Some combinatorial results on Bernoulli sets and codes

Aldo de Luca\textsuperscript{a,b,*}

\textsuperscript{a}Dipartimento di Matematica dell'Università di Roma "La Sapienza", Piazzale A. Moro 2, 00185 Roma, Italy
\textsuperscript{b}Centro Interdisciplinare 'B. Segre', Accademia dei Lincei, via della Lungara 10, 00100 Roma, Italy

Abstract

A Bernoulli set is a set \( X \) of words over a finite alphabet \( \mathcal{A} \) such that for any positive Bernoulli distribution \( \pi \) in \( \mathcal{A}^* \) one has that \( \pi(X) = 1 \). In the case of a two-letter alphabet \( \mathcal{A} = \{a, b\} \) a characterization of finite Bernoulli sets is given in terms of the function \( x_{i,j} \) counting the number of words of \( X \) having \( i \) occurrences of the letter \( a \) and \( j \) occurrences of the letter \( b \). Moreover, we also derive a necessary and sufficient condition on the distribution \( x_{i,j} \) which characterizes Bernoulli sets which are commutatively equivalent to prefix codes.

\( \copyright \) 2002 Elsevier Science B.V. All rights reserved.

Keywords: Bernoulli sets; Bernoulli distributions; Codes; Commutative equivalence

1. Introduction

Let \( \mathcal{A} \) be a finite alphabet. A Bernoulli distribution \( \pi \) on \( \mathcal{A} \) is any map

\[ \pi : \mathcal{A} \rightarrow \mathbb{R}_+, \]

where \( \mathbb{R}_+ \) is the set of non-negative real numbers, such that

\[ \sum_{a \in \mathcal{A}} \pi(a) = 1. \]

A Bernoulli distribution is positive if for all \( a \in \mathcal{A} \) one has \( \pi(a) > 0 \). We denote by \( \text{PBD}(\mathcal{A}) \), or simply \( \text{PBD} \), the set of all positive Bernoulli distributions on \( \mathcal{A} \).

\* The work for this paper has been supported by the Italian Ministry of Education under Project COFIN '98 'Modelli di calcolo innovativi: metodi sintattici e combinatori'.

* Correspondence address: Dipartimento di Matematica dell'Università di Roma "La Sapienza", Piazzale A. Moro 2, 00185 Roma, Italy.

E-mail address: deluca@mat.uniroma1.it (A. de Luca).
Let \( \mathcal{A}^* \) (resp. \( \mathcal{A}^+ \)) be the free monoid (resp. free semigroup) over \( \mathcal{A} \). We denote by \( \varepsilon \) the identity element of \( \mathcal{A}^* \). The elements of \( \mathcal{A}^* \) are usually called words and \( \varepsilon \) empty word. For any word \( w \in \mathcal{A}^* \), \( |w| \) denotes the length of \( w \). The length of \( \varepsilon \) is taken equal to 0. For any word \( w \in \mathcal{A}^* \) and \( a \in \mathcal{A} \), \( |w|_a \) denotes the number of occurrences of the letter \( a \) in \( w \).

If \( \pi \) is a Bernoulli distribution over \( \mathcal{A} \), then one can extend \( \pi \) to a morphism of \( \mathcal{A}^* \) in the multiplicative monoid \( \mathbb{R}_+ \). Hence, \( \pi(\varepsilon) = 1 \) and for all \( u, v \in \mathcal{A}^* \) one has

\[
\pi(uv) = \pi(u)\pi(v).
\]

One can extend also \( \pi \) to the subsets \( X \) of \( \mathcal{A}^* \) by setting

\[
\pi(X) = \sum_{x \in X} \pi(x).
\]

Let us observe that for some sets \( X \) the value \( \pi(X) \) may be infinite. We recall that a set \( X \) is dense if for all \( w \in \mathcal{A}^* \)

\[
\mathcal{A}^* \setminus \mathcal{A}^* \cap X \neq \emptyset.
\]

A set \( X \) is complete if \( X^* \) is dense. A set \( X \) is a code if it is the base of a free submonoid of \( \mathcal{A}^* \). A code is maximal if it is not properly included in any other code on the same alphabet. As is well known a maximal code is complete. Conversely, a non-dense complete code is maximal (cf. [2]).

In this paper we shall study some structural properties of the sets \( X \subseteq \mathcal{A}^+ \) which satisfy the property: for all \( \pi \in \text{PBD} \):

\[
\pi(X) = 1. \quad (1)
\]

Such sets will be called Bernoulli sets over the alphabet \( \mathcal{A} \). We recall (cf. [2]) that any non-dense and maximal code is a Bernoulli set. However, there exist Bernoulli sets which are not codes.

**Example 1.** Let \( \mathcal{A} = \{a, b\} \) and consider the set

\[
X = \{a, bb, baa, bba\}.
\]

\( X \) is not a code since \( bba = (bb)(a) \) with \( a, bb, bba \in X \). However, since the set \( \{a, bb, baa, bab\} \) is a maximal code one has that \( \pi(X) = 1 \) for all \( \pi \in \text{PBD} \).

Let \( X = \{a, ab, ba\} \). This set is not a code since \( aba = (a)(ba) = (ab)(a) \). For any \( 0 < p < 1 \) let \( \pi_p \in \text{PBD} \) be defined as: \( \pi_p(a) = p \) and \( \pi_p(b) = 1 - p \). One has \( \pi_p(X) = 3p - 2p^2 \), so that \( \pi_p(X) = 1 \) if and only if \( p = 1/2 \).

**Proposition 1.1.** Let \( X \) be a finite Bernoulli set. For any letter \( a \in \mathcal{A} \) there exists, and is unique, an exponent \( k(a) \) such that \( a^{k(a)} \in X \).
Proof. Let \( X \) be a finite set. For any \( \pi \in \text{PBD} \) we set
\[
A(X, \pi) = \pi(X).
\]
Hence, the map \( A \) depends on the set \( X \) and on the real numbers \( \pi(a), a \in \mathcal{A} \) ranging in the open interval \((0, 1)\) under the constraint \( \sum_{a \in \mathcal{A}} \pi(a) = 1 \). We can also write for \( x \in X \):
\[
\pi(x) = \prod_{a \in \mathcal{A}} (\pi(a))^{|x|_a}.
\]
Let us suppose that \( X \) is such that \( A(X, \pi) = 1 \) for all \( \pi \in \text{PBD} \). It follows that for any \( a \in \mathcal{A} \)
\[
\lim_{\pi(a) \to 1} A(X, \pi) = \sum_{x \in X} \lim_{\pi(a) \to 1} \pi(x) = 1.
\]
Now \( \lim_{\pi(a) \to 1} \pi(x) \) vanishes unless \( x = a^{|x|} \); in this case:
\[
\lim_{\pi(a) \to 1} (\pi(a))^{|x|} = 1.
\]
Hence, there must be in \( X \) exactly one power of the letter \( a \). \( \square \)

Let us remark that the hypothesis that \( X \) is finite is necessary. Indeed, if \( \mathcal{A} = \{a, b\} \) and \( X = a^*b \) one has \( \pi(X) = 1 \) for all \( \pi \in \text{PBD} \) and there is no power of \( a \) in \( X \).

Let \( X \subseteq \mathcal{A}^+ \) be a finite Bernoulli set. From the preceding proposition we denote by \( k_X \), or simply \( k \), the map \( k : \mathcal{A} \to \mathbb{N} \) giving for each \( a \in \mathcal{A} \) the unique exponent \( k(a) \) such that \( a^{k(a)} \in X \). We call \( k \) the index function of \( X \) and for each \( a \in \mathcal{A} \), \( k(a) \) is called the index of \( a \) in \( X \).

Let \( X \) be a finite set. We set
\[
N_X = \text{card}(X) \quad \text{and} \quad L_X = \max \{|x| \mid x \in X\}.
\]
We shall simply write \( N \) and \( L \) where there is no confusion.

**Proposition 1.2.** Let \( X \) be a finite set and let \( M = NL + 1 \). The set \( X \) is a maximal code if and only if there exists a \( \pi \in \text{PBD} \) such that
\[
\pi(X) = \pi(X^M) = 1.
\]

**Proof.** The ‘only if’ part is trivial. Indeed, let \( X \) be a finite maximal code. As is well known [2] for any \( \pi \in \text{PBD} \), \( \pi(X) = 1 \). Moreover, since \( X \) is a code one has \( \pi(X^M) = (\pi(X))^M = 1 \).

Let us then prove the ‘if’ part. Let \( \pi \in \text{PBD} \) be such that \( \pi(X) = \pi(X^M) = 1 \). We first prove that for all \( n \) such that \( M > n > 0 \) the product \( XX^n \) is not ambiguous. This is also, trivially, equivalent to the statement that \( \pi(X^{n+1}) = 1 \) for all \( n = 1, \ldots, M - 1 \). Suppose now by contradiction that there exists an integer \( n \) such that \( 1 < n < M \) and
\( \pi(X^n) \neq 1 \). Since \( \pi(X^n) \leq (\pi(X))^n \) one has \( \pi(X^n) < 1 \). Hence,
\[
\pi(X^{n+1}) \leq \pi(X) \pi(X^n) = \pi(X^n) < 1.
\]
This implies \( \pi(X^{i+1}) < 1 \) for all \( i = n, \ldots, M - 1 \). Hence, \( \pi(X^M) < 1 \) which is a contradiction. Let us now suppose that there exists an integer \( n \geq M \) for which the product \( XX^n \) is ambiguous. This implies that there exist words \( x, x_1, \ldots, x_n \) and \( y, y_1, \ldots, y_n \) of the set \( X \) such that \( x \neq y \) and
\[
xx_1 \cdots x_n = yy_1 \cdots y_n.
\]
By the lemma of Levi there exists \( \zeta \in A^+ \) such that if \( |x| > |y| \) (the case \( |x| < |y| \) is symmetrically dealt with)
\[
x = y^\zeta, \quad \zeta x_1 \cdots x_n = y_1 \cdots y_n.
\]
Let \( R_1, \ldots, R_n, \ldots \) be the sequence of the sets of right residuals of \( X \) of the theorem of Sardinas and Patterson (cf. [2, Chapter 1, Theorem 3.1]). We recall that \( R_1 = X^{-1}X \setminus \{ \epsilon \} \) and for all \( n > 1 \)
\[
R_{n+1} = X^{-1}R_n \cup R_n^{-1}X.
\]
For each \( n > 0 \), \( R_n \) is called the set of the right residuals of \( X \) of order \( n \). From Eq. (2) one has \( \zeta \in R_1 = X^{-1}X \setminus \{ \epsilon \} \), and
\[
\zeta X^n \cap X^n \neq \emptyset.
\]
From a lemma on right residual sets (cf. [2, Chapter 1, Lemma 3.2]) one has that
\[
\epsilon \in R_{2n+1}.
\]
From a theorem of Levenstein it follows that an integer \( k < M \) exists such that \( \epsilon \in R_k \).
By using again the lemma on residual sets one has that: \( \epsilon \in R_k \) implies that there exist \( u \in R_1 \) and integers \( i, j \geq 0 \) such that \( i + j + 1 = k \) and
\[
uX^i \cap X^j \neq \emptyset.
\]
Hence, there exist words \( x, x_1, \ldots, x_i \), \( y, y_1, \ldots, y_j \) of the set \( X \) such that
\[
x = yu, \quad ux_1 \cdots x_i = y_1 \cdots y_j.
\]
Hence, one has:
\[
xx_1 \cdots x_i = yy_1 \cdots y_j
\]
and
\[
xx_1 \cdots x_i y y_1 \cdots y_j = yy_1 \cdots y_j xxx_1 \cdots x_i.
\]
Hence, the product \( XX^{i+j+1} \) is ambiguous with \( i+j+1 = k < M \) which is a contradiction.\( \square \)
Let us remark that in the statement of the preceding proposition one can replace the condition $\pi(X) = \pi(X^M) = 1$ with $\pi(X) \leq 1$ and $\pi(X^M) \geq 1$. Indeed, since $\pi \in \text{PBD}$ one has $1 \leq \pi(X^M) \leq (\pi(X))^M \leq 1$. This implies that $\pi(X) = 1$ and $\pi(X^M) = 1$.

Let us recall the following important result on complete sets due to Schützenberger.

**Theorem 1.1.** Let $X$ be a non-dense and complete set. Then for any $\pi \in \text{PBD}$

$$\pi(X) \geq 1.$$ 

When $X$ is a complete set one obtains by Proposition 1.2 the following [3, 2]:

**Corollary 1.1.** Let $X$ be a finite complete set such that there exists a $\pi \in \text{PBD}$ for which $\pi(X) = 1$. Then $X$ is a maximal code.

**Proof.** It is sufficient to observe that $X^M$ is also a complete set, so that by Theorem 1.1

$$1 \leq \pi(X^M) \leq (\pi(X))^M = 1.$$ 

Hence, $\pi(X^M) = 1$ and by the preceding proposition the result follows. □

We shall refer in the following, for the sake of simplicity, to a binary alphabet $\mathcal{A} = \{a, b\}$, even though in our opinion some results can be suitably extended to the case of larger alphabets.

If $X$ is a subset of $\mathcal{A}^+$, then we denote by $X$ the *characteristic series* of the set $X$ and by $\overline{X}$ the corresponding series in commutative variables (cf. [2]). One has

$$X = \sum_{i,j \in \mathbb{N}} x_{i,j} a^i b^j,$$

where $x_{i,j}$ denotes the number of words in $X$ having $i$ occurrences of the letter $a$ and $j$ occurrences of the letter $b$. One has $x_{0,0} = 0$. If $X$ is finite, then we set $L_X = \deg(X)$, where $\deg(X)$ denotes the *degree* of the polynomial $X$.

Let $f_X$ denote the *structure function* of $X$, i.e., for each $n > 0$

$$f_X(n) = \text{card}(X \cap \mathcal{A}^n).$$

One has for all $n > 0$

$$f_X(n) = \sum_{i=0}^{n} x_{i,n-i} = \sum_{i=0}^{n} x_{n-i,i}.$$ 

If $\pi \in \text{PBD}$, then $\pi(b) = 1 - \pi(a)$ so that we can evaluate $\pi(X) = A(X, \pi)$ by the series (or polynomial if $X$ is finite): 

$$\sum_{i,j \in \mathbb{N}} x_{i,j} a^i (1 - a)^j,$$

where the variable $\pi(a)$, simply denoted by $a$, ranges in the open interval $(0, 1)$. We shall then denote $A(X, \pi)$ simply by $A(X, a) = \sum_{i,j \geq 0} x_{i,j} a^i (1 - a)^j$. The condition that
for any \( \pi \in \mathrm{PBD} \), \( \pi(X) = 1 \) becomes: for all \( a \in (0, 1) \)

\[
A(X,a) = 1.
\]

From this it follows that for all \( k > 0 \)

\[
\frac{d^k A(X,a)}{da^k} = 0
\]

for all \( a \in (0, 1) \).

### 2. Derivatives

Let \( X \) be a finite Bernoulli set over the alphabet \( \{a,b\} \). We can rewrite \( A(X,a) \), according to Proposition 1.1, as

\[
A(X,a) = a^{k_a} + (1-a)^{k_b} + \sum_{i,j>0} x_{i,j} a^i (1-a)^j,
\]

having set \( k_a = k(a) \) and \( k_b = k(b) \), where \( k \) is the index function of \( X \). One has

\[
\frac{dA}{da} = k_a a^{k_a-1} - k_b (1-a)^{k_b-1} + \sum_{i,j>0} x_{i,j} (ia^{i-1}(1-a)^j - ja^i(1-a)^{j-1}) = 0. \tag{3}
\]

Let us first suppose \( k_b > 1 \). One has

\[
\lim_{a \to 1} \frac{dA}{da} = k_a - \sum_{i>0} x_{i,1} = 0.
\]

If \( k_b = 1 \) one has

\[
\lim_{a \to 1} \frac{dA}{da} = k_a - k_b - \sum_{i>0} x_{i,1} = 0.
\]

In the first case, \( x_{0,1} = 0 \) and in the second \( x_{0,1} = 1 \), so that in any case one gets the following formula:

\[
k_a = \sum_{i>0} x_{i,1}. \tag{4}
\]

In a similar way, if one compute the \( \lim_{a \to 0} dA/da \), then one obtains

\[
k_b = \sum_{i>0} x_{1,i}. \tag{5}
\]

We can then state the following:

**Proposition 2.1.** Let \( X \) be a finite Bernoulli set over the alphabet \( \{a,b\} \). The index of the letter \( a \) (resp. \( b \)) in \( X \) equals the number of words of \( X \) having one occurrence of the letter \( b \) (resp. \( a \)).
Let us now assume $a = 1/2$. One obtains by Eq. (3) the relation
\[ k_a 2^{-k_a} - k_b 2^{-k_b} + \sum_{i,j>0} x_{i,j}(i-j)2^{-(i+j)} = 0. \]
Let us set $i + j = n$. Since $x_{0,i} = \delta_{i,k_b}$ and $x_{i,0} = \delta_{i,k_a}$, where $\delta_{i,j}$ denotes the symbol of Kronecker, we can rewrite the preceding formula as
\[ \sum_{n>0} \sum_{i=0}^n x_{i,n-i}(2i-n)2^{-n} = 0. \]
One easily checks that $k_a \leq k_b$ if and only if $k_a 2^{-k_a} \geq k_b 2^{-k_b}$.

Let $X$ be a finite set on the alphabet $\{a,b\}$ such that there exist and are unique the exponents $k_a$ and $k_b$ such that $a^{k_a}, b^{k_b} \in X$. If $k_a \leq k_b$ and, moreover, for all words $x \in X = X \setminus \{a^{k_a}, b^{k_b}\}$, one has $2|x|_a \geq |x|$, where the inequality is strict for at least one word $x \in X_0$, then one has that Eq. (6) is not satisfied so that $X$ is not a Bernoulli set and then cannot be a maximal code.

We consider now a finite set $X$ over the alphabet $\{a,b\}$ such that there exists a letter $x$ and a unique exponent $k_a$ for which $x^{k_a} \in X$.

**Proposition 2.2.** Let $X \subseteq \{a,b\}^+$ be a finite set over $\{a,b\}$ such that there exists a letter, say $a$, and a unique exponent $k_a$ for which $a^{k_a} \in X$. The following holds:
1. If for any $\pi \in \text{PBD}$, $\pi(X) \leq 1$, then $k_a \geq \sum_{i \geq 0} x_{i,1}$.
2. If for any $\pi \in \text{PBD}$, $\pi(X) \geq 1$, then $k_a \leq \sum_{i \geq 0} x_{i,1}$.

**Proof.** One easily derives that
\[ \lim_{a \to 1} \frac{dA}{da} = k_a - \sum_{i \geq 0} x_{i,1}. \]
Let us suppose that for any $a \in (0,1)$ one has $A(X,a) \leq 1$ (resp. $A(X,a) \geq 1$). Since $A(X,1) = \lim_{a \to 1} A(X,a) = 1$, then $A(X,a)$ is non-decreasing (resp. non-increasing) in the point $a = 1$ so that $k_a \geq \sum_{i \geq 0} x_{i,1}$ (resp. $k_a \leq \sum_{i \geq 0} x_{i,1}$).

An interesting consequence is the following (cf. [2]):

**Corollary 2.1.** Let $X \subseteq \{a,b\}^+$ be a finite set over $\{a,b\}$ such that there exists a letter, say $a$, and a unique exponent $k_a$ for which $a^{k_a} \in X$. Then, one has
1. If $X$ is a code, then $k_a \geq \sum_{i \geq 0} x_{i,1}$.
2. If $X$ is a complete set, then $k_a \leq \sum_{i \geq 0} x_{i,1}$.

**Proof.** If $X$ is a code, then from the generalized Kraft–McMillan inequality (cf. [2]) one has that for any $\pi \in \text{PBD}$ one has $\pi(X) \leq 1$. If $X$ is a finite complete set, then from the Schützenberger theorem (cf. Theorem 1.1) one has that for any $\pi \in \text{PBD}$ one has $\pi(X) \geq 1$, so that from the preceding proposition the result follows.

**Example 2.** Let us consider the set $Y = \{a^2ba, a^2b, ba, b\}$ and $X = \{a^3\} \cup Y$. The set $X$ is complete as one easily verifies. However, $k_a = 3 < \sum_{i \geq 0} x_{i,1} = 4$, so that $X$ is not a
code. Conversely, the set $X = \{a^5\} \cup Y$ is a code. However, since $k_a = 5 > \sum_{i \geq 0} x_{i,1} = 4$, $X$ is not complete.

3. Higher derivatives

Let us rewrite $A(X,a) = \sum_{i,j \in \mathbb{N}} x_{i,j} a^i (1 - a)^j$ as

$$A(X,a) = \sum_{i,j \in \mathbb{N}} x_{i,j} \sum_{r=0}^{j} (-1)^r \binom{j}{r} a^{i+r}.$$  

For any $k > 0$ one has for all $a \in (0,1)$:

$$\frac{d^k A(X,a)}{d a^k} = \sum_{i,j \in \mathbb{N}} x_{i,j} \sum_{r=\max\{0,k-i\}}^{j} (-1)^r \binom{j}{r} \frac{(r+i)!}{(r+i-k)!} a^{i+r-k} = 0.$$

Let us make the $\lim_{a \to 0} d^k A/da^k$. All the terms vanish except when $r = k - i$, so that one derives for all $k > 0$ the following formula:

$$\sum_{i \leq k} \sum_{j \geq k-i} (-1)^j \binom{j}{k-i} x_{i,j} = 0. \quad (7)$$

For obvious reasons of symmetry the $\lim_{a \to 1} d^k A/da^k$ is given by

$$\sum_{i \leq k} \sum_{j \geq k-i} (-1)^j \binom{j}{k-i} x_{j,i} = 0. \quad (8)$$

For $k = 2$ by Eqs. (4) and (5) one obtains

$$k_a(k_a - 1) = 2 \sum_{i \geq 0} ix_{i,1} - 2 \sum_{i \geq 0} x_{i,2}$$

and

$$k_b(k_b - 1) = 2 \sum_{i \geq 0} ix_{1,i} - 2 \sum_{i \geq 0} x_{2,i}.$$

Let us take now $k = L$ where $L = L_X$ is the maximal length of the words of $X$. In this case Eq. (7) becomes

$$\sum_{p=0}^{L} (-1)^p x_{p,L-p} = 0.$$

If Eq. (7) is satisfied for $k > 0$, then one has

$$\frac{1}{k!} \left( \frac{d^k A}{d a^k} \right)_{a=0} = 0,$$
so that from the McLaurin’s expansion of the polynomial $A(X,a)$, one has

$$A(X,a) = A(X,0) = 1$$

for all $a \in [0,1]$. Let us, moreover, observe that the left-hand side of Eq. (7) for $k = 0$ becomes

$$\sum_{j \geq 0} x_{0,j}.$$ 

This quantity by Proposition 1.1 is equal to 1. We can then state the following:

**Proposition 3.1.** Let $X$ be a finite subset of $\{a,b\}^+$. $X$ is a Bernoulli set if and only if for all $k \geq 0$

$$\sum_{i \leq k} \sum_{j \geq k-i} (-1)^j \binom{j}{k-i} x_{i,j} = \delta_{0,k}. \quad (9)$$

4. Polynomials

Let $\pi \in \mathbb{PBD}$ and $Q = Q(a,b)$ be a polynomial with integral coefficients. One can extend $\pi$ to $\mathbb{Z}[a,b]$ by setting

$$\pi(Q) = Q(\pi(a), \pi(b)).$$

For any polynomial $P \in \mathbb{Z}[a,b]$ we shall denote by $\deg_a(P)$ (resp. $\deg_b(P)$) the degree of $P$ in $a$ (resp. in $b$).

Let $X$ be a finite Bernoulli set over $\{a,b\}$ and consider $X$. Since $X - 1$ vanishes for $b = 1 - a$ it follows from Ruffini’s theorem that $a + b - 1$ has to divide $X - 1$, so that, as one easily derives, there exists a polynomial $P \in \mathbb{Z}[a,b]$ such that $\deg_a(P) = \deg_a(X) - 1$ and $\deg_b(P) = \deg_b(X) - 1$ and $X - 1 = P(a+b-1)$. Conversely, if the above relation is satisfied, then for any $\pi \in \mathbb{PBD}$, $\pi(X) - 1 = 0$ and $X$ is a Bernoulli set. Thus, one derives the following theorem (cf. [2]) which gives a further characterization of the finite Bernoulli sets over $\{a,b\}$.

**Theorem 4.1.** A finite set $X$ over the alphabet $\{a,b\}$ is a Bernoulli set if and only if $a + b - 1$ divides the polynomial $X - 1$, i.e.,

$$X - 1 = P(a + b - 1), \quad (10)$$

where $P$ is a polynomial of $\mathbb{Z}[a,b]$.

**Example 3.** Consider the set $X = \{a,bb,baa,bab\}$. The characteristic polynomial is $X = a + b^2 + ba^2 + bab$. The commutative polynomial $X$ is $X = a + b^2 + a^2b + ab^2$. As
one easily verifies either directly or by using Eq. (9), $X$ is a Bernoulli set and

$$X - 1 = (a + b - 1)(ab + b + 1),$$

so that $P = ab + b + 1$.

Let us observe that there are cases of finite Bernoulli sets $X$ for which the polynomial $P$ has some coefficients which are negative integers. This is shown by the following example due to Perrin [7]:

**Example 4.** Consider the set $X = \{a^3, a^2 ba^2, a^3 b^2, ab, ba, abab, b^2 a^2, b^2 ab^2, b^3\}$, which is a Bernoulli set as one easily verifies either directly or by Eq. (9). One has

$$X - 1 = (a + b - 1)((a^3 b + a^2 + a^2 b + a^3 b - a^2 b^2 + ab + ab^2 + ab^3 + a + b^2 + b + 1).$$

In such a case $\deg_a(X) = 4$.

A further simpler example is the following.

**Example 5.** Consider the set $X = \{a^4, ba^2, a^2 b, aba, ba, b^3 a, b^2\}$ which is a Bernoulli set. One has

$$X - 1 = (a + b - 1)(b^2 a + b + ba - ba^2 + a^3 + a^2 + a + 1).$$

In such a case $\deg_a(X) = 4$ and $\deg_b(X) = 3$.

We shall now analyze some general properties of the polynomial

$$P(a, b) = \sum_{i,j \in \mathbb{N}} p_{i,j} a^i b^j$$

with $p_{i,j} \in \mathbb{Z}$ and $\deg_a(P) = \deg_a(X) - 1$ and $\deg_b(P) = \deg_b(X) - 1$.

**Proposition 4.1.** Let $X$ be a finite Bernoulli set over $\{a, b\}$ and $X - 1 = P(a + b - 1)$. Then

$$p_{0,j} = 1 \text{ for } 0 \leq j < k_b, \quad p_{0,j} = 0 \text{ for } j \geq k_b$$

and

$$p_{j,0} = 1 \text{ for } 0 \leq j < k_a, \quad p_{j,0} = 0 \text{ for } j \geq k_a.$$  

**Proof.** From the equation $X - 1 = P(a + b - 1)$ one obtains for $a = 0$

$$X(0, b) - 1 = P(0, b)(b - 1).$$

Since $X(0, b) = b^{k_b}$ we have

$$b^{k_b} - 1 = P(0, b)(b - 1),$$

so that

$$P(0, b) = 1 + b + b^2 + \ldots + b^{k_b - 1}. $$
Hence, \( p_{0,j} = 1 \) for \( 0 \leq j < k_b \) and \( p_{0,j} = 0 \) for \( j \geq k_b \). In a similar way if one considers the basic Eq. (10) for \( b = 0 \), then one obtains

\[
P(a, 0) = 1 + a + a^2 + \cdots + a^{b-1},
\]

that proves the second part of our assertion. □

An important relation exists between the coefficients of polynomials \( X \) and \( P \).

**Proposition 4.2.** The following holds:

\[
x_{0,0} = 1 - p_{0,0} = 0
\]

and for \( m, n > 0 \):

\[
x_{m,0} = -p_{m,0} + p_{m-1,0}, \quad x_{0,n} = -p_{0,n} + p_{0,n-1},
\]

\[
x_{m,n} = -p_{m,n} + p_{m-1,n} + p_{m,n-1}.
\]

**Proof.** Trivial from Eq. (10) by using the principle of identity of polynomials. □

**Proposition 4.3.** Let \( r \) and \( h \) be positive integers. Then,

\[
\sum_{k=0}^{r} x_{h,k} = -p_{h,r} + \sum_{k=0}^{r} p_{h-1,k}
\]

and

\[
\sum_{k=0}^{r} x_{k,h} = -p_{r,h} + \sum_{k=0}^{r} p_{k,h-1}.
\]

**Proof.** From the previous proposition one has

\[
\sum_{k=0}^{r} x_{h,k} = -\sum_{k=0}^{r} p_{h,k} + \sum_{k=0}^{r} p_{h-1,k} + \sum_{k=1}^{r} p_{h,k-1} = -p_{h,r} + \sum_{k=0}^{r} p_{h-1,k}.
\]

In a symmetric way one proves the second part of the statement. □

**Corollary 4.1.** For all \( h > 0 \)

\[
\sum_{k \geq 0} x_{h,k} = \sum_{k \geq 0} p_{h-1,k}
\]

and for all \( k > 0 \)

\[
\sum_{h \geq 0} x_{k,h} = \sum_{h \geq 0} p_{h,k-1}.
\]

**Proof.** It is sufficient to observe that \( p_{h,r} \) (resp. \( p_{r,h} \)), vanishes when \( h \geq \deg_a(X) \) (resp. \( r \geq \deg_b(X) \)). □
Corollary 4.2. If $k_a$ and $k_b$ are the indices of the letters $a$ and $b$ in $X$, then
\[
\sum_{h \geq 0} x_{h,1} = \sum_{h \geq 0} p_{h,0} = k_a
\]
and
\[
\sum_{k \geq 0} x_{1,k} = \sum_{k \geq 0} p_{0,k} = k_b.
\]

Proof. Trivial from the preceding corollary and Proposition 1.1.

Theorem 4.2. Let $(x_{i,j})_{i,j \in \mathbb{N}}$ and $(p_{i,j})_{i,j \in \mathbb{N}}$ be any two infinite matrices of integers satisfying Eq. (11). Then for $m,n \geq 0$ one has:
\[
p_{n,m} = \left(\frac{m+n}{m}\right) - \sum_{0 \leq j \leq m, j+1 \leq i \leq n} \left(\frac{m+n-i-j}{m-j}\right) x_{i,j} - \sum_{0 \leq i \leq n, i+1 \leq j \leq m} \left(\frac{m+n-2i}{m-i}\right) x_{i,j}.
\]

Proof. Let us denote the r.h.s. of the preceding equation by $q_{n,m}$. The proof is by induction on the integer $k = n + m$. For $k = 0$ one has trivially $q_{0,0} = p_{0,0} = 1$. We suppose the statement true up to $k-1$ and we will prove it for $k$. We make use of the formula
\[
p_{n,m} = p_{n,m-1} + p_{n-1,m} - x_{n,m}
\]
(where $p_{i,j} = 0$ if $i$ or $j$ are negative integers). By induction one has:
\[
p_{n,m} = q_{n,m-1} + q_{n-1,m} - x_{n,m}.
\]
Hence, we have to prove that
\[
q_{n,m-1} + q_{n-1,m} - x_{n,m} = q_{n,m}.
\]
It is convenient to set for $n,m \in \mathbb{Z}$:
\[
A_{n,m} = \begin{cases}
\sum_{0 \leq j \leq m, j+1 \leq i \leq n} \left(\frac{m+n-i-j}{m-j}\right) x_{i,j} & \text{if } n > 0, m \geq 0, \\
0 & \text{otherwise},
\end{cases}
\]
\[
B_{n,m} = \begin{cases}
\sum_{0 \leq i \leq n, i+1 \leq j \leq m} \left(\frac{m+n-i-j}{n-i}\right) x_{i,j} & \text{if } m > 0, n \geq 0, \\
0 & \text{otherwise},
\end{cases}
\]
\[
C_{n,m} = \begin{cases}
\sum_{i=1}^{\min\{n,m\}} \left(\frac{m+n-2i}{m-i}\right) x_{i,i} & \text{if } \min\{n,m\} \geq 1, \\
0 & \text{otherwise}.
\end{cases}
\]
Thus, one can write

\[ q_{n,m} = \binom{m + n}{m} - A_{n,m} - B_{n,m} - C_{n,m}. \]  

(13)

We shall use in the proof often the combinatorial identity: for \(0 < k \leqslant n\)

\[ \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}. \]

We have to consider the following cases.

**Case 1: \(m < n\).** One proves that

\[
\begin{align*}
A_{n, m-1} + A_{n-1, m} &= A_{n, m} - x_{n, m}, \\
B_{n, m-1} + B_{n-1, m} &= B_{n, m}, \\
C_{n, m-1} + C_{n-1, m} &= C_{n, m}.
\end{align*}
\]

(14)

Hence, from Eq. (13) one derives Eq. (12).

**Case 2: \(m > n\).** One proves that

\[
\begin{align*}
A_{n, m-1} + A_{n-1, m} &= A_{n, m}, \\
B_{n, m-1} + B_{n-1, m} &= B_{n, m} - x_{n, m}, \\
C_{n, m-1} + C_{n-1, m} &= C_{n, m}.
\end{align*}
\]

(15)

From Eq. (13), Eq. (12) follows.

**Case 3: \(m = n\).** In this case one proves that

\[
\begin{align*}
A_{n, n-1} + A_{n-1, n} &= A_{n, n}, \\
B_{n, n-1} + B_{n-1, n} &= B_{n, n}, \\
C_{n, n-1} + C_{n-1, n} &= C_{n, n} - x_{n, n}.
\end{align*}
\]

(16)

Also, in this case one derives Eq. (12).

Let us consider the case \(m < n\). If \(m = 0\) or \(m = 1\), Eqs. (14) are trivially verified. Let us then suppose \(m > 1\). Let us first prove that \(A_{n, m-1} + A_{n-1, m} = A_{n, m} - x_{n, m}\). One has

\[
A_{n, m-1} = \sum_{j=0}^{m-1} \sum_{i=j+1}^{n-1} \binom{m + n - 1 - i - j}{m - 1 - j} x_{i, j} + \sum_{j=0}^{m-1} x_{n, j}
\]

and

\[
A_{n-1, m} = \sum_{j=0}^{m-1} \sum_{i=j+1}^{n-1} \binom{m + n - 1 - i - j}{m - j} x_{i, j} + \sum_{i=m+1}^{n-1} x_{i, m}.
\]

Since

\[
A_{n, m} = \sum_{j=0}^{m-1} \sum_{i=j+1}^{n-1} \binom{m + n - i - j}{m - j} x_{i, j} + \sum_{j=0}^{m-1} x_{n, j} + \sum_{i=m+1}^{n-1} x_{i, m} + x_{n, m},
\]

the result follows.
As regard the second equation one has since $m<n$:

$$B_{n,m-1} = \sum_{i=0}^{m-2} \sum_{j=i+1}^{m-1} \binom{m+n-1-i-j}{n-i} x_{i,j}$$

and

$$B_{n-1,m} = \sum_{i=0}^{m-2} \sum_{j=i+1}^{m-1} \binom{m+n-1-i-j}{n-1-i} x_{i,j} + \sum_{i=0}^{m-1} x_{i,m}.$$ 

Since

$$B_{n,m} = \sum_{i=0}^{m-2} \sum_{j=i+1}^{m-1} \binom{m+n-1-i-j}{n-i} x_{i,j} + \sum_{i=0}^{m-1} x_{i,m},$$

one has that $B_{n,m-1} + B_{n-1,m} = B_{n,m}$.

As regard the third equation one has

$$C_{n,m-1} = \sum_{i=1}^{m-1} \binom{m+n-1-2i}{m-1-i} x_{i,i}$$

and

$$C_{n-1,m} = \sum_{i=1}^{m-1} \binom{m+n-1-2i}{m-i} x_{i,i} + x_{m,m}.$$ 

Since,

$$C_{n,m} = \sum_{i=1}^{m-1} \binom{m+n-2i}{m-i} x_{i,i} + x_{m,m},$$

it follows that $C_{n,m-1} + C_{n-1,m} = C_{n,m}$.

The case $m>n$ is symmetrically dealt with. Finally, the proof in the case $m=n$ is similar to that of previous cases. \qed

**Example 6.** We report the values of $p_{n,m}$ for some values of $n$ and $m$. Each $p_{n,m}$ is a polynomial of first degree in the variables $x_{i,j}$, $0 \leq i \leq n$ and $0 \leq j \leq m$. Note that the polynomial $p_{n,n}$ is obtained from $p_{n,m}$ by changing in its expression $x_{i,j}$ with $x_{j,i}$, $0 \leq i \leq n$ and $0 \leq j \leq m$. One has

$$p_{1,0} = 1 - x_{1,0},$$
$$p_{2,0} = 1 - x_{1,0} - x_{2,0}, \quad p_{1,1} = 2 - x_{0,1} - x_{1,0} - x_{1,1},$$
$$p_{3,0} = 1 - x_{1,0} - x_{2,0} - x_{3,0}, \quad p_{2,1} = 3 - x_{0,1} - 2x_{1,0} - x_{2,0} - x_{1,1} - x_{2,1},$$
$$p_{3,1} = 4 - x_{0,1} - 3x_{1,0} - 2x_{2,0} - x_{2,1} - x_{3,0} - x_{1,1} - x_{3,1},$$
$$p_{2,2} = 6 - 3x_{1,0} - 3x_{0,1} - x_{0,2} - x_{2,0} - x_{1,2} - x_{2,1} - 2x_{1,1} - x_{2,2},$$
$$p_{1,3} = 4 - x_{1,0} - 3x_{0,1} - 2x_{0,2} - x_{1,2} - x_{0,3} - x_{1,1} - x_{1,3}. $$
Let $X$ be a finite Bernoulli set. The following propositions allow one, starting from $X$, to construct Bernoulli sets having a larger cardinality.

**Proposition 4.4.** Let $X$ be a finite Bernoulli set over $\{a,b\}$ and $k_b$ be the index of the letter $b$ in $X$. For any $1 \leq n \leq k_b$ the set

$$Z_n = a(X \cup \{b,b^2,\ldots,b^{n-1}\}) \cup \{b^n\}$$

is a Bernoulli set. Moreover, if $X - 1 = P(a + b - 1)$, then

$$Z_n - 1 = Q_n(a + b - 1)$$

with

$$Q_n = aP + b^{n-1} + \cdots + b + 1.$$ 

**Proof.** One can directly prove, by using any positive Bernoulli distribution $\pi$, that $\pi(Z_n) = 1$, so that $Z_n$ is a Bernoulli set. However, this can also be proved by Theorem 4.1, showing that $Q_n(a + b - 1) = Z_n - 1$. Indeed, one has

$$(aP + b^{n-1} + \cdots + b + 1)(a + b - 1) = aP(a + b - 1) + \sum_{i=0}^{n-1} ab^i + \sum_{i=0}^{n-1} (b - 1)b^i.$$ 

Since $X - 1 = P(a + b - 1)$ one derives

$$Q_n(a + b - 1) = a(X - 1) + \sum_{i=1}^{n-1} ab^i + a + b^n - 1 = a(X + b + \cdots + b^{n-1}) + b^n - 1.$$ 

As $b^i \not\in X$ ($i = 1, \ldots, n - 1$) then

$$a(X + b + \cdots + b^{n-1}) + b^n = Z_n$$

that concludes the proof. \(\square\)

In a similar way, one derives the following proposition whose proof we omit.

**Proposition 4.5.** Let $X$ be a finite Bernoulli set over $\{a,b\}$. For any $n \geq 1$ the set

$$Z_n = (aX) \cup \{b,b^2,\ldots,b^{n-1}\}a \cup \{b^n\}$$

is a Bernoulli set. Moreover, if $X - 1 = P(a + b - 1)$, then

$$Z_n - 1 = Q_n(a + b - 1)$$

with

$$Q_n = aP + b^{n-1} + \cdots + b + 1.$$ 

Let $X$ and $Y$ be two sets and let $w \in X$ be a word such that $(X \setminus \{w\}) \cap wY = \emptyset$. One can then associate with $X$, $Y$, and $w$ the set

$$Z = (X \setminus \{w\}) \cup wY.$$
This kind of operation of composition of the sets \( X \) and \( Y \) has been recently considered by Anselmo [1] in the case of factorizing codes.

**Proposition 4.6.** Let \( X \) and \( Y \) be EFFnite Bernoulli sets over \( \{a, b\} \) and \( w \in X \) be such that \((X \setminus \{w\}) \cap wY = \emptyset\). Then the set \( Z = (X \setminus \{w\}) \cup wY \) is a Bernoulli set. Moreover, if

\[
X - 1 = P(a + b - 1), \quad Y - 1 = Q(a + b - 1),
\]

then

\[
Z - 1 = (P + wQ)(a + b - 1).
\]

**Proof.** Since \( X \) and \( Y \) are EFFnite Bernoulli sets one has \( X - 1 = P(a + b - 1) \) and \( Y - 1 = Q(a + b - 1) \). Hence, under the made hypotheses one has

\[
(P + wQ)(a + b - 1) = X - 1 + w(Y - 1) = X\setminus\{w\} + wY - 1 = Z - 1.
\]

\( \square \)

5. Commutative equivalence

We consider in \( \mathcal{A}^+ \) the relation of commutative equivalence \( \sim \) defined as follows: two words \( u, v \in \mathcal{A}^+ \) are commutatively equivalent and we write \( u \sim v \) if

\[ |u|_a = |v|_a \quad \text{for any } a \in \mathcal{A}. \]

Two subsets \( X \) and \( Y \) of \( \mathcal{A}^+ \) are commutatively equivalent and we write \( X \sim Y \), if there exists a bijection \( \delta : X \to Y \) such that for any \( x \in X \) one has \( x \sim \delta(x) \). In terms of the commutative characteristic series one has that \( X \sim Y \) if and only if

\[ X = Y. \]

We recall that a code \( X \) on the alphabet \( \mathcal{A} \) is called prefix code if

\[ X \cap \mathcal{A}_X^+ = \emptyset, \]

i.e., no word \( x \in X \) is a proper prefix of \( y \in X \). A set is called commutatively prefix if it is commutatively equivalent to a prefix code.

The following conjecture was formulated by M.P. Schützenberger at the end of 1950s (cf. [8, 2, 4, 5]):

**Conjecture 1.** Any finite and complete code is commutatively prefix.

Shor [9] has shown the existence of a finite code which is not complete and is not commutatively prefix. Since any code has always a, possibly infinite, completion, both the hypotheses that the code is finite and complete are necessary. It is still open whether the Shor’s code has a finite completion. A reformulation of the conjecture in terms of continued fractions is in [6].
Let us observe that if one replaces in the conjecture the hypothesis of a set $X$ which is a finite and complete code with a finite Bernoulli set $X$, then one has in general a false statement. Indeed, the sets $X$ of the Examples 4 and 5 are finite Bernoulli sets but they are not commutatively prefix. Indeed, one can directly show that either of the two previous sets is not commutatively equivalent to any code. Let, for instance,

$$X = \{a^4, ba^2, a^2b, aba, ba, b^3a, b^2\}.$$ 

If $Y$ is any set commutatively equivalent to $X$, then $Y$ has to contain the subset $Z$ of $X$ given by

$$Z = \{a^4, ba^2, a^2b, aba, b^2\}.$$ 

Moreover, $Y$ has to contain either $ab$ or $ba$. Since the sets $Z \cup \{ab\}$ and $Z \cup \{ba\}$ are not codes, $Y$ cannot be a code.

One can also show that the sets $X$ of the Examples 4 and 5 are not commutatively prefix by using Proposition 5.2 reported below and the fact that the polynomials $(X - 1)/(a + b - 1)$ have one negative coefficient.

The following holds (cf. [2]):

**Proposition 5.1.** Let $X$ be any subset of $\{a, b\}^+$. $X$ is commutatively prefix if and only if the series

$$\frac{X - 1}{a + b - 1}$$

has non-negative coefficients.

From the preceding proposition and Theorem 4.1 one derives

**Proposition 5.2.** A finite Bernoulli set $X$ over $\{a, b\}$ is commutatively prefix if and only if the polynomial

$$\frac{X - 1}{a + b - 1}$$

has non-negative coefficients.

**Corollary 5.1.** Let $X$ be a finite Bernoulli set over $\{a, b\}$ such that for any $x \in X$, $|x|_b \leq 2$. Then $X$ is commutatively prefix.

**Proof.** Let $X - 1 = P(a + b - 1)$. Since for any $x \in X$, $|x|_b \leq 2$ one has $\deg_b(P) \leq 1$, so that $p_{i,j} = 0$ if $i > 0$ and $j \geq 2$. Moreover, from Proposition 4.1, $p_{j,0} = 1$ for $0 \leq j < k_a$ and $p_{j,0} = 0$ for $j \geq k_a$. From Corollary 4.1 one has for $h > 0$

$$x_{h,0} + x_{h,1} + x_{h,2} = p_{h-1,0} + p_{h-1,1}.$$
If $h-1 \geq k_a$, then $p_{h-1,0} = 0$ so that $p_{h-1,1} \geq 0$. Let us then consider the case $h \leq k_a$.

In this case $p_{h-1,0} = 1$ and

$$p_{h-1,1} = x_{h,0} + x_{h,1} + x_{h,2} - 1.$$  

If $h = k_a$ then $x_{h,0} = 1$, so that $p_{k_a-1,1} = x_{h,1} + x_{h,2} \geq 0$. Let us then suppose that $0 < h < k_a$. From Proposition 4.2 one derives

$$p_{h,1} = p_{h-1,1} + p_{h,0} - x_{h,1} = x_{h,1} + x_{h,2} - 1 + 1 - x_{h,1} = x_{h,2} \geq 0,$$

and this concludes the proof.

Let us observe that above result is not true, in general, if one supposes that $X$ is a finite Bernoulli set such that for any $x \in X$, $|x|_b \leq 3$. This is shown by Example 5 since in such a case $\text{deg}_b(X) = 3$ and $X$ is not commutatively prefix. However, as a consequence of a result of de Felice (cf. [4, 5]), the result is true under the hypothesis that $X$ is a finite code.

Proposition 5.3. Let $X$ be a finite Bernoulli set over $\{a,b\}$, $k_b$ be the index of the letter $b$ in $X$, and, for any $1 \leq n \leq k_b$, $Z_n$ be the set

$$Z_n = a(X \cup \{b \in \{b^2, \ldots, b^{n-1}\} \} \cup \{b^n\}.$$  

One has that $X$ is commutatively prefix if and only if $Z_n$ is so.

Proof. By Proposition 4.4 if $X - 1 = P(a + b - 1)$, then $Z_n - 1 = Q_n(a + b - 1)$ with $Q_n = aP + b^{n-1} + \cdots + b + 1$. Since $P$ has non-negative coefficients if and only if $Q_n$ has this property, it follows that $X$ is commutatively prefix if and only if so is $Z_n$.

In a similar way by Proposition 4.5 one derives

Proposition 5.4. Let $X$ be a finite Bernoulli set over $\{a,b\}$ and $n \geq 1$. The set $X$ is commutatively prefix if and only if the set

$$Z_n = (aX \cup \{b \in \{b^2, \ldots, b^{n-1}\} \} \cup \{b^n\}$$  

is commutatively prefix.

Proposition 5.5. Let $X$ and $Y$ be finite Bernoulli sets over $\{a,b\}$ and $w \in X$ be such that $(X \setminus \{w\}) \cap wY = \emptyset$. If $X$ and $Y$ are commutatively prefix, then the set $Z = (X \setminus \{w\}) \cup wY$ is commutatively prefix.

Proof. By Proposition 4.6 one has that if

$$X - 1 = P(a + b - 1), \quad Y - 1 = Q(a + b - 1),$$  

then

$$Z - 1 = (P + wQ)(a + b - 1).$$
Since the polynomials $P$ and $Q$ have all coefficients which are non-negative also the coefficients of $P + wQ$ will be non-negative. By Proposition 5.2 the set $Z$ is commutatively prefix.

Let us observe that the converse of the preceding proposition does not, in general, hold. In fact, the set $Z = (X \setminus \{w\}) \cup wY$ can be commutatively prefix while $X$ or $Y$ are not so. This is shown by the following:

**Example 7.** Let $X$ be the set of the Example 5, i.e.,

$$X = \{a^4, ba^2, a^2 b, aba, ba, b^3 a, b^2\}.$$  

Let, moreover, $Y = \{a^2, ab, ba, b^2\}$ and $w = ba^2$. One has that $X$ and $Y$ are Bernoulli sets, $(X \setminus \{ba^2\}) \cap ba^2 Y = \emptyset$ and

$$Z = \{a^4, ba^4, ba^3 b, a^2 b, ba^2 ba, ba^2 b^2, aba, b^3 a, ba, b^2\}.$$  

Moreover, one has $Q = a + b + 1$ and (cf. Example 5) $P = b^2 a + b + ba - ba^2 + a^3 + a^2 + a + 1$, so that

$$P + a^2 bQ = a^3 b + a^3 + a^2 b^2 + ab^2 + ab + b + a^2 + a + 1.$$  

Since the coefficients of this polynomial are non-negative, $Z$ is commutatively prefix while $X$ is not so.

Let us mention that under the hypotheses of Proposition 5.5 when $X$ and $Y$ are factorizing codes, then $Z$ is also a factorizing code [1]. This, trivially, implies that $Z$ is commutatively prefix.

Let $X \subseteq \{a, b\}^+$ be a finite set and $M = NL + 1$. If $X$ and $X^M$ are Bernoulli sets, then, by Proposition 1.2, $X$ is a maximal code. Conversely, if $X$ is a maximal code, then $X$ and $X^M$ are Bernoulli sets. Hence, by Theorem 4.1 and Proposition 5.2, Conjecture 1 can be, equivalently, restated, in the case of a two-letter alphabet, as follows.

Let $X \subseteq \{a, b\}^+$ be a finite set. If $X$ and $X^M$ are Bernoulli sets, then $X$ is commutatively prefix.

In other words if there exist polynomials $P, Q \in \mathbb{Z}[a, b]$ such that

$$X - 1 = P(a + b - 1) \quad \text{and} \quad X^M - 1 = Q(a + b - 1),$$

then the coefficients of $P$ are non-negative integers.

Let us observe that, if $X$ and $X^M$ are Bernoulli sets, then $X$ is a complete code, so that for any $n \geq 1$, $X^n$ is a complete code and $X^n = X^n$. Thus, one has for all $n > 0$

$$X^n - 1 = Q_n(a + b - 1)$$

with $Q_n \in \mathbb{Z}[a, b]$ and $Q_1 = P$.

There exists the following relation between polynomials $Q_{n+1}$ and $Q_n$, $n \geq 1$:

$$Q_{n+1} = Q_n + PX^n.$$
so that
\[ Q_n = P(1 + X + X^2 + \cdots + X^{n-1}). \]
From this one derives the trivial fact that if \( X \) is commutatively prefix, then so will be \( X^n \) for all \( n > 0 \). One can pose the following conjectures.

**Conjecture 2.** Let \( X \) be a finite and complete code. If an integer \( n > 1 \) exists such that \( X^n \) is commutatively prefix, then \( X \) will be so.

In other words if there exists an integer \( n > 1 \) such that \( Q_n \) has non-negative coefficients, then also \( P \) will have non-negative coefficients.

**Conjecture 3.** Let \( X \) be a finite and complete code. There exists an integer \( n > 1 \) such that \( X^n \) is commutatively prefix.

In other words if \( X \) is a finite and complete code, then there exists always an integer \( n > 1 \) such that \( Q_n \) has non-negative coefficients.

Let us observe that Conjecture 1 has a positive answer if and only if both Conjectures 2 and 3 have a positive answer.

Let \( X \) be a set over the alphabet \( \{a, b\} \) and
\[
X = \sum_{i,j \in \mathbb{N}} x_{i,j} a^i b^j.
\]
It is convenient to extend the definition of \( x_{i,j} \) from \( \mathbb{N} \times \mathbb{N} \) to \( \mathbb{Z} \times \mathbb{Z} \) by setting \( x_{i,j} = 0 \) if \( i < 0 \) or \( j < 0 \). We denote by \( D_X \), or simply \( D \), the map \( D: \mathbb{Z} \times \mathbb{Z} \to \mathbb{N} \) recursively defined as
\[
D(n, m) = 0 \quad \text{if} \quad n < 0 \quad \text{or} \quad m < 0, \\
D(0, 0) = D(1, 0) = D(0, 1) = 1, \\
D(i, j) = D(i-1, j) - x_{i-1,j} + D(i, j-1) - x_{i,j-1}, \quad \text{for} \quad i, j \geq 0 \quad \text{and} \quad i + j > 1.
\]

Let us observe that the value of \( D(n, m) \) depends on the values of \( x_{i,j} \) with \( i \leq n, j \leq m \) and \( i + j < n + m \).

**Proposition 5.6.** Let \( X \subseteq \{a, b\}^+ \) be a set and \( X \) its commutative characteristic series. \( X \) is commutatively prefix if and only if for all \( i, j \geq 0 \)
\[
x_{i,j} \leq D(i, j).
\]

**Proof.** (\( \Leftarrow \)). Let us set
\[
p_{i,j} = D(i, j) - x_{i,j} \geq 0.
\]
One derives:
\[
p_{0,0} = 1, \quad p_{1,0} = 1 - x_{1,0}, \quad p_{0,1} = 1 - x_{0,1}
\]
and for $i + j > 1$,

$$x_{i,j} = -p_{i,j} + p_{i-1,j} + p_{i,j-1}.$$

Let $s$ be the series with non-negative coefficients:

$$s = \sum_{i,j \geq 0} p_{i,j} a^i b^j.$$

One derives

$$s(a + b - 1) = \sum_{i,j \geq 0} x_{i,j} a^i b^j - 1.$$

Since $s$ has non-negative coefficients from Proposition 5.1 one has that $X$ is commutatively prefix.

($\Rightarrow$). If $X$ is commutatively prefix, then by Proposition 5.1

$$X - 1 = s(a + b - 1),$$

where $s = \sum_{i,j \geq 0} p_{i,j} a^i b^j$ and $p_{i,j} \geq 0$ for $i,j \geq 0$. Moreover, from the above equality, one has, $p_{0,0} = 1$, $p_{1,0} = 1 - x_{1,0}$, $p_{0,1} = 1 - x_{0,1}$, and for $i + j > 1$ $x_{i,j} = -p_{i,j} + p_{i-1,j} + p_{i,j-1}$. If we set

$$D(i,j) = p_{i,j} + x_{i,j},$$

then one gets

$$D(i,j) = D(i - 1,j) - x_{i-1,j} + D(i,j - 1) - x_{i,j-1}$$

and $x_{i,j} \leq D(i,j)$. □

An interpretation of the map $D$, as well as a more direct proof of the implication ($\Leftarrow$) in the preceding proof, is obtained as follows.

Let $X$ be a set and consider the complete binary tree. We wish to construct, under the hypothesis that $x_{i,j} \leq D(i,j)$, a prefix code $Y$ such that $X = \subseteq Y$. Let us denote by $E(i,j)$ the number of nodes in the tree representing words having $i$ occurrences of the letter $a$ and $j$ occurrences of the letter $b$ and which can be utilized in order to construct the code $Y$. One has of course $E(0,0) = E(0,1) = E(1,0) = 1$. One must have for all $i,j \geq 0$, $x_{i,j} = y_{i,j} \leq E(i,j)$. Thus if one makes a choice of $x_{i,j}$ such nodes (make a choice of a node means to cut in the general tree the subtree generated by that node) there will remain $q_{i,j} = E(i,j) - x_{i,j}$ nodes. These are prefixes of $q_{i,j}$ nodes having $i + 1$ occurrences of the letter $a$ and $j$ occurrences of the letter $b$ and also prefixes of $q_{i,j}$ nodes having $i$ occurrences of the letter $a$ and $j + 1$ occurrences of the letter $b$. Thus, the following relation holds:

$$E(i,j) = E(i,j - 1) - x_{i,j-1} + E(i - 1,j) - x_{i-1,j}.$$

Hence, one derives that for all $i,j \in \mathbb{N}$, $E(i,j) = D(i,j)$ and, moreover, $q_{i,j} = p_{i,j}$. 
**Proposition 5.7.** For $m, n \geq 0$ one has:

$$D(n, m) = \binom{m + n}{m} - (A_{n-1,m} + A_{n,m-1}) - (B_{n-1,m} + B_{n,m-1}) - (C_{n-1,m} + C_{n,m-1}).$$

**Proof.** Let us set for $m, n \geq 0$

$$p_{n,m} = D(n, m) - x_{n,m}.$$  

The following holds:

$$x_{0,0} = 1 - p_{0,0} = 0$$

and for $m, n > 0$:

$$x_{m,0} = -p_{m,0} + p_{m-1,0}, \quad x_{0,n} = -p_{0,n} + p_{0,n-1}$$

and

$$x_{m,n} = -p_{m,n} + p_{m-1,n} + p_{m,n-1}.$$  

From Theorem 4.2 one has

$$p_{n,m} = \binom{m + n}{m} - A_{n,m} - B_{n,m} - C_{n,m}.$$  

From Eqs. (14), (15), and (16) one has that in all cases:

$$A_{n,m} + B_{n,m} + C_{n,m} = x_{n,m} + (A_{n-1,m} + A_{n,m-1}) + (B_{n-1,m} + B_{n,m-1}) + (C_{n-1,m} + C_{n,m-1});$$

from this the result follows. □

**Example 8.** In the case of the set $X$ of the Example 4 one has that $x_{2,2} = 3$ and $D(2,2) = 2$. Thus, $X$ is not commutatively prefix.

In conclusion, we observe that from Propositions 5.6 and 5.7 a set $X$ on the alphabet \{a, b\} is commutatively prefix if and only if for all $n, m \geq 0$ the number $x_{n,m}$ of the words of $X$ having $n$ occurrences of the letter $a$ and $m$ occurrences of the letter $b$ is upperbounded by the quantity $D(n, m)$ which depends only on the distribution $x_{i,j}$ of the words of $X$ of smaller length and having $i \leq n$ occurrences of the letter $a$ and $j \leq m$ occurrences of the letter $b$.

**References**