Words guaranteeing minimal image

S.W. Margolis J.-E. Pin M.V. Volkov*

Abstract

Given a positive integer n and a finite alphabet A, a word w over A is said to *guarantee minimal image* if, for every homomorphism φ from the free monoid A^* over A into the monoid of all transformations of an n-element set, the range of the transformation $w\varphi$ has the minimum cardinality among the ranges of all transformations of the form $v\varphi$ where v runs over A^*. Although the existence of words guaranteeing minimal image is pretty obvious, the problem of their explicit description is very far from being trivial. Sauer and Stone in 1991 gave a recursive construction for such a word w but the length of the word resulting from that construction was doubly exponential (as a function of n). We first show that some known results of automata theory immediately lead to an alternative construction which yields a simpler word that guarantees minimal image: it has exponential length, more precisely, its length is $O(|A|^{\frac{1}{6}(n^3-n)})$. Then using a different approach, we find a word guaranteeing minimal image similar to that of Sauer and Stone but of the length $O(|A|^{\frac{1}{2}(n^2-n)})$. On the other hand, we observe that the length of any word guaranteeing minimal image cannot be less than $|A|^{n-1}$.

Let X be a non-empty set. A *transformation* of the set X is an arbitrary function f whose domain is X and whose range (denoted by $\mathsf{Im}(f)$) is a non-empty subset of X. The *rank* $\mathsf{rk}(f)$ of the function f is the cardinality of the set $\mathsf{Im}(f)$. Transformations of X form a monoid under the usual composition of functions; the monoid is called *the full transformation monoid over* X and

*This work was initiated when the third-named author was visiting Bar-Ilan University (Ramat Gan, Israel) with the support of Department of Mathematics and Computer Science, Bar-Ilan University, of Russian Education Ministry (through its Grant Center at St Petersburg State University, grant E00-1.0-92) and of Russian Basic Research Foundation. The work was also partially supported by the INTAS through the Network project 99-1224 "Combinatorial and Geometric Theory of Groups and Semigroups and its Applications to Computer Science", by the Emmy Noether Research Institute for Mathematics and the Minerva Foundation of Germany, by the Excellency Center "Group Theoretic Methods in the study of Algebraic Varieties" of the Israel Science foundation, and by the NSF.

is denoted by $T(X)$. If the set X is finite with n elements, the monoid $T(X)$ is also denoted by T_n.

Now let A be a finite set called an *alphabet*. The elements of A are called *letters*, and strings of letters are called *words over* A. The number of letters forming a word v is called the *length* of v and is denoted by $\ell(v)$. Words over A (including the empty word) form a monoid under the concatenation operation; the monoid is called *the free monoid over the alphabet* A and is denoted by A^*.

Both words over a finite alphabet and transformations of a finite set are classical objects of combinatorics. On the other hand, their interaction is essentially the main subject of the theory of finite automata. One of the aims of the present paper is to demonstrate how certain quite well known facts about finite automata may be utilized to improve some recent combinatorial results concerned with words and transformations. Vice versa, we shall also apply certain purely combinatorial considerations to some questions which, as we intend to show, are rather natural from the automata viewpoint.

The combinatorial results we have in sight group around the notion of a *word guaranteeing minimal image* introduced by Sauer and Stone in [21]. To describe it, let us first fix a positive integer n (the size of the domain X of our transformations) and a finite alphabet A. Now suppose we have a mapping $\varphi : A \to T_n$. It extends in a unique way to a homomorphism of the free monoid A^* into T_n; we will denote the homomorphism by φ as well. Now, with each word $v \in A^*$, we associate the transformation $v\varphi$. A word $w \in A^*$ is said to *guarantee minimal image* if the inequality

$$\mathsf{rk}(w\varphi) \leq \mathsf{rk}(v\varphi) \tag{1}$$

holds **for every word** $v \in A^*$ and **for every mapping** $\varphi : A \to T_n$.

Clearly, words guaranteeing minimal image exist [20, Proposition 2.3]. Indeed, for each mapping $\varphi : A \to T_n$, there is a word w_φ such that

$$\mathsf{rk}(w_\varphi\varphi) \leq \mathsf{rk}(v\varphi) \tag{2}$$

for all $v \in A^*$. Since there are only finitely many mappings between the finite sets A and T_n and since the composition of transformations cannot increase the size of its image, we can concatenate all words w_φ getting an (apparently very long) word w satisfying (1).

Words guaranteeing minimal image have been proved to have some interesting algebraic applications. In [20] they were used to find identities in the full transformation monoids. Recently these words have been applied for studying the structure of the free profinite semigroup, see [2]. Of course, for application purposes, the pure existence statement is not sufficient, and one seeks an explicit construction.

The only construction of words guaranteeing minimal image known so far was due to Sauer and Stone [21, Corollary 3.5]. The construction makes an elegant use of recursion but results in very long words such that, even over a two-element alphabet, it is hardly possible to write down the Sauer–Stone word that guarantees minimal image, say, in T_5.

To build a word guaranteeing minimal image in T_n, Sauer and Stone make use of an intermediate notion which is also of independent interest. Given a transformation f of a finite set X, we denote by $\mathsf{df}(f)$ its *deficiency*, that is, the difference $|X| - \mathsf{rk}(f)$. For a homomorphism $\varphi : A^* \to T(X)$, we denote by $\mathsf{df}(\varphi)$ the maximum of the deficiencies $\mathsf{df}(v\varphi)$ where v runs over A^*; in other words, $\mathsf{df}(\varphi) = \mathsf{df}(w_\varphi\varphi)$ where w_φ is any word satisfying (2). Now we say that a word $w \in A^*$ *witnesses for deficiency* k (*has property* Δ_k in Sauer and Stone's terminology), provided that, **for all homomorphisms** $\varphi : A^* \to T(X)$ where X is a finite set, $\mathsf{df}(w\varphi) \geq k$ whenever $\mathsf{df}(\varphi) \geq k$. The following easy observation explains how the two properties under consideration relate:

Lemma 1. *If a word w witnesses for deficiency k for all $0 \leq k < n$, then it guarantees minimal image in T_n.*

Proof. Take an arbitrary homomorphism $\varphi : A^* \to T_n$ and apply it to an arbitrary word $v \in A^*$ thus obtaining a transformation $v\varphi \in T_n$. Suppose that $\mathsf{rk}(v\varphi) = r$. Then $1 \leq r \leq n$ and

$$\mathsf{df}(\varphi) \geq \mathsf{df}(v\varphi) = n - r$$

whence $\mathsf{df}(w\varphi) \geq n - r$ as w witnesses for deficiency $n - r$. Therefore

$$\mathsf{rk}(w\varphi) = n - \mathsf{df}(w\varphi) \leq n - (n - r) = r = \mathsf{rk}(v\varphi),$$

as the definition of a word guaranteeing minimal image requires. □

Since the cardinality of the set X is **not** fixed in the definition of a word which witnesses for deficiency k, it is not obvious that such a word should exist for every k. However, it is clear that if $A = \{a_1, \ldots, a_t\}$, then the product $w_1 = a_1 \cdots a_t$ witnesses for deficiency 1. (Indeed, if $\mathsf{df}(\varphi) \geq 1$, then at least one of the letters $a_1, \ldots, a_t$ should be evaluated at a transformation which is not a permutation whence $w_1\varphi$ is not a permutation as well). Using this observation as the induction basis, Sauer and Stone then proceed by defining

$$w_{k+1} = w_k \prod_{v \in Q_k} (vw_k) \tag{3}$$

where Q_k denotes the set of all words v over A such that $\ell(v) \leq 1 + \frac{3}{4}2^k$. Their main results say that, for each k, the word w_k witnesses for deficiency

k [21, Theorem 3.3] and, given any $n > 1$, the word w_{n-1} guarantees minimal image in T_n [21, Corollary 3.5].

Using (3), it is rather easy to see that the growth of $\ell(w_k)$ as a function of k is double exponential; more precisely, it can be calculated that the leading monomial in the expansion of $\ell(w_k)$ as a polynomial of t (the size of the alphabet) equals $t^{3\cdot 2^{k-2}+k-2}$ for all $k \geq 2$. The reader may verify that applying that construction to produce a word over a 2-letter alphabet guaranteeing minimal image in T_5 results in a word of length 216 248; thus, we were not exaggerating as we said that it would be rather hard to write down this word! Sauer and Stone formulate in [21] the following open problem: for a given alphabet with t letters, determine for each positive integer k the length $\mu_k(t)$ of the shortest word that witnesses for deficiency k. Obviously $\mu_1(t) = t$ for any t; besides that, the only value of the function $\mu_k(t)$ known so far is $\mu_2(2) = 8$ — it is shown in [21, Corollary 3.4] that the word aba^2b^2ab witnesses for deficiency 2, and it can be checked that no shorter word does the job. We notice that the word over $\{a, b\}$ with the same property obtained via (3) is much longer — its length is 24. This gap is large enough to suggest that there should be more economic constructions than (3). We are going to present two approaches to such constructions.

Our first approach is based on certain developments in finite automata theory which arose from numerous attempts to resolve a (still open) problem by Černý [4] on synchronizing automata. A *finite automaton* $\mathcal{A}$ may be thought of as a triple (X, A, φ) where X is a finite set (called *the state set of* $\mathcal{A}$), A is another finite set (called *the alphabet of* $\mathcal{A}$), and φ is a mapping which assigns a transformation of the set X to each letter $a \in A$. As above, φ extends to a homomorphism of the free monoid A^* into $T(X)$ so one may speak about words over A acting on the state set X via φ. With this convention, a *synchronizing* automaton is one such that there exists a word $w \in A^*$ whose action resets the automaton, that is, brings all its states to a particular one: $x(w\varphi) = x'(w\varphi)$ for all $x, x' \in X$. Any word w with this property is said to be a *reset* word for the automaton. It is rather natural to ask how long such a word may be. We refer to the question of determining the length of the shortest reset word as to the *Černý problem.* Černý conjectured in [4]—that is, almost 40 years ago—that for any synchronizing automaton with n states there exists a reset word of length $(n-1)^2$. Although being confirmed in some special cases (cf. [5, 16, 9, 8, 11, 14], to mention a few most representative papers only), this conjecture still constitutes an open problem.

The second-named author has extended Černý's problem in the following way (see [17, 18]). Suppose that in the automaton $\mathcal{A} = (X, A, \varphi)$, the deficiency of φ is no less than k, where $1 \leq k < |X|$. Then the problem (which we shall refer to as *the generalized Černý problem*) is to determine the length of the shortest word $w \in A^*$ verifying $\mathsf{df}(w\varphi) \geq k$. Clearly, the initial Černý problem corresponds to the case $k = |X| - 1$. (The second-named author also generalized the Černý conjecture in the following natural way: if $\mathsf{df}(\varphi) \geq k$, then there exists a word $w \in A^+$ of length k^2 for which $\mathsf{df}(w\varphi) \geq k$. In [17, 18] he proved this generalized conjecture for $k \leq 3$, but recently J. Kari [13] exhibited a counter example in the case $k = 4$.)

A comparison between the generalized Černý problem and the aforementioned problem of determining the shortest word witnessing for deficiency k immediately reveals an obvious similarity in them. In fact, the only difference between the two situations in question is that in the former case we look for the shortest rank-decreasing word for a given homomorphism of deficiency $\geq k$ while in the latter case we are interested in a word with the same properties but with respect to an arbitrary homomorphism of deficiency $\geq k$. In the language of automata theory, we may alternatively describe this difference by saying that in the second situation we also look for the shortest word decreasing rank by k for an automaton, but in contrast with the generalized Černý problem situation, the automaton is a black-box about which we only know that it admits a word of deficiency k. If thinking of a real computational device as a composite made from many finite automata, each a with relatively small number of states, a reasonable construction for an input signal which would simultaneously reset all those automata and which could be generated without analyzing the structure of each particular component of the device might be of some practical interest.

As far as theoretical aspects are concerned, the connection just discussed leads to the following conclusion:

Theorem 2. *For each $k \geq 3$ and for each finite alphabet A, there exists a word of length $|A|^{\frac{1}{6}k(k+1)(k+2)-1} + \frac{1}{6}k(k+1)(k+2) - 2$ over A that witnesses for deficiency k.*

Proof. We utilize a result by the second-named author [19]. This result which is based on a combinatorial theorem by Frankl [10] yields the best approximation to the size of the shortest reset word known so far:

Proposition 3. *Suppose that the automaton (X, A, φ) is such that the deficiency of the mapping φ is no less than k, where $3 \leq k < |X|$. Then there exists a word $w \in A^*$ of length $\frac{1}{6}k(k+1)(k+2) - 1$ verifying $\mathsf{df}(w\varphi) \geq k$.* $\square$

For brevity, let $m = \frac{1}{6}k(k+1)(k+2) - 1$. By a well known result of DeBruijn [7], there is a cyclic sequence over A, of length $|A|^m$, such that each word over A of length m appears as a factor of the sequence. Cut this cycle in an arbitrary place and make it a word u of the same length $|A|^m$. Since our cut goes through exactly $m-1$ factors of length m, the word u still contains all but $m-1$ words of length m as factors. Now let v be the prefix of u of length $m-1$ and let $w = uv$. Note that the word w has length $|A|^m + m - 1$. Clearly, this procedure restores all those factors of length m that we destroyed by cutting the initial DeBruijn sequence, and therefore each word over A of length m appears as a factor in w. We note that there is an efficient procedure that, given A and m, builds DeBruijn's sequences so, if necessary, the word w may be explicitly written.

By Proposition 3, for any finite set X and for any homomorphism $\varphi : A^* \to T(X)$ with $\mathsf{df}(\varphi) \geq k$, there exists a word $w_\varphi \in A^*$ of length m such that $\mathsf{df}(w_\varphi \varphi) \geq k$. By the above construction of the word w, the word w_φ must appear as a factor in w so $\mathsf{df}(w\varphi) \geq k$ as well, and thus, w witnesses for deficiency k. □

It should be mentioned that the natural idea used in the above proof (of "gluing together" individual reset words in order to produce an "universal" reset word) first appeared in a paper by Ito and Duske, cf. [12, Theorem 3.1].

Corollary 4. *Over each finite alphabet A and for each $n > 3$, there exists a word of length $|A|^{\frac{1}{6}(n^3-n)-1} + \frac{1}{6}(n^3 - n) - 2$ that guarantees minimal image in T_n.* □

Proof. As in the proof of Theorem 2, we construct a word w of length $|A|^{\frac{1}{6}(n^3-n)-1} + \frac{1}{6}(n^3 - n) - 2$ that has every word of length $\frac{1}{6}(n^3 - n) - 1$ as a factor. Then of course w has also every word of length $\frac{1}{6}k(k+1)(k+2) - 1$, $1 \leq k < n$, as a factor and, as such, witnesses for deficiency k for all $1 \leq k < n$ by Proposition 3. We may also assume w witnessing for deficiency 0 as every word does so. The corollary now immediately follows from Lemma 1. □

Obviously, the constructions to which Theorem 2 and Corollary 4 refer are asymptotically (that is, for sufficiently large values of k and respectively n) more economic than the Sauer–Stone construction. Still, the length of the resulting words is exponential as a function of k. Can we do essentially better by finding some words of polynomial length doing the same job? The following result answers this question in the negative:

Theorem 5. *Any word over a finite alphabet A guaranteeing minimal image in T_n contains every word over A of length $n-1$ as a factor and has the length at least $|A|^{n-1} + n - 2$.*

Proof. We recall the construction of the minimal automaton of a language of the form A^*wA^*, where $w \in A^*$. This construction can be readily obtained from the well-known construction of the minimal automaton of A^*w, which is used, for instance, in pattern matching algorithms (implicitly in [15], and explicitly in [1, 3, 6]).

Given two words u and v words of A^*, we denote by $\mathrm{overlap}(u, v)$ the longest word $z \in A^*$ such that $u = u'z$, $v = zv'$ for some $u', v' \in A^*$. In other terms, $\mathrm{overlap}(u, v)$ is the longest suffix of u which is at the same time a prefix of v.

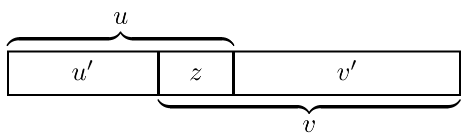

Figure 1: $z = \mathrm{overlap}(u, v)$

Now given a word $w = a_1 \cdots a_m \in A^*$, the minimal automaton of A^*wA^* is $\mathcal{A}(w) = (X, A, \varphi)$, with the set of states $X = \{a_1 \cdots a_i \mid 0 \le i \le m\}$, that is, the set of all prefixes of the word w, and the function $\varphi : A \to T(X)$ defined as follows: for all $a \in A$

$$a_1 \cdots a_m(a\varphi) = a_1 \cdots a_m, \tag{4}$$

$$a_1 \cdots a_i(a\varphi) = \mathrm{overlap}(a_1 \cdots a_i a, w) \quad \text{for } 0 \le i < m. \tag{5}$$

The initial state is the empty word, and the unique final state is the word w.

Lemma 6. *The automaton $\mathcal{A}(w)$ is synchronizing, and $u \in A^*$ is a reset word for $\mathcal{A}(w)$ if and only if the word w is a factor of u.*

Proof. Since the final state is stabilized by each letter, a reset word u in $\mathcal{A}(w)$ necessarily sends every state on the final state. In particular, it sends the initial state to the final state, and thus is accepted by $\mathcal{A}(w)$. It follows that w is a factor of u.

Conversely, if w is a factor of u, and x is a state, then w is a factor of xu. It follows that the word xu is accepted by $\mathcal{A}(w)$, whence $x(u\varphi) = w$. Thus u is a reset word. □

Now take an arbitrary word $v \in A^*$ of length $n - 1$ and consider the automaton $\mathcal{A}(v) = (X, A, \varphi)$. By Lemma 6, the mapping $\varphi : A \to T(X) = T_n$ verifies $\mathsf{rk}(v\varphi) = 1$. By the definition, any word $w \in A^*$ that guarantees minimal image in T_n should satisfy $\mathsf{rk}(w\varphi) \le \mathsf{rk}(v\varphi)$ whence $\mathsf{rk}(w\varphi) = 1$. Thus, w should be a reset word for automaton $\mathcal{A}(v)$. By Lemma 6, w then has the word v as a factor.

Since there are $|A|^{n-1}$ different words over A of length $n-1$ and since a word of length $m \geq n-1$ has $m-n+2$ factors of length $n-1$, any word over A containing every word over A of length $n-1$ as a factor has the length at least $|A|^{n-1}+n-2$. (This is, in fact, an exact bound—see the reasoning with the DeBruijn sequences in the proof of Theorem 2.) $\square$

Another natural question concerns the behavior of the constructions for small values of k and for small sizes of the alphabet A. Here the Sauer–Stone construction is often better as the following table shows. In the table, t denotes the size of the alphabet A and we omit some of the summands in the second column to fit onto the page.

Table 1: The Sauer–Stone construction vs. Theorem 2

k	The length of the word from:	
	the Sauer–Stone construction	Theorem 2
3	$t^7+4t^6+6t^5+10t^4+9t^3+7t^2+3t$	t^9+8
4	$t^{14}+5t^{13}+11t^{12}+21t^{11}+30t^{10}+37t^9+\cdots+4t$	$t^{19}+18$
5	$t^{27}+6t^{26}+17t^{25}+38t^{24}+68t^{23}+105t^{22}+\cdots+5t$	$t^{34}+33$
6	$t^{52}+7t^{51}+24t^{50}+62t^{49}+130t^{48}+\cdots+6t$	$t^{55}+54$
7	$t^{101}+8t^{100}+32t^{99}+94t^{98}+224t^{97}+\cdots+7t$	$t^{83}+82$

Using the values collected in this table, one can easily calculate that, for any $t>2$, the Sauer–Stone construction produces shorter words than the construction based on Proposition 3 for $k=3,4,5,6$. The case $t=2$ deserves some special attention. Here the following table, in which all words are meant to be over a two-letter alphabet, collects the necessary information:

Table 2: The case of a two-letter alphabet

k	The length of the word from:	
	the Sauer–Stone construction	Theorem 2
3	842	520
4	216 248	524 306
5	3542 987 594	17 179 869 217
6	237 765 870 667 058 360	36 028 797 018 964 022

We see that, for $k = 4, 5$, the Sauer–Stone construction over a two-letter alphabet is more economic than one arising from Theorem 2. Moreover, we recall that Sauer and Stone have found a word of length 8 that witnesses for deficiency 2. Though this is not explicitly mentioned in [21], it is pretty obvious that starting a recursion analogous to (3) with that word, one obtains a sequence of words over a two-letter alphabet such that the $(k-1)^{th}$ member of the sequence witnesses for deficiency k for each $k \geq 2$ and is shorter than the word w_k arising from (3). A straight calculation shows that this produces a word of length 346 witnessing for deficiency 3, a word of length 89 768 witnessing for deficiency 4, a word of length 1470 865 754 witnessing for deficiency 5, a word of length 98 708 129 987 190 440 witnessing for deficiency 6, etc. Comparing the data in Table 2 with these figures, we observe that the Sauer–Stone construction modified this way yields shorter words than the construction Theorem 2 for $k = 3, 4, 5$.

Yet, having in mind the benchmark we mentioned above, that is, of producing, over a two-letter alphabet, a word of reasonable size that guarantees minimal image in T_5, we cannot be satisfied with a word of length 89 768. A more important motivation for further efforts is provided by the crucial question if any "simultaneous" Černý word which resets all synchronizing automata with n states must indeed consist of all "individual" Černý words (one for each synchronizing automaton) somehow put together. We shall answer this question by exhibiting a better construction than one which we got from the automata-theoretical approach. The behavior of this construction for small deficiencies/alphabet sizes will be also better than that of any of the constructions above.

Given a transformation $f : X \to X$, we denote by $\mathsf{Ker}(f)$ its *kernel*, that is, the partition of the set X into $\mathsf{rk}(f)$ classes such that $x, y \in X$ belong to the same class of the partition if and only if $xf = yf$. By a *cross-section* of a partition π of X we mean any subset of X having a singleton intersection with each π-class. We need an obvious and well known lemma:

Lemma 7. *Let $f, g : X \to X$ be two transformations of rank r. Then the product fg has rank r if and only if $\mathsf{Im}(f)$ is a cross-section of $\mathsf{Ker}(g)$.* $\square$

Let $\varphi : A^* \to T(X)$ be a homomorphism, $w \in A^*$ a word with $\mathsf{rk}(w\varphi) = r$. Suppose that there exists a word $v \in A^*$ such that $\mathsf{rk}(wvw\varphi) < r$ and let $u = a_1a_2 \cdots a_m$ be a shortest word with this property. Setting, for $0 \leq i \leq m$,

$$\pi_i = \mathsf{Ker}((a_{m-i+1} \cdots a_m w)\varphi),$$
$$C_i = \mathsf{Im}((wa_1 \cdots a_i)\varphi),$$

we have the following proposition:

Proposition 8.

(1) $\pi_0, \pi_1, \ldots, \pi_{m-1}$ *are pairwise distinct partitions of* X *into* r *parts.*
(2) $C_0, C_1, \ldots, C_{m-1}$ *are pairwise distinct subsets of* X *of cardinality* r*.*
(3) *If* $i + j < m$*,* C_i *is a cross-section of* π_j*.*
(4) *If* $i + j = m$*,* C_i *is not a cross-section of* π_j*.*

Proof. Let $i < m$. If π_i has less than r classes, then

$$\mathsf{rk}((wa_{m-i+1} \cdots a_m w)\varphi) < r,$$

a contradiction with the choice of u. Similarly, the set C_i should consist of r elements. Thus, both $(wa_1 \cdots a_i)\varphi$, for $0 \le i \le m-1$, and $(a_{j+1} \cdots a_m w)\varphi$, for $1 \le j \le m$, are transformations of rank r. If $i < j$ and the set C_i is not a cross-section of the partition π_{m-j}, then by Lemma 7, the product

$$(wa_1 \cdots a_i)\varphi(a_{j+1} \cdots a_m w)\varphi = (wa_1 \cdots a_i a_{j+1} \cdots a_m w)\varphi$$

has rank $< r$, again a contradiction with the choice of u. Furthermore, by the same lemma, C_i cannot be a cross-section of π_{m-i} since $\mathsf{rk}(wuw\varphi) < r$. In particular, if $i < j$, the set C_{m-j} is a cross-section for π_i, but not for π_j. It follows that the partitions π_i and π_j are different provided that $i \neq j$. Similarly, all the sets C_i, for $0 \le i \le m-1$, are different. □

It is Proposition 8 that allows us to improve the Sauer–Stone construction. If we mimic the strategy of [21] and want to create a sequence of words witnessing for deficiency k by induction on k, then on each step, we may assume that we have some word w of deficiency k and we seek for a bound to the length of the shortest word v verifying $\mathsf{df}(wvw\varphi) > k$ for a given evaluation φ of deficiency $> k$. Proposition 8 shows that the length of such a minimal word is tightly related to the size of a specific combinatorial configuration involving subsets and partitions of an n-element set. According to a well-known method in combinatorics, we now convert this combinatorial problem into a problem of linear algebra.

Let $X = \{1, \ldots, n\}$. We identify each subset $C \subseteq X$ with its *characteristic vector* $(c_1, \ldots, c_n)$ in $\mathbb{R}^n$, defined by

$$c_i = \begin{cases} 1 & \text{if } i \in C, \\ 0 & \text{otherwise.} \end{cases}$$

The notation $|C|$, originally used to denote the number of elements of C, extends naturally to a linear form on $\mathbb{R}^n$ defined by

$$|C| = \sum_{1 \le i \le n} c_i.$$

Finally, if $C, D \subseteq X$, then denoting by $C \cdot D$ the scalar product $\sum_{1 \le i \le n} c_i d_i$, we observe that

$$C \cdot D = |C \cap D|.$$

It follows that a subset C of X is a cross-section of the partition $\{D_1, \ldots, D_r\}$ if and only if $C \cdot D_s = 1$ for all $s = 1, \ldots, r$.

With this notation in hand, we can prove the following bound for the size of the combinatorial configuration arising in Proposition 8:

Proposition 9. *If the partitions π_0, π_1, $\ldots$,π_{m-1} and the subsets C_0, C_1, $\ldots$, C_{m-1} of an n-element set satisfy the conditions* (1)–(4) *of Proposition* 8*, then $m \le n - r + 1$.*

Proof. We first prove that the vectors $C_0, C_1, \ldots, C_{m-1}$ are linearly independent. Otherwise, one of the C_j's is a linear combination of the preceding vectors $C_0, C_1, \ldots, C_{j-1}$, say

$$C_j = \sum_{0 \le i \le j-1} \lambda_i C_i.$$

It follows, since the map $C \mapsto |C|$ is linear,

$$r = |C_j| = \sum_{0 \le i \le j-1} \lambda_i |C_i| = r \sum_{0 \le i \le j-1} \lambda_i$$

whence $\sum\limits_{0 \le i \le j-1} \lambda_i = 1$. Consider the partition $\pi_{m-j} = \{D_1, D_2, \ldots, D_r\}$. Since each of the sets $C_0, C_1, \ldots, C_{j-1}$ is a cross-section of this partition, we obtain, for each $s = 1, \ldots, r$,

$$C_j \cdot D_s = \Big(\sum_{0 \le i \le j-1} \lambda_i C_i \Big) \cdot D_s = \sum_{0 \le i \le j-1} \lambda_i (C_i \cdot D_s) = \sum_{0 \le i \le j-1} \lambda_i = 1$$

whence C_j also is a cross-section of π_{m-j}, a contradiction.

Now $\pi_0 = \{B_1, B_2, \ldots, B_r\}$. Since the B_i's are pairwise disjoint and nonempty, their characteristic vectors are linearly independent. Furthermore, since $C_0, C_1, \ldots, C_{m-1}$ are cross-sections of π_0, the relation $C_i \cdot B_s = 1$ holds for $0 \le i \le m-1$ and $1 \le s \le r$. It follows in particular that

$$C_i \cdot (B_s - B_t) = 0 \quad \text{for } 1 \le s, t \le r. \tag{6}$$

Now, the vectors $B_s - B_t$, for $1 \le s, t \le r$, generate a vector space of dimension $r - 1$ and the relation (6) shows that each C_i is orthogonal to this space. It follows that the rank of the family $\{C_i\}_{0 \le i \le m-1}$ is at most $n - r + 1$, whence $m \le n - r + 1$. □

It is easy to see that the bound of Proposition 9 is exact. Applying Proposition 9 to the situation of Proposition 8 yields

Corollary 10. *Let k be a positive integer, $\varphi : A^* \to T(X)$ a homomorphism of deficiency $> k$. Then for any word $w \in A^*$ with $\mathsf{df}(w\varphi) = k$, there exists a word v of length $\leq k+1$ such that $\mathsf{df}(wvw\varphi) > k$.*

Now suppose that $A = \{a_1, \dots, a_t\}$ and let $u_1 = a_1 \cdots a_t$ and

$$u_{k+1} = u_k \prod_{\ell(v) \leq k+1} (vu_k). \tag{7}$$

Theorem 11. *For any positive integer k, the word u_k defined via (7) witnesses for deficiency k.*

Proof. By induction on k. The case $k = 1$ is obvious. Suppose that u_k witnesses for deficiency k and take any homomorphism $\varphi : A^* \to T(X)$ of deficiency $> k$. We are to verify that $\mathsf{df}(u_{k+1}\varphi) > k$. If already $\mathsf{df}(u_k\varphi) > k$, we have nothing to prove. If $\mathsf{df}(u_k\varphi) = k$, then by Corollary 10 there exists a word v of length $\leq k+1$ such that $\mathsf{df}(u_kvu_k\varphi) > k$. Since by (7) the word u_kvu_k appears as a factor in u_{k+1}, we also have $\mathsf{df}(u_{k+1}\varphi) > k$, as required. $\square$

From Theorem 11 and Lemma 1 we obtain

Corollary 12. *For each $n > 1$, the word u_{n-1} guarantees minimal image in T_n.* $\square$

A comparison between the definitions (3) and (7) shows that the word u_k is shorter than the Sauer–Stone word w_k (on the same alphabet) for each $k \geq 3$. In fact, the leading monomial in the expansion of $\ell(u_k)$ as a polynomial of $t = |A|$ equals $t^{\frac{1}{2}(k^2-k)}$; this means that asymptotically the construction (7) is better than the construction from Theorem 2. Moreover, we see that the shortest word in A^* that resets all synchronizing automata with a fixed number of states and with the input alphabet A does not need consisting of all shortest "individual" reset words somehow put together.

The following table exhibits some data about the size of words arising from (7) for small k and/or t. The data in the last column refer to a slight modification for the construction in the case when the alphabet consists of two letters; the modification is similar to the modification of the Sauer–Stone construction discussed above. Namely, we can make the word aba^2b^2ab play the role of u_2 and proceed by (7) for $k \geq 3$.

Viewing the data in Table 3 against the corresponding data in Tables 1 and 2 shows that the gain provided by the new construction is quite large

Table 3: The length of the words defined via (7)

k	$\|A\| = t$	$\|A\| = 2$	$u_2 = aba^2b^2ab$
1	t	2	
2	t^3+3t^2+2t	24	8
3	$t^6+4t^5+6t^4+9t^3+7t^2+3t$	394	154
4	$t^{10}+5t^9+11t^8+20t^7+27t^6+29t^5+\cdots+4t$	12 312	4872
5	$t^{15}+6t^{14}+17t^{13}+37t^{12}+64t^{11}+\cdots+5t$	775 914	307 194
6	$t^{21}+7t^{20}+24t^{19}+61t^{18}+125t^{17}+\cdots+6t$	98 541 720	39 014 280
7	$t^{28}+8t^{27}+32t^{26}+93t^{25}+218t^{24}+\cdots+7t$	25 128 140 138	9 948 642 938

even for small deficiencies and alphabet sizes. As for our "benchmark", that is, a word over a two-letter alphabet that guarantees minimal image in T_5, Table 3 indicates that there is such a word of length 4872. Yet too lengthy to be written down here, the word appears to be much closer to what may be called "a word of reasonable length" for its size is already well comparable with the size of the monoid T_5 itself (which is 3125).

References

[1] A. V. Aho, J. E. Hopcroft, and J. D. Ullman, The design and analysis of computer algorithms, Addison-Wesley, 1974.

[2] J. Almeida and M. V. Volkov, *Profinite methods in finite semigroup theory*, Centro de Matemática da Universidade do Porto, 2001, Preprint 2001–02.

[3] D. Beauquier, J. Berstel, and Ph. Chrétienne, Eléments d'algorithmique, Masson, 1994 [in French].

[4] J. Černý, *Poznámka k homogénnym eksperimentom s konecnými avtomatami*, Mat.-Fyz. Cas. Slovensk. Akad. Vied. **14** (1964) 208–216 [in Slovak].

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

[6] M. Crochemore and W. Rytter, Text algorithms, Oxford University Press, 1994.

[7] N. G. DeBruijn, *A combinatorial problem*, Proc. Nederl. Akad. Wetensch. **49** (1946) 758–764; Indagationes Math. **8** (1946) 461–467.

[8] L. Dubuc, *Les automates circulaires biaisés verifient la conjecture de Černý*, RAIRO, Inform. Theor. Appl. **30** (1996) 495–505 [in French].

[9] D. Eppstein, *Reset sequences for monotonic automata*, SIAM J. Comput. **19** (1990) 500–510.

[10] P. Frankl, *An extremal problem for two families of sets*, Eur. J. Comb. **3** (1982) 125–127.

[11] W. Goehring, *Minimal initializing word: A contribution to Černý conjecture*, J. Autom. Lang. Comb. **2** (1997) 209–226.

[12] M. Ito and J. Duske, *On cofinal and definite automata*, Acta Cybernetica **6** (1983) 181–189.

[13] J. Kari, *A counter example to a conjecture concerning synchronizing words in finite automata*, EATCS Bulletin **73** (2001) 146.

[14] J. Kari, *Synchronizing finite automata on Eulerian digraphs*, Math. Foundations Comput. Sci.; 26th Internat. Symp., Marianske Lazne 2001, Lect. Notes Comput. Sci. **2136** (2001) 432–438.

[15] D. E. Knuth, J. H. Morris, Jr, and V. R. Pratt, *Fast pattern matching in strings*, SIAM J. Comput. **6** (1977) 323–350.

[16] J.-E. Pin, *Sur un cas particulier de la conjecture de Černý*, Automata, Languages, Programming; 5th Colloq., Udine 1978, Lect. Notes Comput. Sci. **62** (1978) 345–352 [in French].

[17] J.-E. Pin, Le problème de la synchronisation. Contribution à l'étude de la conjecture de Černý, Thèse 3e cycle, Paris, 1978 [in French].

[18] J.-E. Pin, *Sur les mots synchronisants dans un automate fini*, Elektron. Informationverarbeitung und Kybernetik **14** (1978) 283–289 [in French].

[19] J.-E. Pin, *On two combinatorial problems arising from automata theory*, Ann. Discrete Math. **17** (1983) 535–548.

[20] R. Pöschel, M. V. Sapir, N. Sauer, M. G. Stone, and M. V. Volkov, *Identities in full transformation semigroups*, Algebra Universalis **31** (1994) 580–588.

[21] N. Sauer and M. G. Stone, *Composing functions to reduce image size*, Ars Combinatoria **31** (1991) 171–176.