On two combinatorial problems arising from automata theory

Jean-Éric Pin
LITP, CNRS and Université Paris 6 (France)

Abstract

We present some partial results on the following conjectures arising from automata theory. The first conjecture is the triangle conjecture due to Perrin and Schützenberger. Let $A = \{a, b\}$ be a two-letter alphabet, d a positive integer and let $B_d = \{a^i b a^j \mid 0 \leqslant i + j \leqslant d\}$. If $X \subset B_d$ is a code, then $|X| \leqslant d + 1$. The second conjecture is due to Černý and the author. Let $\mathcal{A}$ be an automaton with n states. If there exists a word of rank $\leqslant n - k$ in $\mathcal{A}$, there exists such a word of length $\leqslant k^2$.

1 Introduction

The theory of automata and formal langauges provides many beautiful combinatorial results and problems which, I feel, ought to be known. The book recently published: *Combinatorics on words*, by Lothaire [8], gives many examples of this.

In this paper, I present two elegant combinatorial conjectures which are of some importance in automata theory. The first one, recently proposed by Perrin and Schützenberger [9], was originally stated in terms of coding theory. Let $A = \{a, b\}$ be a two-letter alphabet and let A^* be the free monoid generated by A. Recall that a subset C of A^* is a code whenever the submonoid of A^* generated by C is free with base C; i.e., if the relation $c_1 \cdots c_p = c'_1 \cdots c' q$, where $c_1, \ldots, c_p, c'_1, \ldots, c'_q$ are elements of C implies $p = q$ and $c_i = c'_i$ for $1 \leqslant i \leqslant p$. Set, for any $d > 0$, $B_d = \{a^i b a^j \mid 0 \leqslant i + j \leqslant d\}$. One can now state the following conjecture:

The triangle conjecture. *Let $d > 0$ and $X \subset B_d$. If X is a code, then $|X| \leqslant d + 1$.*

The term "The triangle conjecture" originates from the following construction: if one represents every word of the form $a^i b a^j$ by a point $(i, j) \in \mathbb{N}^2$, the set B_d is represented by the triangle $\{(i, j) \in \mathbb{N}^2 \mid 0 \leqslant i + j \leqslant d\}$. The second conjecture was originally stated by Černý (for $k = n - 1$) [3] and extended by the author. Recall that a finite automaton $\mathcal{A}$ is a triple (Q, A, δ), where Q is a finite set (called the set of states), A is a finite set (called the alphabet) and $\delta : Q \times A \to Q$ is a map. Thus δ defines an action of each letter of A on Q. For simplicity, the action of the letter a on the state q is usually denoted by qa. This action can be extended to A^* (the free monoid on A) by the associativity rule

$$(qw)a = q(wa) \text{ for all } q \in Q, w \in A^*, a \in A$$

Thus each word $w \in A^*$ defines a map from Q to Q and the rank of w in $\mathcal{A}$ is the integer $\mathrm{Card}\{qw \mid q \in Q\}$.

One can now state the following

Conjecture (C). *Let $\mathcal{A}$ be an automaton with n states and let $0 \leqslant k \leqslant n - 1$. If there exists a word of rank $\leqslant n - k$ in $\mathcal{A}$, there exists such a word of length $\leqslant k^2$.*

2 The triangle conjecture

I shall refer to the representation of X as a subset of the triangle $\{(i,j) \in \mathbb{N}^2 \mid 0 \leqslant i+j \leqslant d\}$ to describe some properties of X. For example, "X has at most two columns occupied" means that there exist two integers $0 \leqslant i_1 < i_2$ such that X is contained in $a^{i_1}ba^* \cup a^{i_2}ba^*$.

Only a few partial results are known on the triangle conjecture. First of all the conjecture is true for $d \leqslant 9$; this result has been obtained by a computer, somewhere in Italy.

In [5], Hansel computed the number t_n of words obtained by concatenation of n words of B_d. He deduced from this the following upper bound for $|X|$.

Theorem 2.1 *Let $X \subset B_d$. If X is a code, then $|X| \leqslant (1 + (1/\sqrt{2}))(d+1)$.*

Perrin and Schützenberger proved the following theorem in [9].

Theorem 2.2 *Assume that the projections of X on the two components are both equal to the set $\{0, 1, \ldots, r\}$ for some $r \leqslant d$. If X is a code, then $|X| \leqslant r + 1$.*

Two further results have been proved by Simon and the author [15].

Theorem 2.3 *Let $X \subset B_d$ be a set having at most two rows occupied. If X is a code, then $|X| \leqslant d + 1$.*

Theorem 2.4 *Assume there is exactly one column of $X \subset B_d$ with two points or more. If X is a code, then $|X| \leqslant d + 1$.*

Corollary 2.5 *Assume that all columns of X are occupied. If X is a code, then $|X| \leqslant d + 1$.*

Proof. Indeed assume that $|X| > d + 1$. Then one of the columns of X has two points or more. Thus one can find a set $Y \subset X$ such that: (1) all columns but one of Y contain exactly one point; (2) the exceptional column contains two points. Since $|Y| > d + 1$, Y is a non-code by Theorem 2.4. Thus X is a non-code. □

Of course statements 2.3, 2.4, 2.5 are also true if one switches "row" and "column".

3 A conjecture on finite automata

We first review some results obtained for Conjecture (C) in the particular case $k = n-1$: "Let $\mathcal{A}$ be an automaton with n states containing a word of rank 1. Then there exists such a word of length $\leqslant (n-1)^2$."

First of all the bound $(n-1)^2$ is sharp. In fact, let $\mathcal{A}_n = (Q, \{a, b\}, \delta)$, where $Q = \{0, 1, \ldots, n-1\}$, $ia = i$ and $ib = i + 1$ for $i \neq n-1$, and $(n-1)a = (n-1)b = 0$.

Then the word $(ab^{n-1})^{n-2}a$ has rank 1 and length $(n-1)^2$ and this is the shortest word of rank 1 (see [3] or [10] for a proof).

Moreover, the conjecture has been proved for $n = 1, 2, 3, 4$ and the following upper bounds have been obtained

$2^n - n - 1$	(Černý [2], 1964)
$\frac{1}{2}n^3 - \frac{3}{2}n^2 + n + 1$	(Starke [16, 17], 1966)
$\frac{1}{2}n^3 - n^2 + \frac{n}{2}$	(Kohavi [6], 1970)
$\frac{1}{3}n^3 - \frac{3}{2}n^2 + \frac{25}{6}n - 4$	(Černý, Pirická et Rosenauerová [4], 1971)
$\frac{7}{27}n^3 - \frac{17}{18}n^2 + \frac{17}{6}n - 3$	(Pin [11], 1978)

For the general case, the bound k^2 is also the best possible (see [10]) and the conjecture has been proved for $k = 0, 1, 2, 3$ [10]. The best known upper bound was

$$\frac{1}{3}k^3 - \frac{1}{3}k^2 + \frac{13}{6}k - 1[11]$$

We prove here some improvements of these results. We first sketch the idea of the proof. Let $\mathcal{A} = (Q, A, \delta)$ be an automaton with n states. For $K \subset Q$ and $w \in A^*$, we shall denote by Kw the set $\{qw \mid q \in K\}$. Assume there exists a word of rank $\leqslant n - k$ in $\mathcal{A}$. Since the conjecture is true for $k \leqslant 3$, one can assume that $k \geqslant 4$. Certainly there exists a letter a of rank $\neq n$. (If not, all words define a permutation on Q and therefore have rank n).Set $K_1 = Qa$. Next look for a word m_1 (of minimal length) such that $K_2 = K_1m_1$ satisfies $|K_2| < |K_1|$. Then apply the same procedure to K_2, etc. until one of the $|K_i|$'s satisfies $|K_i| \leqslant n - k$:

$$Q \xrightarrow{a} K_1 \xrightarrow{m_1} K_2 \xrightarrow{m_2} \cdots K_{r-1} \xrightarrow{m_{r-1}} K_r \qquad |K_r| \leqslant n - k$$

Then $am_1 \cdots m_{r-1}$ has rank $\leqslant n - k$.

The crucial step of the procedure consists in solving the following problem:

Problem P. Let $\mathcal{A} = (Q, A, \delta)$ be an automaton with n states, let $2 \leqslant m \leqslant n$ and let K be an m-subset of Q. Give an upper bound of the length of the shortest word w (if it exists) such that $|Kw| < |K|$.

There exist some connections between Problem P and a purely combinatorial Problem P'.

Problem P'. Let Q be an n-set and let s and t be two integers such that $s + t \leqslant n$. Let $(S_i)_{1 \leqslant i \leqslant p}$ and $(T_i)_{1 \leqslant i \leqslant p}$ be subsets of Q such that

(1) For $1 \leqslant i \leqslant p$, $|S_i| = s$ and $|T_i| = t$.
(2) For $1 \leqslant i \leqslant p$, $S_i \cap T_i = \emptyset$.
(3) For $1 \leqslant j < i \leqslant p$, $S_j \cap T_i = \emptyset$.

Find the maximum value $p(s, t)$ of p.

We conjecture that $p(s, t) = \binom{s+t}{s} = \binom{s+t}{t}$. Note that if (3) is replaced by

(3′) For $1 \leqslant i \neq j \leqslant p$, $S_i \cap T_j = \emptyset$.

then the conjecture is true (see Berge [1, p. 406]).

We now state the promised connection between Problems P and P'.

Proposition 3.1 *Let $\mathcal{A} = (Q, A, \delta)$ be an automaton with n states, let $0 \leqslant s \leqslant n - 2$ and let K be an $(n - s)$-subset of Q. If there exists a word w such that $|Kw| < |K|$, one can choose w with length $\leqslant p(s, 2)$.*

Proof. Let $w = a_1 \cdots a_p$ be a shortest word such that $|Kw| < |K| = n - s$ and define $K_1 = K$, $K_2 = K_1 a_1$, ..., $K_p = K_{p-1} a_{p-1}$. Clearly, an equality of the form $|K_i| = |Ka_1 \cdots a_i| < |K|$ for some $i < p$ is inconsistent with the definition of w. Therefore $|K_1| = |K_2| = \cdots = |K_p| = (n - s)$. Moreover, since $|K_p a_p| < |K_p|$, K_p contains two elements x_p and y_p such that $x_p a_p = y_p a_p$.

Define 2-sets $T_i = \{x_i, y_i\} \subset K_i$ such that $x_i a_i = x_{i+1}$ and $y_i a_i = y_{i+1}$ for $1 \leqslant i \leqslant p - 1$ (the T_i are defined from $T_p = \{x_p, y_p\}$). Finally, set $S_i = Q \setminus K_i$. Thus we have

(1) For $1 \leqslant i \leqslant p$, $|S_i| = s$ and $|T_i| = 2$.

(2) For $1 \leqslant i \leqslant p$, $S_i \cap T_i = \emptyset$.

Finally assume that for some $1 \leqslant j < i \leqslant p$, $S_i \cap T_i = \emptyset$, i.e., $\{x_i, y_i\} \subset K_i$. Since

$$x_i a_i \cdots a_p = y_i a_i \cdots a_p,$$

it follows that

$$|Ka_1 \cdots a_{j-1} a_i \cdots a_p| = |K_j a_i \cdots a_p| < n - s$$

But the word $a_1 \cdots a_{j-1} a_i \cdots a_p$ is shorter that w, a contradiction.

Thus the condition (3), for $1 \leqslant j < i \leqslant p$, $S_j \cap T_i \neq \emptyset$, is satisfied, and this concludes the proof. □

I shall give two different upper bounds for $p(s) = p(2, s)$.

Proposition 3.2

(1) $p(0) = 1$,

(2) $p(1) = 3$,

(3) $p(s) \leqslant s^2 - s + 4$ *for* $s \geqslant 2$.

Proof. First note that the S_i's (T_i's) are all distinct, because if $S_i = S_j$ for some $j < i$, then $S_i \cap T_i = \emptyset$ and $S_i \cap T_j \neq \emptyset$, a contradiction.

Assertion (1) is clear.

To prove (2) assumet that $p(1) > 3$. Then, since $T_4 \cap S_1 \neq \emptyset$, $T_4 \cap S_2 \neq \emptyset$, $T_4 \cap S_3 \neq \emptyset$, two of the three 1-sets S_1, S_2, S_3 are equal, a contradiction.

On the other hand, the sequence $S_1 = \{x_1\}$, $S_2 = \{x_2\}$, $S_3 = \{x_3\}$, $T_1 = \{x_2, x_3\}$, $T_2 = \{x_1, x_3\}$, $T_3 = \{x_1, x_2\}$ satisfies the conditions of Problem P'. Thus $p(1) = 3$.

To prove (3) assume at first that $S_1 \cap S_2 = \emptyset$ and consider a 2-set T_i with $i \geqslant 4$. Such a set meets S_1, S_2 and S_3. Since S_1 and S_2 are disjoint sets, T_i is composed as follows:

- either an element of $S_1 \cap S_3$ with an element of $S_2 \cap S_3$,
- or an element of $S_1 \cap S_3$ with an element of $S_2 \setminus S_3$,
- or an element of $S_1 \setminus S_3$ with an element of $S_2 \cap S_3$.

Therefore

$$\begin{aligned} p(s) - 3 &\leqslant |S_1 \cap S_3||S_2 \cap S_3| + |S_1 \cap S_3||S_2 \setminus S_3| + |S_1 \setminus S_3||S_2 \cap S_3| \\ &= |S_1 \cap S_3||S_2| + |S_1||S_2 \cap S_3| - |S_1 \cap S_3||S_2 \cap S_3| \\ &= s(|S_1 \cap S_3| + |S_2 \cap S_3|) - |S_1 \cap S_3||S_2 \cap S_3| \end{aligned}$$

Since S_1, S_2, S_3 are all distinct, $|S_1 \cap S_3| \leqslant s - 1$. Thus if $|S_1 \cap S_3| = 0$ or $|S_2 \cap S_3| = 0$ it follows that

$$p(s) \leqslant s(s - 1) + 3 = s^2 - s + 3$$

If $|S_1 \cap S_3| \neq 0$ and $S_2 \cap S_3| \neq 0$, one has

$$|S_1 \cap S_3||S_2 \cap S_3| \geqslant |S_1 \cap S_3||S_2 \cap S_3| - 1,$$

and therefore:

$$p(s) \leqslant 3 + (s-1)(|S_1 \cap S_3| + |S_2 \cap S_3|) + 1 \leqslant s^2 - s + 4,$$

since $|S_1 \cap S_3| + |S_2 \cap S_3| \leqslant |S_3| = s$.

We now assume that $a = |S_1 \cap S_2| > 0$, and we need some lemmata.

Lemma 3.3 *Let x be an element of Q. Then x is contained in at most $(s+1)$ T_i's.*

Proof. If not there exist $(s+2)$ indices $i_1 < \ldots < i_{s+2}$ such that $T_{i_j} = \{x, x_{i_j}\}$ for $1 \leqslant j \leqslant s+2$. Since $S_{i_1} \cap T_{i_1} \neq \emptyset$, $x \notin S_{i_1}$. On the other hand, S_{i_1} meets all T_{i_j} for $2 \leqslant j \leqslant s+2$ and thus the s-set S_{i_1} has to contain the $s+1$ elements $x_{i_2}, \ldots, x_{i_{s+2}}$, a contradiction. □

Lemma 3.4 *Let R be an r-subset of Q. Then R meets at most $(rs+1)$ T_i's.*

Proof. The case $r = 1$ follows from Lemma 3.3. Assume $r \geqslant 2$ and let x be an element of R contained in a maximal number N_x of T_i's. Note that $N_x \leqslant s+1$ by Lemma 3.3. If $N_x \leqslant s$ for all $x \in R$, then R meets at most rs T_i's. Assume there exists an $x \in R$ such that $N_x = s+1$. Then x meets $(s+1)$ T_i's, say $T_{i_1} = \{x, x_{i_1}\}$, ..., $T_{i_{s+1}} = \{x, x_{i_{s+1}}\}$ with $i_1 < \ldots < i_{s+1}$.

We claim that every $y \neq x$ meets at most s T_i's such that $i \neq i_1, \ldots, i_{s+1}$. If not, there exist $s+1$ sets $T_{j_1} = \{y, y_{j_1}\}$, ..., $T_{j_{s+1}} = \{y, y_{j_{s+1}}\}$ with $j_1 < \ldots < j_{s+1}$ containing y. Assume $i_1 < j_1$ (a dual argument works if $j_1 < i_1$). Since $S_{i_1} \cap T_{i_1} = \emptyset$, $x \notin T_{i_1}$ and since S_{i_1} meets all other T_{i_k}, $S_{i_1} = \{x_{i_2}, \ldots, x_{i_{s+1}}\}$. If $y \in T_{i_1}$, y belongs to $(s+2)$ T_i's in contradiction to Lemma 3.3. Thus $|S_{i_1}| > s$, a contradiction. This proves the claim and the lemma follows easily. □

We can now conclude the proof of (3) in the case $|S_1 \cap S_2| = a > 0$. Consider a 2-set T_i with $i \geqslant 3$. Since T_i meets S_1 and S_2, either T_i meets $S_1 \cap S_2$, or T_i meets $S_1 \setminus S_2$ and $S_2 \setminus S_1$. By Lemma 3.4, there are at most $(as+1)$ T_i's of the first type and at most $(s-a)^2$ T_i's of the second type. It follows that

$$p(s) - 2 \leqslant (s-a)^2 + as + 1$$

and hence $p(s) \leqslant s^2 + a^2 - as + 3 \leqslant s^2 - s + 4$, since $1 \leqslant a \leqslant s-1$. □

Two different upper bounds were promised for $p(s)$. Here is the second one, which seems to be rather unsatisfying, since it depends on $n = |Q|$. In fact, as will be shown later, this new bound is better than the first one for $s > \lfloor n/2 \rfloor$.

Proposition 3.5 *Let $a = \lfloor n/(n-s) \rfloor$. Then*

$$p(s) \leqslant \frac{1}{2}ns + a = \binom{a+1}{2}s^2 + (1-a^2)ns + \binom{a}{2}n^2 + a$$

if $n - s$ divides n, and

$$p(s) \leqslant \binom{a+1}{2}s^2 + (1-a^2)ns + \binom{a}{2}n^2 + a + 1$$

if $n - s$ does not divide n.

Proof. Denote by N_i the number of 2-sets meeting S_j for $j < i$ but not meeting S_i. Note that the conditions of Problem P' just say that $N_i > 0$ for all $i \leqslant p(s)$. The idea of the proof is contained in the following formula

$$\sum_{1 \leqslant i \leqslant p(s)} N_i \leqslant \binom{n}{2} \tag{1}$$

This is clear since the number of 2-subsets of Q is $\binom{n}{2}$. The next lemma provides a lower bound for N_i.

Lemma 3.6 *Let* $Z_i = \bigcap_{j<i} S_j \setminus S_i$ *and* $|Z_i| = z_i$. *Then* $N_i \geqslant \binom{z_i}{2} + z_i(n - s - z_i)$.

Proof. Indeed, any 2-set contained in Z_i and any 2-set consisting of an element of Z_i and of an element of $Q \setminus (S_i \cup Z_i)$ meets all S_j for $j < i$ but does not meet S_i.

We now prove the proposition. First of all we claim that

$$\bigcup_{1 \leqslant i \leqslant p(s)} Z_i = Q$$

If not,

$$Q \setminus (\cup Z_i) = \bigcap_{1 \leqslant i \leqslant s(p)} S_i$$

is nonempty, and one can select an element x in this set. Let T be a 2-set containing x and S be an s-set such that $S \cap T = \emptyset$. Then the two sequences $S_1, \dots, S_{p(s)}, S$ and $T_1, \dots, T_{p(s)}, T$ satisfy the conditions of Problem P' in contradiction to the definition of $p(s)$. Thus the claim holds and since all Z_i's are pairwise disjoint:

$$\sum z_i = n \tag{2}$$

It now follows from (1) that

$$p(s) \leqslant \binom{n}{2} - \sum_{1 \leqslant i \leqslant p(s)} (N_i - 1) \tag{3}$$

Since $N_i > 0$ for all i, Lemma 3.6 provides the following inequality:

$$p(s) \leqslant \binom{n}{2} - \sum_{z_i > 0} f(z_i) \tag{4}$$

where $f(z) = \binom{z}{2} + z(n - s - z) - 1$.

Thus, it remains to find the minimum of the expression $\sum f(z_i)$ when the z_i's are submitted to the two conditions

(a) $\sum z_i = n$ (see (2)) and

(b) $0 < z_i \leqslant n - s$ (because $Z_i \subset Q \setminus S_i$).

Consider a family (z_i) reaching this minimum and which furthermore contains a minimal number α of z_i's different from $(n - s)$.

We claim that $\alpha \leqslant 1$. Assume to the contrary that there exist two elements different from $n - s$, say z_1 and z_2. Then an easy calculation shows that

$$\begin{aligned} &f(z_1 + z_2) \leqslant f(z_1) + f(z_2) && \text{if } z_1 + z_2 \leqslant n - s, \\ &f(n - s) + f(z_1 + z_2 - (n - s)) \leqslant f(z_1) + f(z_2) && \text{if } z_1 + z_2 > n - s. \end{aligned}$$

Thus replacing z_1 and z_2 by $z_1 + z_2$ — in the case $z_1 + z_2 \leqslant n - s$ — or by $(n - s)$ and $z_1 + z_2 - (n - s)$ — in the case $z_1 + z_2 > n - s$ — leads to a family (z'_i) such that $\sum f(z'_i) \leqslant \sum f(z_i)$ and containing at most $(\alpha - 1)$ elements z'_i different from $n - s$, in contradiction to the definition of the family (z_i). Therefore $\alpha = 1$ and the minimum of $f(z_i)$ is obtained for

$$z_1 = \cdots = z_\alpha = n - s \qquad \text{if } n = a(n-s),$$

and for

$$z_1 = \cdots = z_\alpha = n - s,\ z_{\alpha+1} = r \qquad \text{if } n = a(n-s) + r \text{ with } 0 < r < n - s.$$

It follows from inequality (4) that

$$p(s) \leqslant \binom{n}{2} - af(n-s) \qquad \text{if } n = a(n-s),$$
$$p(s) \leqslant \binom{n}{2} - af(n-s) - f(r) \qquad \text{if } n = a(n-s) + r \text{ with } 0 < r < n - s.$$

where $f(z) = \binom{n}{2} + z(n-z) - 1$.

Proposition 3.5 follows by a routine calculation. □

We now compare the two upper bound for $p(s)$ obtained in Propositions 3.2 and 3.5 for $2 \leqslant s \leqslant n-2$.

Case 1. $2 \leqslant s \leqslant (n/2) - 1$.

Then $a = 1$ and Proposition 3.5 gives $p(s) \leqslant s^2 + 2$. Clearly $s^2 - s + 4$ is a better upper bound.

Case 2. $s = n/2$.

Then $a = 2$ and Proposition 3.5 gives $p(s) \leqslant s^2 + 2$. Again $s^2 - s + 4$ is better.

Case 3. $(n+1)/2 \leqslant s \leqslant (2n-1)/3$.

Then $a = 2$ and Proposition 3.5 gives

$$\begin{aligned} p(s) &\leqslant 3s^2 - 3ns + n^2 + 3 = s^2 - s + 4 + (n-s-1)(n-2s+1) \\ &\leqslant s^2 - s + 4 \end{aligned}$$

Case 4. $2n/3 \leqslant s$.

Then $a \geqslant 3$ and Proposition 3.5 gives

$$\begin{aligned} p(s) &\leqslant \binom{a+1}{2} s^2 + (1-a^2)ns + \binom{a}{2} n^2 + a + 1 \\ &\leqslant s^2 - s + \frac{1}{2}a(a-1)(n-s)^2 - ((a-1)(n-s)-1)s + a + 1 \end{aligned}$$

Since $s \leqslant (1-a)(n-s)$, a short calculation shows that

$$p(s) \leqslant s^2 - s + 4 - \frac{1}{2}(a-1)(a-2)(n-s)^2 + (a-1)(n-s) + (a-3)$$

Since $a \geqslant 3$, $-\frac{1}{2}(a-1) \leqslant -1$ and thus

$$p(s) \leqslant s^2 - s + 4 - (a-2)(n-s)^2 + (a-1)(n-s) + (a-3),$$

and it is not difficult to see that for $n - s \geqslant 2$,

$$-(a-2)(n-s)^2 + (a-1)(n-s) + (a-3) \leqslant 0$$

Therefore Proposition 3.5 gives a better bound in this case.

The next theorem summarizes the previous results.

Theorem 3.7 *Let $\mathcal{A} = (Q, A, \delta)$ be an automaton with n states, let $0 \leqslant s \leqslant n-2$ and let K be an $(n-s)$-subset of Q. If there exists a word w such that $|Kw| < |K|$, one can choose w with length $\leqslant \varphi(n, s)$ where $a = \lfloor n/(n-s) \rfloor$ and*

$$\varphi(n,s) = \begin{cases} 1 & \textit{if } s = 0, \\ 3 & \textit{if } s = 3, \\ s^2 - s + 4 & \textit{if } 3 \leqslant s \leqslant n/2, \end{cases}$$

$$\varphi(n,s) = \binom{a+1}{2} s^2 + (1 - a^2)ns + \binom{a}{2} n^2 + a = \frac{1}{2}ns + a$$

$$\textit{if } n = a(n-s) \textit{ and } s > n/2,$$

$$\varphi(n,s) = \binom{a+1}{2} s^2 + (1 - a^2)ns + \binom{a}{2} n^2 + a + 1$$

$$\textit{if } n-s \textit{ does not divide } n \textit{ and } s > n/2.$$

We can now prove the main results of this paper.

Theorem 3.8 *Let $\mathcal{A}$ be an automaton with n states and let $0 \leqslant k \leqslant n-1$. If there exists a word of rank $\leqslant n-k$ in $\mathcal{A}$, there exists such a word of length $\leqslant G(n,k)$ where*

$$G(n,k) = \begin{cases} k^2 & \textit{for } k = 0, 1, 2, 3, \\ \frac{1}{3}k^3 - k^2 + \frac{14}{3}k - 5 & \textit{for } 4 \leqslant k \leqslant (n-2) + 1, \\ 9 + \sum_{3 \leqslant s \leqslant k-1} \varphi(n,s) & \textit{for } k \geqslant (n+3)/2. \end{cases}$$

Observe that in any case

$$G(n,k) \leqslant \frac{1}{3}k^3 - k^2 + \frac{14}{3}k - 5$$

Table 1 gives values of $G(n,k)$ for $0 \leqslant k \leqslant n \leqslant 12$.

$k \backslash n$	1	2	3	4	5	6	7	8	9	10	11	12
1	0	1	4	9	19	34	56	85	125	173	235	310
2		0	1	4	9	19	35	57	89	128	180	244
3			0	1	4	9	19	35	59	90	133	186
4				0	1	4	9	19	35	59	93	135
5					0	1	4	9	19	35	59	93
6						0	1	4	9	19	35	59
7							0	1	4	9	19	35
8								0	1	4	9	19
9									0	1	4	9
10										0	1	4
11											0	1
12												0

Figure 1: Values of $G(n,k)$ for $0 \leqslant k \leqslant n \leqslant 12$.

Proof. Assume that there exists a word w of rank $\leqslant n-k$ in $\mathcal{A}$. Since Conjecture (C) has been proved for $k \leqslant 3$, we may assume $k \geqslant 4$ and there exists a word w_1 of length $\leqslant 9$ such that $Qw_1 = K_1$ satisfies $|K_1| \leqslant n-3$. It suffices now to apply the method decribed at the beginning of this section which consists of using Theorem 3.7 repetitively. This method shows that one can find a word of rank $\leqslant n-k$ in $\mathcal{A}$ of length

$\leqslant 9 + \sum_{3 \leqslant s \leqslant k-1} \varphi(n,s) = G(n,k)$. In particular, $\varphi(n,s) = s^2 - s + 4$ for $s \leqslant n/2$ and thus

$$G(n,k) = \frac{1}{3}k^3 - k^2 + \frac{14}{3}k - 5 \quad \text{for } 4 \leqslant k \leqslant (n-2)+1$$

It is interesting to have an estimate of $G(n,k)$ for $k = n-1$.

Theorem 3.9 *Let $\mathcal{A}$ be an automaton with n states. If there exists a word of rank* 1 *in $\mathcal{A}$, there exists such a word of length $\leqslant F(n)$ where*

$$F(n) = (\frac{1}{2} - \frac{\pi^2}{36})n^3 + o(n^3).$$

Note that this bound is better than the bound in $\frac{7}{27}n^3$, since $7/27 \simeq 0.2593$ and $(\frac{1}{2} - \frac{\pi^2}{36}) \simeq 0.2258$.

Proof. Let $h(n,s) = \binom{a+1}{2}s^2 + (1-a^2)ns + \binom{a}{2}n^2 + a + \varepsilon(s)$, where

$$\varepsilon(s) = \begin{cases} 0 & \text{if } n = a(n-s) \\ 1 & \text{if } n-s \text{ does not divide } n. \end{cases}$$

The above calculations have shown that for $3 \leqslant s \leqslant n/2$,

$$s^2 - s + 4 \leqslant h(n,s) \leqslant s^2 + 2.$$

Therefore

$$\sum_{0 \leqslant s \leqslant n/2} \varphi(n,s) \sim 9 + \sum_{3 \leqslant s \leqslant n-2} s^2 \sim \frac{1}{24}n^3 \sim \sum_{0 \leqslant s \leqslant n/2} h(n,s)$$

It follows that

$$\begin{aligned} F(n) = G(n,n-1) &= \sum_{0 \leqslant s \leqslant n-2} h(n,s) + o(n^3) \\ &= \sum_{0 \leqslant s \leqslant n-1} h(n,s) + o(n^3) \end{aligned}$$

A new calculation shows that

$$h(n,n-s) = n^2 + (\lfloor n/s \rfloor + 1)(\frac{1}{2}\lfloor n/s \rfloor s^2 - sn + 1) - \varepsilon(n-s)$$

Therefore

$$F(n) = \sum_{1 \leqslant i \leqslant 6} T_i(n) + o(n^3)$$

where

$$T_1 = \sum_{s=1}^{n} n^2 = n^3, \qquad T_4 = -n\sum_{s=1}^{n} \lfloor n/s \rfloor s$$

$$T_1 = \frac{1}{2}\sum_{s=1}^{n} \lfloor n/s \rfloor^2 s^2, \qquad T_5 = -n\sum_{s=1}^{n} s,$$

$$T_3 = \frac{1}{2}\sum_{s=1}^{n} \lfloor n/s \rfloor s, \qquad T_6 = \sum_{s=1}^{n} \lfloor n/s \rfloor s + 1 - \varepsilon(n-s).$$

Clearly $T_5 = -\frac{1}{2}n^3 + o(n^3)$ and $T_6 = o(n^3)$. The terms T_2, T_3 and T_4 need a separate study.

Lemma 3.10 *We have* $T_3 = \frac{1}{6}\zeta(3)n^3 + o(n^3)$ *and* $T_4 = -\frac{1}{2}\zeta(2)n^3 + o(n^3)$, *where* $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ *is the usual zeta-function.*

These two results are easy consequences of classical results of number theory (see [7, p. 117, Theorem 6.29 and p. 121, Theorem 6.34])

$$\text{(a)} \quad \sum_{s=1}^{n} \lfloor n/s \rfloor s = \sum_{s=1}^{n} \sum_{d=1}^{\lfloor n/s \rfloor} s = \frac{1}{2} \sum_{s=1}^{n} (\lfloor n/s \rfloor^2 + \lfloor n/s \rfloor)$$
$$= \frac{1}{2} n^2 \sum_{k=1}^{n} \frac{1}{k^2} + o(n^2) = \frac{1}{2}\zeta(2)n^2 + o(n^2)$$

Therefore $T_4 = -\frac{1}{2}\zeta(2)n^3 + o(n^3)$.

$$\text{(b)} \quad \sum_{s=1}^{n} \lfloor n/s \rfloor s^2 = \sum_{s=1}^{n} \sum_{d=1}^{\lfloor n/s \rfloor} s^2 = \frac{1}{2} \sum_{s=1}^{n} (2\lfloor n/s \rfloor^3 + 3\lfloor n/s \rfloor^2 + \lfloor n/s \rfloor)$$
$$= \frac{1}{3} n^3 \left(\sum_{k=1}^{n} \frac{1}{s^3} \right) + o(n^3) = \frac{1}{3}\zeta(3)^3 + o(n^3)$$

Therefore $T_3 = \frac{1}{6}\zeta(3)n^3 + o(n^3)$.

Lemma 3.11 *We have* $T_2 = \frac{1}{6}(2\zeta(2) - \zeta(3))n^3 + o(n^3)$.

Proof. It is sufficient to prove that

$$\lim_{n\to\infty} \frac{1}{n^3} \sum_{s=1}^{n} \lfloor n/s \rfloor^2 s^2 = \frac{1}{6}(2\zeta(2) - \zeta(3))$$

Fix an integer n_0. Then

$$\frac{1}{n^3} \sum_{j=1}^{n_0} j^2 \sum_{s=\lfloor n/(j+1) \rfloor + 1}^{\lfloor n/j \rfloor} s^2 \leqslant \frac{1}{n^3} \sum_{s=1}^{n} \lfloor n/s \rfloor^2 s^2$$
$$\leqslant \frac{1}{n} \left\lfloor \frac{n}{n_0 + 1} \right\rfloor + \frac{1}{n^3} \sum_{j=1}^{n_0} j^2 \sum_{s=\lfloor n/(j+1) \rfloor + 1}^{\lfloor n/j \rfloor} s^2$$

Indeed, $\lfloor n/s \rfloor s \leqslant n$ implies the inequality

$$\frac{1}{n^3} \sum_{s=1}^{\lfloor n/(n_0+1) \rfloor} \left\lfloor \frac{n}{s} \right\rfloor^2 s^2 \leqslant \frac{1}{n} \left\lfloor \frac{n}{n_0 + 1} \right\rfloor$$

Now

$$\lim_{n\to\infty} \frac{1}{n^3} \sum_{\lfloor n/(j+1) \rfloor + 1 \leqslant s \leqslant \lfloor n/j \rfloor} s^2 = \frac{1}{3} \left(\frac{1}{j^3} - \frac{1}{(j+1)^3} \right)$$

It follows that for all $n_0 \in \mathbb{N}$

$$\begin{aligned}\frac{1}{2}\sum_{j=1}^{n_0} j^2\left(\frac{1}{j^3}-\frac{1}{(j+1)^3}\right) &\leqslant \liminf_{n\to\infty}\frac{1}{n^3}\sum\left\lfloor\frac{n}{k}\right\rfloor^2 k^2\\ &\leqslant \limsup_{n\to\infty}\frac{1}{n^3}\sum\left\lfloor\frac{n}{k}\right\rfloor^2 k^2\\ &\leqslant \limsup_{n\to\infty}\frac{1}{n}\left\lfloor\frac{n}{n_0+1}\right\rfloor+\frac{1}{3}\sum_{j=1}^{n_0} j^2\left(\frac{1}{j^3}-\frac{1}{(j+1)^3}\right)\end{aligned}$$

Since

$$\limsup_{n\to\infty}\frac{1}{n}\left\lfloor\frac{n}{n_0+1}\right\rfloor=\frac{1}{n_0+1}$$

We obtain for $n_0 \to \infty$,

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{n^3}\sum_{s=1}^{n}\left\lfloor\frac{n}{s}\right\rfloor^2 s^2 &= \frac{1}{3}\sum_{j=1}^{\infty} j^2\left(\frac{1}{j^3}-\frac{1}{(j+1)^3}\right)\\ &= \frac{1}{3}\sum_{j=1}^{\infty}\frac{2j-1}{j^3}=\frac{1}{3}(2\zeta(2)-\zeta(3))\end{aligned}$$

Finally we have

$$\begin{aligned}F(n) &= n^3\left(1+\frac{1}{6}\left(2\zeta(2)-\zeta(3)\right)+\frac{1}{6}\zeta(3)-\frac{1}{2}\zeta(2)-\frac{1}{2}\right)+o(n^3)\\ &= \left(\frac{1}{2}-\frac{1}{6}\zeta(2)\right)n^3+o(n^3)\\ &= \left(\frac{1}{2}-\frac{\pi^2}{36}\right)n^3+o(n^3)\end{aligned}$$

which concludes the proof of Theorem 3.9. □

Note added in proof

(1) P. Shor has recently found a counterexample to the triangle conjecture.
(2) Problem P' has been solved by P. Frankl. The conjectured estimate $p(s,t)=\binom{s+t}{s}$ is correct. It follows that Theorem 3.8 can be sharpened as follows: if there exists a word of rank $\leqslant n-k$ in $\mathcal{A}$ there exists such a word of length $\leqslant \frac{1}{6}k(k+1)(k+2)-1$ (for $3 \leqslant k \leqslant n-1$).

References

[1] C. Berge, *Graphes et hypergraphes*, Dunod, Paris, 1973. Deuxième édition, Collection Dunod Université, Série Violette, No. 604.

[2] J. Černý, Poznámka k. homogénnym experimentom s konecnými automatmi, *Mat. fyz. čas SAV* **14** (1964), 208–215.

[3] J. Černý, Communication, in *Bratislava Conference on Cybernetics*, 1969.

[4] J. Černý, A. Pirická and B. Rosenauerova, On directable automata, *Kybernetica* **7** (1971), 289–298.

[5] G. Hansel, Baionnettes et cardinaux, *Discrete Math.* **39**,3 (1982), 331–335.

[6] Z. Kohavi, *Switching and finite automata theory*, McGraw Hill, New-York, 1970.

[7] W. J. LeVeque, *Topics in number theory. Vols. 1 and 2*, Addison-Wesley Publishing Co., Inc., Reading, Mass., 1956.

[8] M. Lothaire, *Combinatorics on Words*, *Encyclopedia of Mathematics and its Applications* vol. 17, Cambridge University Press, 1983.

[9] D. Perrin and M.-P. Schützenberger, A conjecture on sets of differences of integer pairs, *J. Combin. Theory Ser. B* **30**,1 (1981), 91–93.

[10] J.-E. Pin, *Le problème de la synchronisation. Contribution à l'étude de la conjecture de Černý*, Thèse de 3ème cycle, Université Paris VI, 1978.

[11] J.-E. Pin, Sur les mots synchronisants dans un automate fini, *Elektron. Informationsverarb. Kybernet.* **14** (1978), 293–303.

[12] J.-E. Pin, Sur un cas particulier de la conjecture de Černý, in *5th ICALP*, Berlin, 1978, pp. 345–352, *LNCS* n° 62, Springer.

[13] J.-E. Pin, Utilisation de l'algèbre linéaire en théorie des automates, in *Actes du 1er Colloque AFCET-SMF de Mathématiques Appliquées*, pp. 85–92, AFCET, 1978.

[14] J.-E. Pin, Le problème de la synchronisation et la conjecture de Černý, in *Noncommutative structures in algebra and geometric combinatorics*, A. De luca (ed.), pp. 37–48, *Quaderni de la Ricerca Scientifica* vol. 109, CNR, Roma, 1981.

[15] J.-E. Pin and I. Simon, A note on the triangle conjecture, *J. Combin. Theory Ser. A* **32**,1 (1982), 106–109.

[16] P. H. Starke, Eine Bemerkung über homogene Experimente., *Elektr. Informationverarbeitung und Kyb.* **2** (1966), 257–259.

[17] P. H. Starke, *Abstrakte Automaten*, V.E.B. Deutscher Verlag der Wissenschaften, Berlin, 1969.