* is application-dependent).

We study here two correlation properties, the *autodistance* and the *reverse autodistance*. The autodistance measures how well, in the worst case, the receiver will be able to distinguish between the sequence and a non-identical circular permutation of it (in this case, we consider that circular permutations of a sequence are related to it). The reverse autodistance measures the difficulty that the receiver will have, in the worst case, distinguishing between the sequence and a circular permutation of its one's complement (here, we consider that circular permutations of the one's complement of a sequence are related to the sequence).

In this study, we focus on searching for, and estimating the number of, sequences that exhibit a high autodistance (the *synchronizing sequences*) and those that exhibit both a high autodistance and a low reverse autodistance (the *double synchronizing sequences*).

1.2 Contents

Section 2 of the article introduces the necessary notation and mathematical objects (including precise definitions of autodistance and reverse autodistance).

In Section 3, we investigate which values the autodistance and reverse autodistance can attain. We establish, for each length l, an upper bound on the autodistance of sequences of this length (Section 3.1); we complete this basic result with several remarks about the reverse autodistance of certain classes of sequences (Sections 3.2–3.3).

In Sections 4-6, we either find, or prove the existence of, sequences whose autodistance and reverse autodistance approach the previously established bounds.

In Section 4, quoting already known results [4], we introduce the *maximal period linear recurring sequences*, a family of double synchronizing sequences which achieve the bounds for certain lengths l.

In Section 5, we describe examples of double synchronizing sequences whose lengths are between 3 and 405; these examples achieve, or almost achieve, the bounds. We present a computational method, based on *simulated annealing*, which we used to find the examples.

In Section 6, we establish a theorem implying that among very long sequences of bits, almost all have their autodistances and reverse autodistances close to the respective bounds.

2 Definitions and Notation

2.1 Basic notation

$i \sqcap j$	greatest common divisor (GCD) of $i, j \in \mathbf{N}$
$[a \,..\, b]$	interval $\left\{ \; i \in \mathbf{Z} \;\middle|\; a \le i \le b \; \right\}$
$[a \,..\, b)$	interval $\left\{ \; i \in \mathbf{Z} \;\middle|\; a \le i < b \; \right\}$
$\mathbf{N}_{2+}$	set of natural numbers ≥ 2
$\{0,1\}^{2+}$	set of words over $\{0,1\}$ of length ≥ 2
$\{0,1\}^{l}$	for $l \in \mathbf{N}_{2+}$, set of words over $\{0,1\}$ of length l
$\lvert S\rvert$ $\quad \lvert E\rvert$	length of the word $S \in \{0,1\}^{2+}$; cardinality of the set E
$\lvert S\rvert_0$ $\quad \lvert S\rvert_1$	number of *zeros* (resp. *ones*) in $S \in \{0,1\}^{2+}$
$(F_x)_{x \in X}$	the family of elements F_x, indexed by elements $x \in X$; by definition, $\lvert (F_x)_{x \in X}\rvert = \lvert X\rvert$
$\lvert \mathcal{F}\rvert_A$	number of elements of the family $\mathcal{F}$ belonging to the set A; if $\mathcal{F} = (F_x)_{x \in X}$, then

$$\lvert \mathcal{F}\rvert_A = \left| \left\{ \; x \in X \;\middle|\; F_x \in A \; \right\} \right|$$

$A \triangle B$	symmetrical difference between sets: $A \triangle B = (A \cup B) - (A \cap B)$
$x A$	for $x \in \mathbf{R}$ and $A \subset \mathbf{R}$, the set $\left\{ \; xy \;\middle|\; y \in A \; \right\}$; the definitions of $A + x$ and $A - x$ are analogous
$S[i]$	for $S \in \{0,1\}^{2+}$ and $0 \le i < \lvert S\rvert$, the i-th digit of S
τ_p	circular permutation by p of words from $\{0,1\}^{2+}$:

$$\tau_p(S)[i] \quad = \quad S\left[(i + p) \bmod \lvert S\rvert\right]$$

$\mathrm{d}(S, T)$	for $S, T \in \{0,1\}^{l}$, the Hamming distance between S and T:

$$\mathrm{d}(S, T) = \left| \left\{ \; i \in [0 \,..\, l) \;\middle|\; S[i] \neq T[i] \; \right\} \right|$$

2.2 Notation of objects defined in the article

$\mathrm{d}(S)$	for $S \in \{0,1\}^{2+}$, the autodistance of S (Definition 1 below)
$\mathrm{d}'(S)$	for $S \in \{0,1\}^{2+}$, the reverse autodistance of S (Definition 2 below)
$\mathrm{up}(l)$	for $l \in \mathbf{N}, l \ge 3$, $\mathrm{up}(l) = 2 \lfloor (l + 1)/4 \rfloor$ (Definition 7 below)

2.3 Autodistance and synchronizing sequences

Definition 1 (autodistance) *For $S \in \{0,1\}^{2+}$, the* autodistance *of S is the minimum of the Hamming distances between S and all its images by circular permutations other than identity:*

$$\mathrm{d}(S) = \min_{p \in [1 \,..\, \lvert S\rvert)} \mathrm{d}\left(S, \tau_p(S)\right)$$

Definition 2 (reverse autodistance) *For* $S \in \{0,1\}^{2+}$*, the* reverse autodistance *of* S *is the maximum of the Hamming distances between* S *and all its images by circular permutations:*

$$\mathrm{d}'(S) = \max_{p \in [0\,..\,|S|)} \mathrm{d}\left(S, \tau_p(S)\right)$$

Examples: The null word of any length satisfies $\mathrm{d}(S) = \mathrm{d}'(S) = 0$. The words `001` and `0011` satisfy

$$\begin{aligned} \mathrm{d}(\texttt{001}) = \mathrm{d}'(\texttt{001}) &= 2 \\ \mathrm{d}(\texttt{0011}) &= 2 \\ \mathrm{d}'(\texttt{0011}) &= 4 \end{aligned}$$

Definition 3 (optimal synchronizing sequence) *An* optimal synchronizing sequence *of length* $l \in \mathbf{N}_{2+}$ *is a word* $S \in \{0,1\}^l$ *whose autodistance is maximal; in symbols,* $S \in \{0,1\}^l$ *is an optimal synchronizing sequence if and only if*

$$\forall (T \in \{0,1\}^l)\ \mathrm{d}(T) \leq \mathrm{d}(S)$$

Informally, we call any word $S \in \{0,1\}^l$ *whose autodistance is maximal or nearly maximal a* synchronizing sequence *of length* l*.*

Definition 4 (double-optimal synchronizing sequence) *A* double-optimal synchronizing sequence *of length* $l \in \mathbf{N}_{2+}$ *is a word* $S \in \{0,1\}^l$ *whose autodistance is maximal, and whose reverse autodistance is minimal among all words in* $\{0,1\}^l$ *having the maximal autodistance; in symbols,* $S \in \{0,1\}^l$ *is a double-optimal synchronizing sequence if and only if*

$$\forall (T \in \{0,1\}^l)\ \mathrm{d}(T) < \mathrm{d}(S) \vee \left(\mathrm{d}(T) = \mathrm{d}(S) \wedge \mathrm{d}'(T) \geq \mathrm{d}'(S)\right)$$

Informally, any word $S \in \{0,1\}^l$ *whose autodistance is maximal or nearly maximal and whose reverse autodistance is, among the words having the same autodistance as* S*, minimal or nearly minimal, will be called a* double synchronizing sequence *of length* l*.*

Definition 5 (uniform sequence) *A* uniform sequence *is a word* $S \in \{0,1\}^{2+}$ *such that*

$$\mathrm{d}(S) = \mathrm{d}'(S)$$

It follows from Definitions 1 and 2 above that the sequence $S \in \{0,1\}^{2+}$ is uniform if and only if the number $\mathrm{d}(S, \tau(S))$, where τ is a non-identical circular permutation, does not depend on the choice of τ.

Examples: The null word of any length is a uniform sequence. A word of any length containing a unique `1` and having all other digits equal to `0` is a uniform sequence.

Definition 6 (uniform optimal synchronizing sequence) *A word from* $\{0,1\}^{2+}$ *is a* uniform optimal synchronizing sequence *if it is a uniform sequence and an optimal synchronizing sequence.*

Informally, any word from $\{0,1\}^{2+}$ *which is both a uniform sequence and a synchronizing sequence will be called a* uniform synchronizing sequence.

It follows from the definitions above that a uniform optimal synchronizing sequence is also a double-optimal synchronizing sequence.

Example: The word `001` is a uniform optimal synchronizing sequence. Long optimal synchronizing sequences are never trivial.

3 Bounds on Synchronizing Sequence Characteristics

Theorem 1 below establishes an upper bound on the autodistances of synchronizing sequences. Theorems 2 and 3 establish that uniform synchronizing sequences of certain forms do not exist. Theorem 4 states that all optimal synchronizing sequences in a certain category are uniform.

3.1 An upper bound on the autodistance

Theorem 1 (an upper bound on the autodistance) *For every* $l \in \mathbf{N}$, $l \geq 3$, *the autodistance of every word* $S \in \{0,1\}^l$ *is less than or equal to the value given in the following table (for* $n \in \mathbf{Z}$*):*

$l = \lvert S \rvert$	$\mathrm{d}(S)$
$4n$	$2n$
$4n+1$	$2n$
$4n+2$	$2n$
$4n+3$	$2n+2$

Definition 7 ($\mathrm{up}(l)$**)** *For every* $l \geq 3$, *the upper bound given in the table in Theorem 1 will be denoted* $\mathrm{up}(l)$.

In order to prove the theorem, let us establish two lemmas.

Lemma 1 (parity of $\mathrm{d}(S)$**)** *The autodistance of every word* $S \in \{0,1\}^{2+}$ *is even.*

Proof: By Definition 1, for some $p \in \mathbf{N}$ we have $\mathrm{d}(S) = \mathrm{d}\left(S, \tau_p(S)\right)$. It is therefore sufficient to prove that the Hamming distance between a word $S \in \{0,1\}^{2+}$ and any of its circular permutations is even.

Let T be a circular permutation of S. We define, for $x, y \in \{0, 1\}$, the four sets

$$A_{xy} = \left\{ \; i \in [0 \,..\, |S|) \;\; \middle| \;\; S[i] = x \wedge T[i] = y \; \right\}$$

which trivially have the following properties:

$$\begin{aligned} |S|_1 &= |A_{10}| + |A_{11}| \\ |T|_1 &= |A_{01}| + |A_{11}| \\ \mathrm{d}(S, T) &= |A_{01}| + |A_{10}| \end{aligned}$$

These equations, together with the fact that $|S|_1 = |T|_1$, imply

$$\mathrm{d}(S, T) = 2\,|A_{01}|$$

so $\mathrm{d}(S, T)$ is even. □

Lemma 2 (a weaker version of Theorem 1) *For $l \geq 3$, the autodistance of every word $S \in \{0, 1\}^l$ is less than or equal to $\lceil l/2 \rceil$.*

Proof: Let $S \in \{0, 1\}^l$. We define for $i \in [0 \,..\, l)$ and $x \in \{0, 1\}$:

$$N_x[i] = \left| \left\{ \; p \in [0 \,..\, l) \;\; \middle| \;\; \tau_p(S)[i] = x \; \right\} \right|$$

By definition of $\tau_p(S)$,

$$N_x[i] = \left| \left\{ \; p \in [0 \,..\, l) \;\; \middle| \;\; S[(i + p) \bmod l] = x \; \right\} \right|$$

and, regardless of i,

$$N_x[i] = |S|_x \tag{1}$$

Let us define the *total autodistance* of S, called K, as

$$K = \sum_{p=0}^{l-1} \mathrm{d}\left(S, \tau_p(S)\right) \tag{2}$$

By definition of $\mathrm{d}(S, T)$, K satisfies:

$$\begin{aligned} K &= \sum_{p=0}^{l-1} \left| \left\{ \; i \in [0 \,..\, l) \;\; \middle| \;\; S[i] \neq \tau_p(S)[i] \; \right\} \right| \\ &= \left| \left\{ \; (p, i) \in [0 \,..\, l)^2 \;\; \middle| \;\; S[i] \neq \tau_p(S)[i] \; \right\} \right| \\ &= \sum_{i=0}^{l-1} \left| \left\{ \; p \in [0 \,..\, l) \;\; \middle| \;\; S[i] \neq \tau_p(S)[i] \; \right\} \right| \\ &= \sum_{\substack{i \in [0 \,..\, l) \\ S[i]=0}} N_1[i] + \sum_{\substack{i \in [0 \,..\, l) \\ S[i]=1}} N_0[i] \\ &= \sum_{\substack{i \in [0 \,..\, l) \\ S[i]=0}} |S|_1 + \sum_{\substack{i \in [0 \,..\, l) \\ S[i]=1}} |S|_0 \qquad \text{(by (1))} \\ K &= 2\,|S|_0\,|S|_1 \end{aligned} \tag{3}$$

The autodistance of S is, by its definition, the minimum of the family $\left(\mathrm{d}\left(S, \tau_p(S)\right)\right)_{p \in [1\,..\,l)}$. Let us define the *average autodistance* of S, called M, as the average of the same family:

$$M = \frac{\sum_{p=1}^{l-1} \mathrm{d}\left(S, \tau_p(S)\right)}{l-1} \tag{4}$$

This definition implies that $M \geq \mathrm{d}(S)$.

Equations (2) and (4) and the fact that $\mathrm{d}(S, \tau_0(S)) = 0$, lead to the following expression of M:

$$\begin{aligned} M &= \frac{K}{l-1} \\ M &= \frac{2\,|S|_0\,|S|_1}{l-1} \quad \text{(by (3))} \end{aligned} \tag{5}$$

If l is even, M is maximal for $|S|_0 = |S|_1 = l/2$, and we have,

$$\begin{aligned} M &\leq \frac{2(l/2)(l/2)}{l-1} \\ M &\leq \frac{l}{2} + \frac{1}{2(1-1/l)} \end{aligned}$$

Since $l \geq 3$,

$$M < \frac{l}{2} + 1$$

Since $\mathrm{d}(S) \leq M$ and $\mathrm{d}(S) \in \mathbf{Z}$,

$$\mathrm{d}(S) \leq \frac{l}{2}$$

and the lemma holds for l even.

If l is odd, M is maximal for $|S|_0 = (l-1)/2$ and $|S|_1 = (l+1)/2$. We have therefore,

$$\begin{aligned} M &\leq \frac{2(l/2+1/2)(l/2-1/2)}{l-1} \\ M &\leq \frac{l+1}{2} \end{aligned} \tag{6}$$

Then,

$$\mathrm{d}(S) \leq \lceil l/2 \rceil$$

and the lemma holds for l odd. □

Proof of Theorem 1: Lemma 2 implies that, for $l \geq 3$, no word can have an autodistance greater than the value $\mathrm{d}(S)$ listed in the table below:

$l = \lvert S \rvert$	$\mathrm{d}(S)$
$4n$	$2n$
$4n+1$	$2n+1$
$4n+2$	$2n+1$
$4n+3$	$2n+2$

Lemma 1 says that no word can have an autodistance of the form $2n + 1$, which makes us deduce the table in Theorem 1 from the one above. □

3.2 Non existence of certain uniform sequences

Lemma 3 (domain of $\mathrm{d}'(S)$) *For any word $S \in \{0,1\}^l$, $l \in \mathbf{N}_{2+}$, the reverse autodistance of S is even and satisfies*

$$\mathrm{d}(S) \leq \mathrm{d}'(S) \leq l \tag{7}$$

Proof: Substituting $\mathrm{d}'(S)$ for $\mathrm{d}(S)$ in the proof of Lemma 1 gives the evenness of $\mathrm{d}'(S)$. Relation (7) results directly from the definitions of autodistance and reverse autodistance. □

Theorem 2 (nontrivial uniform sequences for $l-1$ prime) *Let $l \in \mathbf{N}_{2+}$ and let $l-1$ be prime. Then among the words $S \in \{0,1\}^l$, exactly those verifying one of the conditions*

$$|S|_0 = 0 \tag{8}$$
$$|S|_0 = 1 \tag{9}$$
$$|S|_0 = l \tag{10}$$
$$|S|_0 = l-1 \tag{11}$$

are uniform sequences.

Proof: The reader may easily verify the fact that each of the conditions (8)–(11) implies that S is a uniform sequence.

Supposing that $l-1$ is prime and that $S \in \{0,1\}^l$ is a uniform sequence, let us prove that one of relations (8)–(11) holds. From the definitions of autodistance and reverse autodistance, we get

$$\forall\, (p \in [1\,..\,l))\ \mathrm{d}(S) \leq \mathrm{d}\left(S, \tau_p(S)\right) \leq \mathrm{d}'(S)$$

which implies that M, the average autodistance of S defined as in the proof of Lemma 2, relation (4), satisfies

$$\mathrm{d}(S) \leq M \leq \mathrm{d}'(S)$$

Since $\mathrm{d}(S) = \mathrm{d}'(S)$, we successively get

$$\begin{aligned}
M &= \mathrm{d}(S) \\
M &\in 2\mathbf{N} \quad \text{(from Lemma (1))} \\
\frac{2\,|S|_0\,|S|_1}{l-1} &\in 2\mathbf{N} \quad \text{(from (5))} \\
|S|_0\,(1-|S|_0) &\in (l-1)\mathbf{N} \\
|S|_0 \in (l-1)\mathbf{N} \quad &\text{or} \quad (1-|S|_0) \in (l-1)\mathbf{N} \quad \text{(since } l-1 \text{ is prime)}
\end{aligned} \tag{12}$$

Relation (12) implies that one of the conditions (8)–(11) holds. □

Theorem 3 (uniform optimal synchronizing sequences) *Let* $l \in \mathbf{N}_{2+}$. *If one of the following holds*

i. $l = 4n$ *where* $n \in \mathbf{N}$ *and* $\sqrt{n} \notin \mathbf{N}$.

ii. $l = 4n + 1$ *where* $n \in \mathbf{N}$ *and* $\sqrt{8n+1} \notin \mathbf{N}$.

iii. $l = 4n + 2$ *where* $n \in \mathbf{N}$ *and* $\sqrt{3n+1} \notin \mathbf{N}$.

then no uniform sequence $S \in \{0,1\}^l$ *will satisfy the equality* $\mathrm{d}(S) = \mathrm{up}(l)$.

Proof: Suppose that $S \in \{0,1\}^l$ is a uniform sequence with $\mathrm{d}(S) = \mathrm{d}'(S) = \mathrm{up}(l)$. Then, reasoning as in the proof of Theorem 2, we can say that M, the average autodistance of S, satisfies

$$M = \mathrm{d}(S)$$

which, by (5), translates into

$$2\,|S|_0\,(l - |S|_0) = (l-1)\mathrm{up}(l) \tag{13}$$

If (i) holds, then $l = 4n$, and (13) becomes

$$|S|_0^2 - 4n\,|S|_0 + 4n^2 - n = 0$$

Solving this second degree equation in $|S|_0$, we deduce that (13) is equivalent to

$$|S|_0 = 2n + \sqrt{n} \quad \text{or} \quad |S|_0 = 2n - \sqrt{n}$$

which is impossible since $\sqrt{n} \notin \mathbf{N}$.

If (ii) holds, then (13) becomes

$$\begin{aligned} |S|_0^2 - (4n+1)\,|S|_0 + 4n^2 &= 0 \\ |S|_0 = \frac{1}{2}\left(4n + 1 + \sqrt{8n+1}\right) \quad &\text{or} \quad |S|_0 = \frac{1}{2}\left(4n + 1 - \sqrt{8n+1}\right) \end{aligned} \tag{14}$$

Recalling that the square root of a natural number is either natural or irrational, we deduce that $\sqrt{8n+1}$ is irrational. Therefore, the alternative (14) implies that $|S|_0$ is irrational, which is impossible.

If (iii) holds, then (13) becomes

$$\begin{aligned} |S|_0^2 - 2(2n+1)\,|S|_0 + (4n+1)n &= 0 \\ |S|_0 = 2n + 1 + \sqrt{3n+1} \quad &\text{or} \quad |S|_0 = 2n + 1 - \sqrt{3n+1} \end{aligned} \tag{15}$$

which is impossible since $\sqrt{3n+1} \notin \mathbf{N}$. □

3.3 Uniformity of certain sequences

Theorem 4 (certain sequences are uniform) *For* $l = 4n + 3$, $n \in \mathbf{N}$, *every word from* $\{0, 1\}^l$ *whose autodistance is equal to* $\mathrm{up}(l)$*, is a uniform optimal synchronizing sequence.*

Theorem 5 below says that sequences satisfying the hypotheses of Theorem 4 exist for $l = 2^n - 1$, $n \in \mathbf{N}_{2+}$. In Section 5.2 (Figure 2 and Table 1) examples of sequences are quoted for $l = 3, 7, 11, 15, 19, 23, 31, 35$.

Proof of Theorem 4: Let S satisfy the hypotheses of the theorem. Then S is, by Theorem 1 and by the definition of $\mathrm{up}(l)$, an optimal synchronizing sequence.

Let us prove that S is a uniform sequence. We use M, as defined by equation (4) in the proof of Lemma 2. Since l is odd, we can, as in the proof of Lemma 2, obtain inequality (6). This inequality and the fact that $\mathrm{d}(S) = \frac{l+1}{2}$ imply that $M \leq \mathrm{d}(S)$. Since M is, by its definition, greater than or equal to $\mathrm{d}(S)$, we get

$$M = \mathrm{d}(S)$$

The average and the minimum of the finite family of integers $\left(\mathrm{d}\left(S, \tau_p(S)\right)\right)_{p \in [1\,..\,l)}$ are then equal. All the numbers in the family are therefore equal and $\mathrm{d}'(S) = \mathrm{d}(S)$. □

4 Maximal Period Linear Recurring Sequences

Theorem 5 ($\mathrm{up}(l)$ **is optimal for** $l = 2^n - 1$**)** *For every* l *of the form* $l = 2^n - 1$, $n \in \mathbf{N}_{2+}$, *there exists a word* $S_n \in \{0, 1\}^l$ *verifying*

$$\mathrm{d}(S_n) = \mathrm{d}'(S_n) = \mathrm{up}(l) \tag{16}$$

Since this theorem is a straightforward corollary of known results, we will not quote the proof in its entirety. Instead, we only describe a way to construct the sequence S_n. The proof that this construction is correct and that the resulting S_n satisfies relation (16) is a direct consequence of well-known results from the theory of finite fields (see *e.g.* [4], paragraphs 2.11, 6.32, 6.33 and 7.44). The construction itself is discussed in detail by Sarwate and Pursley ([7], Section 3).

Construction: Let $\mathbf{GF}_2$ denote the Galois field of order 2 (*i.e.* the field composed of elements 0 and 1) and $\mathbf{GF}_2[X]$ denote the ring of polynomials over $\mathbf{GF}_2$.

For every $n \in \mathbf{N}_{2+}$, there exists in $\mathbf{GF}_2[X]$ at least one primitive polynomial of degree n (see [4], 2.11). Let us choose one such polynomial and call it P_n; the coefficients of P_n will be called $p_0, \cdots, p_n$ (with $p_n = 1$):

$$P_n(X) = p_0 + p_1 X + \cdots + p_n X^n$$

P_n can be used as the characteristic polynomial to build an infinite *linear feedback sequence* of bits S'_n. To build S'_n, we arbitrarily choose its first n bits $S'_n[0], \ldots, S'_n[n-1]$, with the only restriction that these bits may not be all equal to 0 (this gives us $2^n - 1$ different choices of S'_n). Then, we define the other bits of S'_n by the recurrence formula

$$0 = p_0 S'_n[i] + p_1 S'_n[i+1] + \cdots + p_n S'_n[i+n] \quad \text{(for any } i \in \mathbf{N}\text{)} \tag{17}$$

which translates into

$$S'_n[i+n] = p_0 S'_n[i] + p_1 S'_n[i+1] + \cdots + p_{n-1} S'_n[i+n-1] \quad \text{(for any } i \in \mathbf{N}\text{)} \tag{18}$$

The sequence S'_n is periodic and its least period is $l = 2^n - 1$ (see [4], 6.33). We define S_n to be the left factor of S'_n of length l (therefore S_n represents one period of S'_n). S_n satisfies (16) (see [4], 7.44).

Consequences of the theorem: Theorem 5 implies that for all values l of the form $2^n - 1$, the upper bound $\mathrm{up}(l)$ is achieved by some word from $\{0,1\}^l$. For these values of l the upper bound $\mathrm{up}(l)$ can therefore not be improved.

The results presented in the remainder of this article imply that, in fact, the upper bound $\mathrm{up}(l)$ is optimal or nearly optimal for *any* length l.

5 Example Double Synchronizing Sequences

5.1 How the examples have been found

Simulated annealing, the technique used here to find double synchronizing sequences, was first described by Kirkpatrick *et al.* [3]. Let us describe briefly both the technique and the way in which it has been adapted to our problem.

Simulated annealing is an optimization algorithm. It provides approximate solutions to difficult problems (*i.e.* to problems for which finding the global optimum would involve an extremely long computing time). More precisely, for a set $\mathcal{X}$, on which is defined a function, called *energy*, $\mathcal{E} : \mathcal{X} \to \mathbf{R}$, simulated annealing will try to find an element $x \in \mathcal{X}$ such that $\mathcal{E}(x)$ be as low as possible.

In our case, the algorithm is run separately for each value of l and we have $\mathcal{X} = \{0,1\}^l$. When searching for synchronizing sequences, we try to maximize $\mathrm{d}(x)$; therefore $\mathcal{E}(x) = -\mathrm{d}(x)$. When searching for double synchronizing sequences, we try both to maximize $\mathrm{d}(x)$ and to minimize $\mathrm{d}'(x)$. In this case, the choice of $\mathcal{E}$ is not obvious; after experimentation, the author chose $\mathcal{E}(x) = \mathrm{d}'(x) - 3\mathrm{d}(x)$, although various other formulas apparently lead to identical results.

Simulated annealing requires that for every $x \in \mathcal{X}$, a *set of neighbors* $\mathcal{N}(x)$ be defined. Intuitively, x and y are neighbors (*i.e.* $y \in \mathcal{N}(x)$) if they are similar in a way implying that

$\mathcal{E}(x) \approx \mathcal{E}(y)$. In our case, we consider that two words from $\{0,1\}^l$ are neighbors if their Hamming distance is equal to 0 or 1. For the two energy functions mentionned above, this implies that if $y \in \mathcal{N}(x)$, then respectively $|\mathcal{E}(x) - \mathcal{E}(y)| \leq 2$ or $|\mathcal{E}(x) - \mathcal{E}(y)| \leq 8$.

The simulated annealing algorithm is a loop composed of a high number of similar steps. In each step, the algorithm tries to update the *current solution* $x \in \mathcal{X}$. To do so, it randomly chooses a solution $y \in \mathcal{N}(x)$. Then, if y is better than x (*i.e.* $\mathcal{E}(y) \leq \mathcal{E}(x)$), y replaces x and becomes the current solution. Otherwise (*i.e.* if $\mathcal{E}(y) > \mathcal{E}(x)$) one of two possibilities is randomly selected: either, with probability $p = e^{(\mathcal{E}(x)-\mathcal{E}(y))/\theta}$, y replaces x and becomes the current solution or, with probability $1 - p$, x remains the current solution and y is discarded.

The current solution x present after the last step is output by the algorithm to be considered as its result.

The parameter θ is a positive real number, called *temperature*; it decreases slowly during the computation from a problem-dependent initial value to zero. Note that for θ very high, the algorithm reduces to randomly walking through the search space $\mathcal{X}$, regardless of the energy function (because for θ high, always $p \approx 1$); for $\theta \approx 0$, the algorithm descends quickly towards a local minimum of $\mathcal{E}$. For intermediate values of θ, the algorithm randomly walks through $\mathcal{X}$, visiting more frequently elements x with $\mathcal{E}(x)$ low.

5.2 What we can learn from the examples

The curve on Fig. 1 (and its magnified version, Fig. 2) shows, for each $l \in [3\,..\,405]$, the autodistance and the reverse autodistance of the best double synchronizing sequence found for the length l by simulated annealing. The autodistance can be compared to up(l), also shown on the figures. Table 1 reproduces part of these results.

5.2.1 The autodistance

For $3 \leq l \leq 42$, the autodistance of the examples is, with the exceptions of $l = 27$ and $l = 39$, equal to up(l). For the particular cases of $l = 27$ and $l = 39$, exhaustive searches showed that there are no synchronizing sequences with autodistance equal to up(l)[1]; the examples found for these two values of l are therefore optimal.

We are thus certain that, for $l \leq 42$ (as well as for $l = 45, 46, 49, 50, 54$, see Fig. 2), the simulated annealing program actually found optimal synchronizing sequences. For these values, with the exceptions of $l = 27$ and $l = 39$, the upper bound of Theorem 1 is exact. For $l = 27$ and $l = 39$, the maximal autodistance is less than up(l), and Theorem 1 could be improved to take this fact into account.

According to Theorem 5, for lengths of the form $l = 2^n - 1$, some sequences achieve the upper bound up(l). Therefore, for $l = 63, 127, 255$, the simulated annealing program found

[1] For $l = 39$, the exhaustive search was performed by Mark Shand [8] using a carefully optimized search program.

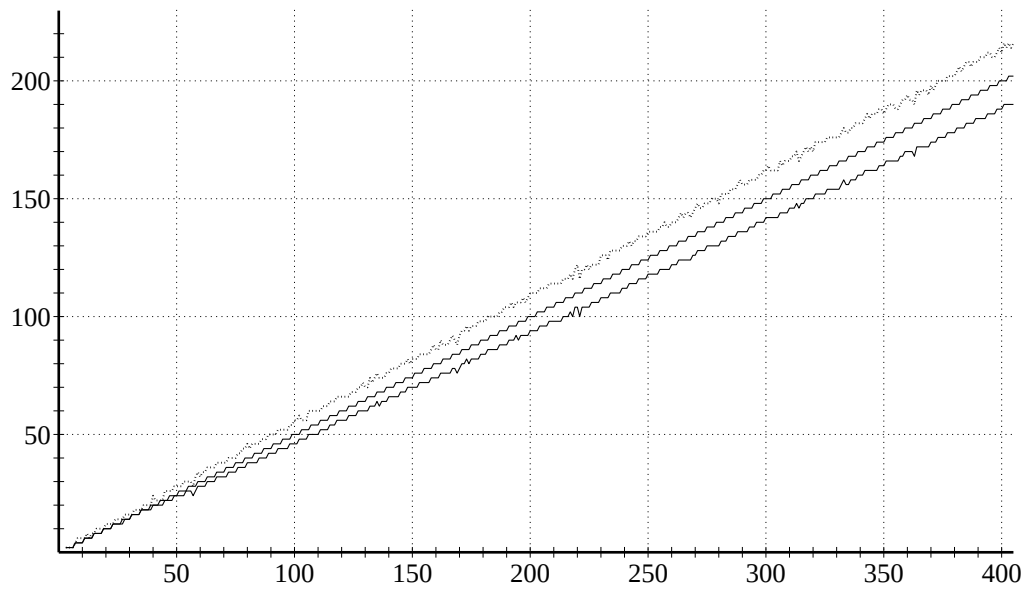

Figure 1: Autodistance and reverse autodistance of example sequences as a function of their lengths l. The lower line shows the autodistance of the best double synchronizing sequence found by simulated annealing for each length. The upper, dotted line shows the reverse autodistance of the same sequences. The middle, perfectly regular line shows up (l).

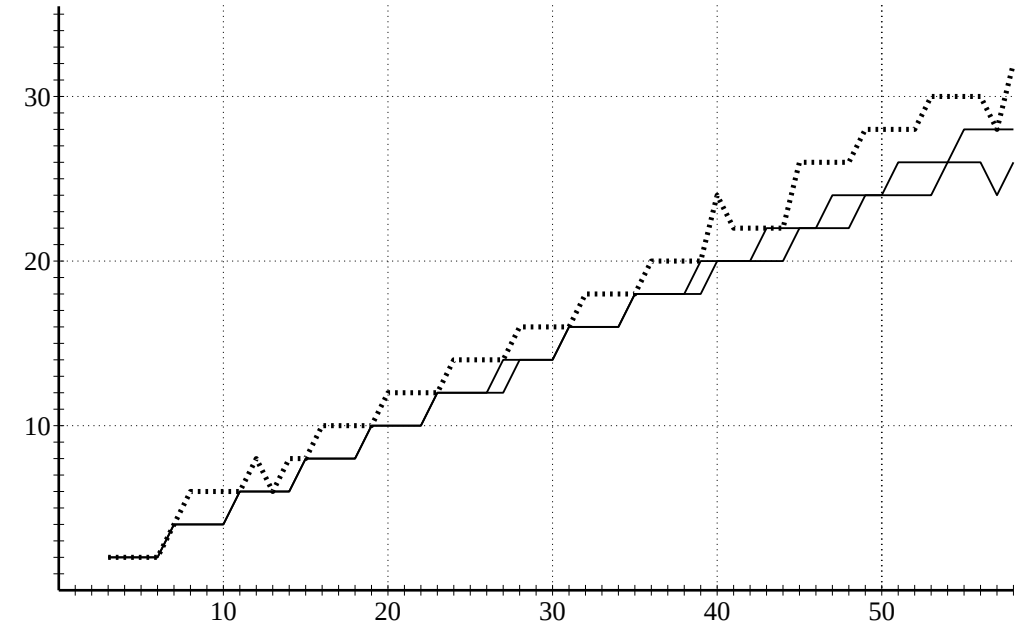

Figure 2: A fragment of the curves from Fig. 1, magnified.

$l = \|S\|$	d(S)	d′(S)	S
3	2	2	100
4	2	2	0100
5	2	2	01000
6	2	2	000100
7	4	4	1110100
8	4	6	11100010
9	4	6	110000010
10	4	6	0000010110
11	6	6	10001001011
12	6	8	111001100101
13	6	6	1000000101001
14	6	8	11100100010000
15	8	8	000100110101111
16	8	10	1101110000011010
17	8	10	11001101101010001
18	8	10	110010110010000101
19	10	10	1001111010100001100
20	10	12	01000011011011000101
21	10	12	011110000100101110110
22	10	12	010000101000100111011
23	12	12	000001010011001101011111
24	12	14	100011110110110000010101
25	12	14	101100011000000101110100
26	12	14	100101001111100010000100010
27	12	14	110100010111001100000000010
28	14	16	011100111111010010011010100
29	14	16	000001011001111110010100111101
30	14	16	111001100101101010111000111111
31	16	16	111101101001100000111001000 1010
32	16	18	000100010110010001110110101111 00
33	16	18	100100111000111011101000010000101
34	16	18	101000111101101001001100100000010
35	18	18	000001110001011011001010111101 10001
36	18	20	100010011110111100001011010001011000
37	18	20	001101101011101000110000100011011 1101
38	18	20	010100010000000110011110001101101 00001
39	18	20	010010110101110011100000011101000100010
40	20	24	000100001110100011010011001101011011 0111
41	20	22	000111010111110000010010100001001101 10001
42	20	22	111111010000001000100110001010010010111000
43	20	22	111011000101011110010011110100111001011 1011
44	20	22	111101101001111111001111101010100110010011 10
45	22	26	001000110001101000101110001011010011011111101
46	22	26	101101011011101001000100011111000111001001 0111
47	22	26	011110101010001011010110000011000100111100 11011
48	22	26	011011000110001010101110010010111101000000011000
49	24	28	010000110101110111111011000001110011011000010 1010
50	24	28	110000101101110010100110011011101011100001000001 10

Table 1: Examples of synchronizing sequences.

only sub-optimal synchronizing sequences.

For $l = 43, 44, 48$, by systematically searching through a significant fraction of $\{0, 1\}^l$, Mark Shand [8] found words achieving $\mathrm{up}(l)$; the best examples found by simulated annealing for these values of l are therefore non-optimal.

For all values of l not mentionned above, we do not know whether the synchronizing sequences found using simulated annealing are optimal; we do not know, either, whether $\mathrm{up}(l)$ is the exact upper bound for those values. Unlike for $l \leq 44$, the exhaustive search, which costs $O(2^l)$ in time, cannot be applied to answer these questions.

5.2.2 The reverse autodistance of optimal synchronizing sequences

Lemma 3 and Theorem 3 imply that the examples found for $l \in \{3 .. 15, 17 .. 21, 23, 24, 26, 28 .. 33, 35, 37, 42\}$ are double-optimal synchronizing sequences.

As indicated in Section 5.2.1 above, for $l = 27$ there are no words $S \in \{0, 1\}^l$ with $\mathrm{d}(S) = \mathrm{up}(l)$; a computation analogous to the these in the proof of Theorem 3 shows that there is also no word of this length with $\mathrm{d}(S) = \mathrm{d}'(S) = \mathrm{up}(l) - 2$. Therefore, the corresponding example is a double-optimal synchronizing sequence.

For $l = 16, 22, 25$, exhaustive searches showed that there is no word $S \in \{0, 1\}^l$ satisfying $\mathrm{d}(S) = \mathrm{d}'(S) = \mathrm{up}(l)$; the corresponding examples are therefore double-optimal synchronizing sequences.

For $l \in \{34, 36, 38, 40, 41, 45, 46, 49, 50, 54\}$, the examples found are optimal synchronizing sequences, but the author has not been able to establish whether they are double-optimal.

6 Double Synchronizing Sequences of Length $l \to +\infty$

6.1 The result

Theorem 6 (double synchronizing sequences for large l) *Let $\alpha \in \mathbf{R}$, $0 < \alpha < 1$. There exists a function $\varepsilon : \mathbf{N}_{2+} \to \mathbf{R}_+$ such that $\lim_{+\infty} \varepsilon = 0$ and that for every $l \in \mathbf{N}$, $l \geq 3$, there are at least $\alpha 2^l$ distinct words $S \in \{0, 1\}^l$ satisfying*

$$\mathrm{up}(l) - l\varepsilon(l) \leq \mathrm{d}(S) \leq \mathrm{d}'(S) \leq \mathrm{up}(l) + l\varepsilon(l)$$

6.2 How the proof is organized

The proof of Theorem 6 is long. Let us summarize it here.

Section 6.3 states two capital lemmas from which the theorem directly results.

Section 6.4 defines several notational conventions.

Section 6.5 contains auxiliary lemmas, which recall generally known mathematical facts.

Sections 6.6–6.9 contain the proof of the first capital lemma.

In Section 6.6, we choose a function ε which, as we will prove, satisfies both capital lemmas (and thus the theorem). We define then the set $E \subset \{0,1\}^l$ of words whose autodistance is less than $\mathrm{up}(l) - \varepsilon(l)l$, and we represent it as equal to the union of a family of sets called $E_{p,D}$.

Then, in Sections 6.7 and 6.8, we establish intermediate results which will enable us to estimate the cardinals of the sets $E_{p,D}$. Finally, in Section 6.9, we use these results to prove that $|E| \leq \frac{1-\alpha}{2} 2^l$, from what the first capital lemma results.

In Section 6.10, rather than fully describing the proof of the second capital lemma, we simply indicate in which ways it differs from the proof of the first capital lemma.

6.3 The two capital lemmas

Theorem 6 follows in a straightforward way from the two following lemmas.

Capital Lemma 1 (autodistance for high l) *Let $\alpha \in \mathbf{R}$, $0 < \alpha < 1$. There exists a function $\varepsilon : \mathbf{N}_{2+} \to \mathbf{R}_+$ such that $\lim_{+\infty} \varepsilon = 0$ and for every $l \in \mathbf{N}$, $l \geq 3$, there are at most $\frac{1-\alpha}{2} 2^l$ distinct words $S \in \{0,1\}^l$ such that*

$$\mathrm{d}(S) < \mathrm{up}(l) - l\varepsilon(l)$$

Capital Lemma 2 (reverse autodistance for high l) *Let $\alpha \in \mathbf{R}$, $0 < \alpha < 1$. There exists a function $\varepsilon : \mathbf{N}_{2+} \to \mathbf{R}_+$ such that $\lim_{+\infty} \varepsilon = 0$ and for every $l \in \mathbf{N}$, $l \geq 3$, there are at most $\frac{1-\alpha}{2} 2^l$ distinct words $S \in \{0,1\}^l$ such that*

$$\mathrm{up}(l) + l\varepsilon(l) < \mathrm{d}'(S)$$

6.4 Conventions

We make, for the whole proof, the following assumptions about the numbers l, p, a, b and μ and about the sets D and P:

$l \in \mathbf{N}_{2+}$,	$3 \leq l$
$p \in \mathbf{Z}$,	$1 \leq p \leq l/2$
$a \in \mathbf{N}$,	$1 \leq a$
$b \in \mathbf{N}$,	$2 \leq b$
$\mu \in \mathbf{R}$,	$0 < \mu < 1/2$
$D \subset [0\,..\,l)$	
$P \subset \mathbf{Z}$,	P is a finite set

These assumptions are valid in lemmas and auxiliary definitions which are part of the proof. They will not be recalled there. For instance, the following

Example Lemma 1 *For every* $\mu \in \mathbf{R}$ *such that* $0 < \mu < 1/2$ *and for every* $n \in \mathbf{Z}$, $\mu \neq n$.

will be abbreviated to

Example Lemma 2 *For every* $n \in \mathbf{Z}$, $\mu \neq n$.

6.5 Auxiliary lemmas

Lemma 4 (approximation of $\binom{n}{d}$) *For every* $n, d \in \mathbf{N}$,

$$d \leq (1/2 - \mu)\, n - 1 \quad \textit{implies} \quad \binom{n}{d} \leq 2^n e^{-\mu^3 n}$$

Proof outline: Let us define $q = \lfloor (1/2 - \mu/2)n \rfloor$. Using the well-known equality $\binom{n}{r} = \frac{n!}{r!(n-r)!}$, we can then state the following:

$$\begin{aligned}
\forall (r \in [d\,..\,q))\ \binom{n}{r} &\leq \frac{1-\mu}{1+\mu}\binom{n}{r+1} \\
\binom{n}{d} &\leq \left(\frac{1-\mu}{1+\mu}\right)^{\mu n/2}\binom{n}{q} \\
\binom{n}{d} &\leq \left(\frac{1-\mu}{1+\mu}\right)^{\mu n/2} 2^n \\
\binom{n}{d} &\leq e^{-\mu^3 n}\, 2^n
\end{aligned}$$

□

Auxiliary Definition 8 (families $\mathcal{F}_i$) *For* $i \in [0\,..\,l \sqcap p)$ *and* $x \in \left[0\,..\,\frac{l}{l \sqcap p}\right)$, *we define the numbers*

$$F_{ix} = (x\,p + i) \bmod l$$

which form the families

$$\mathcal{F}_i = (F_{ix})_{0 \leq x < \frac{l}{l \sqcap p}}$$

The numbers F_{ix} *and the families* $\mathcal{F}_i$ *depend on the numbers* l *and* p *but, for simplicity,* l *and* p *do not appear as indices in their notation.*

Lemma 5 (fundamental property of $\mathcal{F}_i$) *For every* $i \in [0\,..\,l \sqcap p)$, *the family* $\mathcal{F}_i$ *contains exactly once every element of the set* $A_i = ((l \sqcap p)\mathbf{Z} + i) \cap [0\,..\,l)$ *and contains only elements of this set.*

Proof outline: We call $\mathrm{Im}(\mathcal{F}_i)$ the image of the family $\mathcal{F}_i$, namely

$$\mathrm{Im}(\mathcal{F}_i) = \left\{ \; F_{ix} \;\middle|\; 0 \leq x < \tfrac{l}{l \sqcap p} \; \right\}$$

For every $x, y \in \left[0 \,..\, \frac{l}{l \sqcap p}\right)$, the equation $F_{ix} = F_{iy}$ is equivalent to

$$\exists (k \in \mathbf{Z}), \quad (x - y)\frac{p}{l \sqcap p} = k\frac{l}{l \sqcap p}$$

which, thanks to the Gauss theorem [6], implies $x - y \in \frac{l}{l \sqcap p}\mathbf{Z}$. Since $-\frac{l}{l \sqcap p} < x - y < \frac{l}{l \sqcap p}$, we get $x = y$. All the elements of the family $\mathcal{F}_i$ are therefore distinct and the family contains every element of A_i at most once.

Since all the elements of $\mathcal{F}_i$ are distinct, the set $\mathrm{Im}(\mathcal{F}_i)$ contains $\frac{l}{l \sqcap p}$ elements; A_i and $\mathrm{Im}(\mathcal{F}_i)$ have therefore the same number of elements. Since, as the reader may easily verify, $\mathrm{Im}(\mathcal{F}_i) \subset A_i$, we get $\mathrm{Im}(\mathcal{F}_i) = A_i$. The family $\mathcal{F}_i$ contains then each element of A_i at least once and contains no elements from outside A_i. □

Lemma 6 (parity of the cardinal) *If A and B are finite sets, $|A \triangle B|$ has the same parity as $|A| + |B|$. In other words,*

$$|A \triangle B| \equiv |A| + |B| \pmod 2$$

The proof is left to the reader.

6.6 The sets $E_{p,D}$

Let α be defined as in Capital Lemma 1. We define then

$$\begin{aligned}
\mu'(l) &= \left(\frac{1}{\ln l} + \frac{2}{l} \ln l \ln \frac{2l^2}{1-\alpha} \right)^{1/3} \\
\varepsilon'(l) &= \mu'(l) + \frac{2 \ln l}{l} + \frac{1}{l} \\
\varepsilon(l) &= \begin{cases} \varepsilon'(l) & \text{if } \varepsilon'(l) < 1/2 \text{ and } \mu'(l) < 1/2 \\ 1 & \text{otherwise} \end{cases}
\end{aligned}$$

The functions μ', ε' and ε are then strictly positive, and satisfy

$$\begin{aligned}
\lim_{+\infty} \mu' &= 0 \\
\lim_{+\infty} \varepsilon' &= 0 \\
\lim_{+\infty} \varepsilon &= 0
\end{aligned}$$

(the easy, computational proofs of these facts are not reproduced here)

To prove Capital Lemma 1, it is now sufficient to establish, for every l, the property that there are at most $\frac{1-\alpha}{2} 2^l$ distinct words $S \in \{0,1\}^l$ such that $\mathrm{d}(S) < \mathrm{up}(l) - l\varepsilon(l)$.

For l such that $\varepsilon'(l) \geq 1/2$ or $\mu'(l) \geq 1/2$, we have $\varepsilon(l) = 1$ and the property trivially holds. We suppose therefore, for the rest of the proof, that $\varepsilon'(l) < 1/2$ and that $\mu'(l) < 1/2$, and we establish the property in this case.

Define

$$\delta = \mathrm{up}(l) - l\varepsilon(l) \tag{19}$$

$$E = \left\{ S \in \{0,1\}^l \;\middle|\; \mathrm{d}(S) < \delta \right\} \tag{20}$$

The property to be proven can then be expressed by the relation

$$|E| \leq \frac{1-\alpha}{2} 2^l \tag{21}$$

By Definition 1, equation (20) can be rewritten as

$$E = \left\{ S \in \{0,1\}^l \;\middle|\; \exists (q \in [1\,..\,l))\ \mathrm{d}\left(S, \tau_q(S)\right) < \delta \right\} \tag{22}$$

From the definition of the Hamming distance, it is easy to show that for every $q \in \mathbf{Z}$ and every $S \in \{0,1\}^l$,

$$\mathrm{d}\left(S, \tau_q(S)\right) = \mathrm{d}\left(S, \tau_{l-q}(S)\right)$$

and (22) is equivalent to

$$E = \left\{ S \in \{0,1\}^l \;\middle|\; \exists \left(p \in [1\,..\,\lfloor l/2 \rfloor]\right)\ \mathrm{d}\left(S, \tau_p(S)\right) < \delta \right\} \tag{23}$$

We then define

$$E_p = \left\{ S \in \{0,1\}^l \;\middle|\; \mathrm{d}\left(S, \tau_p(S)\right) < \delta \right\} \tag{24}$$

Relation (23) can then be rewritten

$$E = \bigcup_{p=1}^{\lfloor l/2 \rfloor} E_p \tag{25}$$

Let us define, for $S \in \{0,1\}^l$, the *set of differences* $D_{S,p}$:

$$D_{S,p} = \left\{ i \in [0\,..\,l) \;\middle|\; S[i] \neq \tau_p(S)[i] \right\} \tag{26}$$

$$D_{S,p} = \left\{ i \in [0\,..\,l) \;\middle|\; S[i] \neq S[(i+p) \bmod l] \right\} \tag{27}$$

and, for any D, let

$$E_{p,D} = \left\{ S \in \{0,1\}^l \;\middle|\; D_{S,p} = D \right\} \tag{28}$$

Then (24) may be rewritten as

$$E_p = \bigcup_{|D|<\delta} E_{p,D} \tag{29}$$

From equations (25) and (29), we can deduce

$$|E| \leq \sum_{p=1}^{\lfloor l/2 \rfloor} \sum_{|D|<\delta} |E_{p,D}| \tag{30}$$

The rest of this proof consists in bounding the number of terms in this sum and in estimating $|E_{p,D}|$ as a function of l, p and D.

6.7 More auxiliary lemmas

Auxiliary Definition 9 (functions $\varphi[i]$ and expression $f(D,i,j)$) *For $i \in \mathbf{N}$, let us define the functions $\varphi, \varphi[i] : \{0,1\} \to \{0,1\}$*

$$\begin{aligned} \varphi(x) &= 1 - x \\ \varphi[0](x) &= x \\ \varphi[i+1](x) &= \varphi[i] \circ \varphi(x) \end{aligned}$$

For $i \in [0 \,..\, l \sqcap p)$ and $j \in \left[0 \,..\, \frac{l}{l \sqcap p}\right]$, we define

$$f(D,i,j) = \left|(F_{ix})_{0 \le x < j}\right|_D$$

The expression $f(D,i,j)$ depends on l and p, which, for simplicity, do not appear there as indices.

Lemma 7 (relation between $S[i]$, $S[j]$ and $D_{S,p}$) *Let $S \in E_{p,D}$. Then, for $0 \le i < l \sqcap p$ and $0 \le j \le \frac{l}{l \sqcap p}$, we have*

$$S[(i + pj) \bmod l] = \varphi[f(D,i,j)](S[i])$$

Proof: First, observe that for n even, $\varphi[n](x) = x$ and for n odd, $\varphi[n](x) = 1 - x$.

We will prove the lemma by induction on j; the verification that the lemma holds for $j = 0$ is left to the reader.

Let us assume the lemma true for j (with $0 \le j < \frac{l}{l \sqcap p}$) and prove it for $j + 1$. Under the lemma's hypotheses, the fact that $S \in E_{p,D}$ (which implies $D = D_{S,p}$) and relation (27) let us state:

$$\begin{aligned} \text{if } (i + pj) \bmod l \in D, &\qquad S[(i + p(j+1)) \bmod l] = 1 - S[(i + pj) \bmod l] \\ \text{otherwise,} &\qquad S[(i + p(j+1)) \bmod l] = S[(i + pj) \bmod l] \end{aligned}$$

which may be expressed as follows

$$\begin{aligned} S[(i + p(j+1)) \bmod l] &= \varphi\left[\left|D \cap \{(i + pj) \bmod l\}\right|\right](S[(i + pj) \bmod l]) \\ &= \varphi[f(D,i,j+1) - f(D,i,j)](S[(i + pj) \bmod l]) \\ &= \varphi[f(D,i,j+1) - f(D,i,j)](\varphi[f(D,i,j)](S[i])) \\ S[(i + p(j+1)) \bmod l] &= \varphi[f(D,i,j+1)](S[i]) \end{aligned}$$

□

Lemma 8 (some $E_{p,D}$ are empty) *If, for some $i \in [0 \,..\, l \sqcap p)$, the number $|((l \sqcap p)\mathbf{Z} + i) \cap D|$ is odd, then $E_{p,D} = \emptyset$.*

Proof: Let $i \in [0 \,..\, l \sqcap p)$ and let $|((l \sqcap p)\mathbf{Z} + i) \cap D)|$ be odd. By Lemma 5, we get

$$\begin{aligned} |\mathcal{F}_i|_D &= |(((l \sqcap p)\mathbf{Z} + i) \cap [0 \,..\, l)) \;\cap\; D| \\ &= |((l \sqcap p)\mathbf{Z} + i) \cap D| \end{aligned}$$

$|\mathcal{F}_i|_D$ is then odd. Applying Lemma 7, for every $S \in E_{p,D}$ we get then

$$\begin{aligned} S[i] &= S\left[\left(i + p\frac{l}{l \sqcap p}\right) \bmod l\right] \\ S[i] &= \varphi\left[f(D, i, \frac{l}{l \sqcap p})\right](S[i]) \\ S[i] &= \varphi[|\mathcal{F}_i|_D](S[i]) \\ S[i] &= 1 - S[i] \qquad \text{(since } |\mathcal{F}_i|_D \text{ is odd)} \end{aligned}$$

which is impossible. Therefore, $S \in E_{p,D}$ is true for no S and $E_{p,D} = \emptyset$. □

Lemma 9 ($E_{p,D}$ has at most $2^{l \sqcap p}$ members) *For every $S' \in \{0,1\}^{l \sqcap p}$, there exists at most one S such that $S \in E_{p,D}$ and the leftmost factor of S of length $l \sqcap p$ is equal to S'.*

Proof: Let $S \in E_{p,D}$ and $k \in [0 \,..\, l)$. Let i be the remainder in the division of k by $l \sqcap p$. Since $0 \le i < l \sqcap p$ and $k \in ((l \sqcap p)\mathbf{Z} + i) \cap [0 \,..\, l)$, Lemma 5 implies that for some $j \in \left[0 \,..\, \frac{l}{l \sqcap p}\right)$, we have $k = (i + pj) \bmod l$. We can then apply Lemma 7 to get:

$$S[k] = \varphi[f(D, i, j)](S[i])$$

This formula shows that every bit in S can be determined as a function of l, p, D and one of the $l \sqcap p$ leftmost bits of S. Therefore, for any given values of l, p and D, the left factor of S of length $l \sqcap p$ uniquely determines S. □

6.8 The sets $\mathcal{D}_{d,p}$

For any $d \in \mathbf{N}$, let us define

$$\mathcal{D}_{d,p} = \left\{ D \;\middle|\; |D| < d \wedge E_{p,D} \neq \emptyset \right\} \tag{31}$$

(the set $\mathcal{D}_{d,p}$ depends on l, but for simplicity l will not appear as an index in its notation)

We can rewrite equation (30) as follows:

$$|E| \le \sum_{p=1}^{\lfloor l/2 \rfloor} \sum_{D \in \mathcal{D}_{\delta,p}} |E_{p,D}| \tag{32}$$

By Lemma 9, for every $D \in \mathcal{D}_{\delta,p}$, $|E_{p,D}| \leq 2^{l \sqcap p}$ and equation (32) implies

$$|E| \leq \sum_{p=1}^{\lfloor l/2 \rfloor} |\mathcal{D}_{\delta,p}| \, 2^{l \sqcap p} \tag{33}$$

Let us find two different (and both useful) upper bounds on $|\mathcal{D}_{\delta,p}|$.

Since $\mathcal{D}_{\delta,p}$ is only composed of subsets of $[0 \,..\, l)$ containing less than δ elements, we get

$$|\mathcal{D}_{\delta,p}| \leq \sum_{0 \leq x < \delta} \binom{l}{x} \tag{34}$$

and we can easily verify that the hypotheses of Lemma 4 hold (for $\mu = \mu'(l)$); in this way we get the first upper bound on $\mathcal{D}_{\delta,p}$

$$|\mathcal{D}_{\delta,p}| \leq l e^{-\mu'(l)^3 l} \, 2^l \tag{35}$$

Let us compute the second upper bound on $\mathcal{D}_{\delta,p}$. To simplify notation, we define the two intervals I and J:

$$\begin{aligned} I &= [0 \,..\, a(b-1)) \\ J &= [a(b-1) \,..\, ab) \end{aligned}$$

Auxiliary Definition 10 (sets $\mathcal{D}'_{d,a,b,P}$) *For every $d \in \mathbf{N}$, let*

$$\mathcal{D}'_{d,a,b,P}$$

denote the set of sets $D' \subset [0 \,..\, ab)$ such that $|D'| < d$ and, for every $i \in [0 \,..\, a)$, $|D' \cap (a\mathbf{Z} + i)| + |P \cap (a\mathbf{Z} + i)|$ is even.

Lemma 10 *For every $d \in \mathbf{N}$,*

$$\left|\mathcal{D}'_{d,a,b,P}\right| \leq 2^{a(b-1)} \tag{36}$$

Proof: Since the set I has $a(b-1)$ elements, there are at most $2^{a(b-1)}$ possible sets of the form $D' \cap I$. To prove the lemma, it will therefore suffice to establish that for fixed d, a, b and P, and under the condition that $D' \in \mathcal{D}'_{d,a,b,P}$, the set $D' \cap I$ uniquely determines D'.

For every i, $D' \cap (a\mathbf{Z} + i)$ is the disjoint union of $D' \cap I \cap (a\mathbf{Z} + i)$ and $D' \cap J \cap (a\mathbf{Z} + i)$, therefore

$$|D' \cap (a\mathbf{Z} + i)| = |D' \cap I \cap (a\mathbf{Z} + i)| + |D' \cap J \cap (a\mathbf{Z} + i)|$$

The number

$$|D' \cap I \cap (a\mathbf{Z} + i)| + |D' \cap J \cap (a\mathbf{Z} + i)| + |P \cap (a\mathbf{Z} + i)|$$

is therefore even. The parity of $|D' \cap J \cap (a\mathbf{Z} + i)|$ is hence determined by $D' \cap I$.

On the other hand, we have

$$J \cap (a\mathbf{Z} + i) = \{i + a(b-1)\}$$

Therefore,

$$\begin{array}{rlll} \left|D' \cap J \cap (a\mathbf{Z}+i)\right| \text{ even} & \text{implies} & D' \cap J \cap (a\mathbf{Z}+i) = \varnothing \\ \left|D' \cap J \cap (a\mathbf{Z}+i)\right| \text{ odd} & \text{implies} & D' \cap J \cap (a\mathbf{Z}+i) = \{i + a(b-1)\} \end{array}$$

In this way, $D' \cap I$ uniquely determines $D' \cap J \cap (a\mathbf{Z} + i)$ for every i. The (easy to verify) equality

$$D' = (D' \cap I) \cup \bigcup_{i=0}^{a-1} \left(D' \cap J \cap (a\mathbf{Z}+i)\right)$$

implies then that $D' \cap I$ uniquely determines D'. □

Lemma 11 *For every d such that $0 \le d \le (1/2 - \mu)ab - b$,*

$$\left|\mathcal{D}'_{d,a,b,P}\right| \le a\, e^{-\mu^3 a}\, 2^{ab+b-a} \tag{37}$$

Proof: For every value of a, we will prove the lemma by induction on b.

First, we need to verify the lemma for $b = 2$. This verification, when fully described, is extremely long. For this reason, we will omit here numerous computational details.

For any fixed d, a and P satisfying lemma's hypotheses and for $b = 2$, we consider D' as a variable satisfying $D' \in \mathcal{D}'_{d,a,2,P}$ and we estimate the number of values that D' can take (this number is obviously equal to $\left|\mathcal{D}'_{d,a,2,P}\right|$).

We define the sets U and V:

$$\begin{aligned} U &= \left\{ i \in I \;\middle|\; |P \cap (a\mathbf{Z}+i)| \in 2\mathbf{Z} \right\} \\ V &= \left\{ i \in I \;\middle|\; |P \cap (a\mathbf{Z}+i)| \notin 2\mathbf{Z} \right\} \end{aligned}$$

It is easy to see that if $|V| > d$, then $\mathcal{D}'_{d,a,2,P} = \varnothing$ and the lemma holds. We suppose therefore that $|V| \le d$ and verify the lemma in this case only.

Let us quote the following, easy to establish, relations:

$$\begin{aligned} U \cup V &= [0\,..\,a) \\ U \cap V &= \varnothing \\ |U| + |V| &= a \\ U + a &\subset J \\ V + a &\subset J \end{aligned}$$

Let $i \in V$. The cardinal of $D' \cap (a\mathbf{Z} + i)$ is then odd and, since $D' \cap (a\mathbf{Z} + i) \subset \{i, a + i\}$, we get

$$\begin{aligned} a + i \in D' &\iff i \notin D' \\ i \in D' - a &\iff i \notin D' \end{aligned} \tag{38}$$

From here, we can deduce that

$$\begin{aligned} V \cap (D' - a) &= V - D' \\ (V + a) \cap D' &= (V - D') + a \end{aligned} \tag{39}$$

Therefore, $V \cap D'$ uniquely determines $(V + a) \cap D'$. By remarking that $V \cap D'$ can take at most $2^{|V|}$ different values, we conclude that $(V \cup (V + a)) \cap D'$ can only take $2^{|V|}$ different values.

From relation (39) we get

$$\left|(V + a) \cap D'\right| + \left|V \cap D'\right| = |V|$$

V and $V + a$ being disjoint, we conclude that $\left|(V \cup (V + a)) \cap D'\right| = |V|$. Since the sets $V \cup (V + a)$ and $U \cup (U + a)$ are disjoint, we finally get

$$\begin{aligned} \left|(U \cup (U + a)) \cap D'\right| + \left|(V \cup (V + a)) \cap D'\right| &< d \\ \left|(U \cup (U + a)) \cap D'\right| &< d - |V| \end{aligned} \tag{40}$$

A relation concerning U and analogous to (39) can be established:

$$(U + a) \cap D' = (U \cap D') + a \tag{41}$$

and can be used to conclude that $U \cap D'$ uniquely determines $(U + a) \cap D'$.

Relation (41), together with the fact that U and $U + a$ are disjoint, leads to the conclusion that

$$\begin{aligned} \left|U \cap D'\right| &= \left|(U + a) \cap D'\right| \\ &= \frac{1}{2}\left|(U \cup (U + a)) \cap D'\right| \\ \left|U \cap D'\right| &< \frac{d - |V|}{2} \qquad \text{(by (40))} \end{aligned}$$

Since $U \cap D'$ is a set containing less than $(d - |V|)/2$ elements chosen among the $a - |V|$ elements of U, it can take at most

$$\sum_{0 \le k < (d-|V|)/2} \binom{a - |V|}{k}$$

different values; the same is true concerning $(U \cup (U + a)) \cap D'$ (since this set is determined in a unique way by $U \cap D'$).

From the fact that

$$D' = \big((U \cup (U + a)) \cap D'\big) \cup \big((V \cup (V + a)) \cap D'\big)$$

we finally deduce that D' can take no more than

$$\sum_{0 \le k < (d-|V|)/2} \binom{a - |V|}{k} 2^{|V|}$$

different values; then

$$\left|\mathcal{D}'_{d,a,2,P}\right| \quad \le \quad a \binom{a - |V|}{\lfloor (d - |V|)/2 \rfloor} 2^{|V|} \tag{42}$$

We can verify the following relations (remember that $|V| \le d$)

$$\begin{array}{rcccl} 0 & \le & \dfrac{d - |V|}{2} & \le & \left(\dfrac{1}{2} - \mu \dfrac{a}{a - |V|}\right)(a - |V|) - 1 \\ 0 & < & \mu \dfrac{a}{a - |V|} & < & \dfrac{1}{2} \end{array}$$

which, together with (42), enable us to use Lemma 4 and obtain

$$\left|\mathcal{D}'_{d,a,2,P}\right| \quad \le \quad a\, e^{-\mu^3 \frac{a^3}{(a-|V|)^3}(a-|V|)}\, 2^{a-|V|}\, 2^{|V|}$$

from that we deduce that (37) holds and we thus end the verification for $b = 2$.

Now, we suppose that $b \ge 3$ and that the lemma holds for $b' = b - 1$. Supposing that a, d, μ and P satisfy the lemma's hypotheses, let us establish relation (37). Let $D' \in \mathcal{D}'_{d,a,b,P}$. We can split D' into the union of two disjoint subsets D_1 and Q:

$$\begin{array}{rcl} D_1 & = & D' \cap I \\ Q & = & D' \cap J \end{array}$$

By definition of $\mathcal{D}'_{d,a,b,P}$, for every $i \in [0\,..\,a)$ we have

$$\big|D' \cap (a\mathbf{Z} + i)\big| + \big|P \cap (a\mathbf{Z} + i)\big| \in 2\mathbf{N}$$

this can be rewritten as

$$\big|D_1 \cap (a\mathbf{Z} + i)\big| + \big|Q \cap (a\mathbf{Z} + i)\big| + \big|P \cap (a\mathbf{Z} + i)\big| \in 2\mathbf{N}$$

and, by Lemma 6,

$$\big|D_1 \cap (a\mathbf{Z} + i)\big| + \big|(P \triangle Q) \cap (a\mathbf{Z} + i)\big| \in 2\mathbf{N} \tag{43}$$

The facts that $D_1 \subset I$ and that $|D_1| + |Q| = |D'|$, together with relation (43), enable us to state

$$D_1 \in \mathcal{D}'_{d-|Q|,a,b-1,P \triangle Q}$$

We have therefore established that every $D' \in \mathcal{D}'_{d,a,b,P}$ is the union of some $Q \subset J$ and some $D_1 \in \mathcal{D}'_{d-|Q|,a,b-1,P\triangle Q}$. Then,

$$\begin{aligned} \mathcal{D}'_{d,a,b,P} &\subset \bigcup_{Q\subset J} \left\{ D_1 \cup Q \;\middle|\; D_1 \in \mathcal{D}'_{d-|Q|,a,b-1,P\triangle Q} \right\} \\ \left|\mathcal{D}'_{d,a,b,P}\right| &\leq \sum_{Q\subset J} \left|\mathcal{D}'_{d-|Q|,a,b-1,P\triangle Q}\right| \end{aligned} \tag{44}$$

Let us split the sum (44) into two terms X and Y:

$$\begin{aligned} \left|\mathcal{D}'_{d,a,b,P}\right| &\leq X + Y \\ X &= \sum_{\substack{Q\subset J \\ |Q|<(1/2-\mu)a-1}} \left|\mathcal{D}'_{d-|Q|,a,b-1,P\triangle Q}\right| \\ Y &= \sum_{\substack{Q\subset J \\ |Q|\geq(1/2-\mu)a-1}} \left|\mathcal{D}'_{d-|Q|,a,b-1,P\triangle Q}\right| \end{aligned}$$

The sum X is indexed by subsets of J having less than $(1/2-\mu)a-1$ elements. Lemma 4 implies then that the number of terms in the sum is less than or equal to

$$\begin{aligned} \sum_{0\leq i<(1/2-\mu)a-1} \binom{a}{i} \\ \leq\; a\, e^{-\mu^3 a}\, 2^a \end{aligned}$$

From Lemma 10, we deduce that each term in X is less than or equal to 2^{ab-2a}; therefore,

$$X \leq a\, e^{-\mu^3 a}\, 2^{ab-a} \tag{45}$$

The sum Y, being indexed by subsets of J, contains at most 2^a terms. Each term is of the form

$$\left|\mathcal{D}'_{d-|Q|,a,b-1,P\triangle Q}\right|$$

where

$$d - |Q| \leq (1/2-\mu)a(b-1) - (b-1)$$

After straightforward verifications, the induction hypothesis (Lemma 11 applied for $b-1$) may be applied to give

$$\left|\mathcal{D}'_{d-|Q|,a,b-1,P\triangle Q}\right| \leq a\, e^{-\mu^3 a}\, 2^{a(b-1)+(b-1)-a}$$

Therefore,

$$Y \leq a\, e^{-\mu^3 a}\, 2^{ab+(b-1)-a} \tag{46}$$

and

$$\begin{aligned} \left|\mathcal{D}'_{d,a,b,P}\right| &\leq a\, e^{-\mu^3 a}\, 2^{ab-a} + a\, e^{-\mu^3 a}\, 2^{ab+(b-1)-a} \\ \left|\mathcal{D}'_{d,a,b,P}\right| &\leq a\, e^{-\mu^3 a}\, 2^{ab+b-a} \end{aligned}$$

□

The definition of $\mathcal{D}_{\delta,p}$, together with Lemma 8, imply that $\mathcal{D}_{\delta,p} \subset \mathcal{D}'_{\delta,l\sqcap p,\frac{l}{l\sqcap p},\varnothing}$; if we set $\mu = \mu'(l)$, Lemma 11 implies

$$|\mathcal{D}_{\delta,p}| \leq l\, e^{-\mu'(l)^3(l\sqcap p)}\, 2^{l+\frac{l}{l\sqcap p}-l\sqcap p} \tag{47}$$

which is our second upper bound on $\mathcal{D}_{\delta,p}$.

6.9 Conclusion

Let us use the two bounds (35) and (47) to estimate the sum described in (33). For $l \sqcap p \leq \frac{l}{\ln l}$, we have (by (35))

$$\begin{aligned} |\mathcal{D}_{\delta,p}|\, 2^{l\sqcap p} &\leq l\, e^{-\mu'(l)^3 l}\, 2^{l+l\sqcap p} \\ |\mathcal{D}_{\delta,p}|\, 2^{l\sqcap p} &\leq l\, e^{-\mu'(l)^3 l}\, 2^{l+\frac{l}{\ln l}} \end{aligned} \tag{48}$$

For $l \sqcap p > \frac{l}{\ln l}$, we use (47), which implies,

$$\begin{aligned} |\mathcal{D}_{\delta,p}|\, 2^{l\sqcap p} &\leq l\, e^{-\mu'(l)^3(l\sqcap p)}\, 2^{l+\frac{l}{l\sqcap p}} \\ |\mathcal{D}_{\delta,p}|\, 2^{l\sqcap p} &\leq l^2\, e^{-\mu'(l)^3\frac{l}{\ln l}}\, 2^{l} \end{aligned} \tag{49}$$

For every term in the sum (33), either (48) or (49) holds. Therefore,

$$\begin{aligned} |E| &\leq \sum_{p=1}^{\lfloor l/2\rfloor} \max\left(l\, e^{-\mu'(l)^3 l}\, 2^{l+\frac{l}{\ln l}} \;,\; l^2\, e^{-\mu'(l)^3\frac{l}{\ln l}}\, 2^{l}\right) \\ |E| &\leq \max\left(l^2\, e^{-\mu'(l)^3 l}\, 2^{l+\frac{l}{\ln l}} \;,\; l^3\, e^{-\mu'(l)^3\frac{l}{\ln l}}\, 2^{l}\right) \end{aligned} \tag{50}$$

From (50), using the definition of μ', we get (after a tedious computation) relation (21). □

6.10 The proof of Capital Lemma 2

Let us describe the modifications that the proof of Capital Lemma 1 (Sections 6.6–6.9) should undergo in order to become a proof of Capital Lemma 2. Note that the function ε used in both proofs is the same.

By analogy with the objects δ and E (see (19) and (20)), we define

$$\begin{aligned} \overline{\delta} &= \mathrm{up}(l) + l\varepsilon(l) \\ \overline{E} &= \left\{\; S \in \{0,1\}^l \;\middle|\; \mathrm{d}'(S) > \delta \;\right\} \end{aligned} \tag{51}$$

The property to be proven (corresponding with (21)) can then be expressed by the relation (analogous to (21))

$$\left|\overline{E}\right| \leq \frac{1-\alpha}{2} 2^l \tag{52}$$

By analogy with (34), we get

$$\left|\overline{E}\right| \leq \sum_{p=1}^{\lfloor l/2 \rfloor} \sum_{|D|>\delta} |E_{p,D}| \tag{53}$$

By analogy with $\mathcal{D}_{d,p}$ (see (31)), we define for any $d \in \mathbf{N}$,

$$\overline{\mathcal{D}_{d,p}} \;=\; \left\{ \; D \;\middle|\; |D| > l - d \wedge E_{p,D} \neq \emptyset \; \right\} \tag{54}$$

Then, in the same way as relation (34) is obtained, we get

$$\begin{aligned} \left|\overline{\mathcal{D}_{\delta,p}}\right| &\leq \sum_{l-\delta<x\leq l} \binom{l}{x} \\ &\leq \sum_{0\leq x<\delta} \binom{l}{x} \end{aligned}$$

which, in turn, leads us to the first upper bound on $\overline{\mathcal{D}_{\delta,p}}$ (analogous to (35)):

$$\left|\overline{\mathcal{D}_{\delta,p}}\right| \;\leq\; l e^{-\mu'(l)^3 l}\, 2^l \tag{55}$$

In order to obtain the second upper bound on $\overline{\mathcal{D}_{\delta,p}}$ (analogous to (47)), we use Lemma 8 and get, for all $i \in [0\,..\,l \sqcap p)$,

$$D \in \overline{\mathcal{D}_{\delta,p}} \;\Longrightarrow\; |((l \sqcap p)\mathbf{Z} + i) \cap ([0\,..\,l) - D)| + |((l \sqcap p)\mathbf{Z} + i) \cap [0\,..\,l)| \in 2\mathbf{Z} \tag{56}$$

The definition of $\overline{\mathcal{D}_{\delta,p}}$ (formula (54)) implies that

$$D \in \overline{\mathcal{D}_{\delta,p}} \Longrightarrow |[0\,..\,l) - D| \leq \delta \tag{57}$$

From (56) and (57), and from Auxiliary Definition 10, we get

$$\overline{\mathcal{D}_{\delta,p}} \subset \left\{ \; D \subset [0\,..\,l) \;\middle|\; [0\,..\,l) - D \;\in\; \mathcal{D}'_{\delta,\, l\sqcap p,\, \frac{l}{l\sqcap p},\, [0\,..\,l)} \; \right\}$$

Finally, by observing that the function transforming D (for $D \subset [0\,..\,l)$) into $[0\,..\,l) - D$ is bijective, we obtain

$$\left|\overline{\mathcal{D}_{\delta,p}}\right| \leq \left|\mathcal{D}'_{\delta,\, l\sqcap p,\, \frac{l}{l\sqcap p},\, [0\,..\,l)}\right|$$

and using Lemma 11, we get the second upper bound on $\overline{\mathcal{D}_{\delta,p}}$ (analogous to (47)):

$$\left|\overline{\mathcal{D}_{\delta,p}}\right| \leq l\, e^{-\mu'(l)^3 (l\sqcap p)}\, 2^{l+\frac{l}{l\sqcap p}-l\sqcap p} \tag{58}$$

The two bounds (55) and (58) enable us to derive (52) in the same way as (21) is obtained in Section 6.9. □

References

1. Patrice Bernard. Corpac 900, une autre approche. Technical Report 06 10 00 MGT 003, TECSI, 29, rue des Pyramides, 75001 Paris (May 1981).

2. Richard E. Blahut. *Digital Transmission of Information.* Addison-Wesley (1990).

3. S. Kirkpatrick, C. D. Gelatt, Jr., and M. P. Vecchi. Optimization by simulated annealing. *Science*, 220:671–680 (1983).

4. Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge University Press, Cambridge, UK (1986).

5. Raymond L. Pickholtz, Donald L. Schilling, and Laurence B. Milstein. Theory of spread-spectrum communications — a tutorial. *IEEE Transactions on Communications*, COM-30(5):855–884 (May 1982).

6. E. Ramis, C. Deschamps, and J. Odoux. *Cours de Mathématiques Spéciales*, volume 1, section 3.3.2, paragraph 3e. Masson, Paris (1979).

7. Dilip V. Sarwate and Michael B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *Proceedings of the IEEE*, 68(5):593–619 (May 1980).

8. Mark Shand. Private communication (February 1991). shand@prl.dec.com; Digital Equipment Corporation Paris Research Laboratory.

PRL Research Reports

The following documents may be ordered by regular mail from:

Librarian – Research Reports
Digital Equipment Corporation
Paris Research Laboratory
85, avenue Victor Hugo
92563 Rueil-Malmaison Cedex
France.

It is also possible to obtain them by electronic mail. For more information, send a message whose subject line is `help` to `doc-server@prl.dec.com` or, from within Digital, to `decprl::doc-server`.

Research Report 1: *Incremental Computation of Planar Maps*. Michel Gangnet, Jean-Claude Hervé, Thierry Pudet, and Jean-Manuel Van Thong. May 1989.

Research Report 2: *BigNum: A Portable and Efficient Package for Arbitrary-Precision Arithmetic*. Bernard Serpette, Jean Vuillemin, and Jean-Claude Hervé. May 1989.

Research Report 3: *Introduction to Programmable Active Memories*. Patrice Bertin, Didier Roncin, and Jean Vuillemin. June 1989.

Research Report 4: *Compiling Pattern Matching by Term Decomposition*. Laurence Puel and Ascánder Suárez. January 1990.

Research Report 5: *The WAM: A (Real) Tutorial*. Hassan Aït-Kaci. January 1990.

Research Report 6: *Binary Periodic Synchronizing Sequences*. Marcin Skubiszewski. May 1991.

Research Report 7: *The Siphon: Managing Distant Replicated Repositories*. Francis J. Prusker and Edward P. Wobber. May 1991.

Research Report 8: *Constructive Logics. Part I: A Tutorial on Proof Systems and Typed λ-Calculi*. Jean Gallier. May 1991.

Research Report 9: *Constructive Logics. Part II: Linear Logic and Proof Nets*. Jean Gallier. May 1991.

Research Report 10: *Pattern Matching in Order-Sorted Languages*. Delia Kesner. May 1991.

Research Report 11: *Towards a Meaning of LIFE*. Hassan Aït-Kaci and Andreas Podelski. May 1991.

Research Report 12: *Residuation and Guarded Rules for Constraint Logic Programming*. Gert Smolka. May 1991.

Research Report 13: *Functions as Passive Constraints in LIFE*. Hassan Aït-Kaci and Andreas Podelski. May 1991.

Research Report 14: *Automatic Motion Planning for Complex Articulated Bodies.*. Jérôme Barraquand. May 1991.