Words Guaranteeing Minimum Image*

S. W. Margolis† J.-E. Pin‡ M. V. Volkov§

Abstract

Given a positive integer n and a finite alphabet Σ, a word w over Σ is said to *guarantee minimum image* if, for every homomorphism φ from the free monoid Σ^* over Σ 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 Σ^*. Although the existence of words guaranteeing minimum 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 their word was doubly exponential (as a function of n). We first show that some known results of automata theory immediately lead to an alternative construction that yields a simpler word that guarantees minimum image: it has exponential length, more precisely, its length is $O(|\Sigma|^{\frac{1}{6}(n^3-n)})$. Then with some more effort, we find a word guaranteeing minimum image similar to that of Sauer and Stone but of length $O(|\Sigma|^{\frac{1}{2}(n^2-n)})$. On the other hand, we prove that the length of any word guaranteeing minimum image cannot be less than $|\Sigma|^{n-1}$.

Introduction

Let Q be a set. A *transformation* of Q is an arbitrary function f whose domain is Q and whose range (denoted by $\mathsf{Im}(f)$) is a subset of Q. The *rank*

*This work was initiated when the third-named author visited Bar Ilan University (Ramat Gan, Israel) with the support of Department of Mathematics and Computer Science, Bar-Ilan University, and the Russian Foundation of Basic Research. The authors also acknowledge support from the INTAS through Network project 99-1224 'Combinatorial and Geometric Theory of Groups and Semigroups and its Applications to Computer Science'.

†Department of Mathematics and Computer Science, Bar Ilan University, 52900 Ramat Gan, ISRAEL; margolis@macs.biu.ac.il

‡Laboratoire d'Informatique Algorithmique: Fondements et Applications, Université Paris Denis Diderot et CNRS, 75251 Paris, FRANCE; Jean-Eric.Pin@liafa.jussieu.fr

§Department of Mathematics and Mechanics, Ural State University, 620083 Ekaterinburg, RUSSIA; Mikhail.Volkov@usu.ru

$\mathsf{rk}(f)$ of the function f is the cardinality of the set $\mathsf{Im}(f)$. Transformations of Q form a monoid under the usual composition of functions; the monoid is called *the full transformation monoid over* Q and is denoted by $T(Q)$. If the set Q is finite with $|Q| = n$, the monoid $T(Q)$ is also denoted by T_n.

Now let Σ be a finite alphabet and $\varphi : \Sigma^* \to T_n$ be an arbitrary homomorphism of the free monoid Σ^* over Σ into T_n. A word $w \in \Sigma^*$ is said to *guarantee minimum image in* T_n if the inequality

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

holds **for each word** $v \in \Sigma^*$ and **for each homomorphism** $\varphi : \Sigma^* \to T_n$. This notion was introduced by Sauer and Stone in [32].

Clearly, words guaranteeing minimum image exists [29, Proposition 2.3]. Indeed, for each homomorphism $\varphi : \Sigma^* \to T_n$, there is a word w_φ such that

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

for all $v \in \Sigma^*$. Observe that φ is uniquely determined by its restriction to Σ and there are only finitely many mappings between the finite sets Σ and T_n. Since the composition of transformations cannot increase the size of image, we can concatenate all words w_φ getting an (apparently very long) word w satisfying (1).

Words guaranteeing minimum image have been proved to have some interesting algebraic applications. In [29] they were used to find identities in full transformation monoids. Recently these words have been applied for studying the structure of the free profinite semigroup, see [2]. As we will see below, they also play some natural role in the theory of finite automata. Of course, for application purposes, the existence statement outlined above is not sufficient and one seeks an explicit construction.

The construction of words guaranteeing minimum image that is due to Sauer and Stone [32, Corollary 3.5] makes an elegant use of recursion but results in non-realistically long words. Even over a two-element alphabet, it is hardly possible to write down the Sauer–Stone word that guarantees minimum image, say, in T_5. We discuss the Sauer–Stone construction in some detail in Section 1 for we want to compare it with the alternative constructions we present in Sections 2 and 3. Our first approach in Section 2 is based on a tight connection between words guaranteeing minimum image and a black-box version of the famous Černý problem [10] on synchronizing automata. Using this connection we readily obtain words of size $O(|\Sigma|^{\frac{1}{6}(n^3-n)})$ guaranteeing minimum image in T_n. In Section 3 we follow

the recursion approach of Sauer and Stone; however, after explicitly isolating a corresponding combinatorial configuration and carefully analyzing it, we are able to construct a word guaranteeing minimum image in T_n with length $O(|\Sigma|^{\frac{1}{2}(n^2-n)})$. In Section 4 we show that, on the other hand, the length of any word over Σ guaranteeing minimum image in T_n cannot be less than $|\Sigma|^{n-1}$. Section 5 reports on the results of some computer experiments (performed by I. V. Petrov, a student of the third-named author) whose aim was to determine shortest words guaranteeing minimum image in T_n for some small values n and $|\Sigma|$.

1 The Sauer–Stone construction

To build a word guaranteeing minimum 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 Q, we denote by $\mathsf{df}(f)$ its *deficiency*, that is, the difference $|Q| - \mathsf{rk}(f)$. For a homomorphism $\varphi : \Sigma^* \to T(Q)$, we denote by $\mathsf{df}(\varphi)$ the maximum of the deficiencies $\mathsf{df}(v\varphi)$ where v runs over Σ^*; 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 $w \in \Sigma^*$ *witnesses for deficiency* k (*has property* Δ_k in Sauer and Stone's terminology) provided that, **for all homomorphisms** $\varphi : \Sigma^* \to T(Q)$ where Q is a finite set, $\mathsf{df}(w\varphi) \geq k$ whenever $\mathsf{df}(\varphi) \geq k$.

We note that the cardinality of the set Q is **not** fixed in this definition; therefore it is not obvious that a word which witnesses for deficiency k should exist for every k. On the other hand, it is clear that if $\Sigma = \{a_1, \ldots, a_t\}$, then the product $w_1 = a_1 \cdots a_t$ witnesses for deficiency 1. (Indeed, if $\mathsf{df}(\varphi) \geq 1$ for a homomorphism φ, then at least one of the letters $a_1, \ldots, a_t$ should be sent to 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

$$w_{k+1} = w_k \prod_{|v| \leq 1+3\cdot 2^{k-2}} (vw_k). \tag{3}$$

Their main result says that, for each k, the word w_k witnesses for deficiency k [32, Theorem 3.3]. Now the following simple observation applies:

Lemma 1.1. *If a word w witnesses for deficiency k for all $0 \leq k < n$, then it guarantees minimum image in T_n.*

Proof. Take an arbitrary homomorphism $\varphi : \Sigma^* \to T_n$ and apply it to an arbitrary word $v \in \Sigma^*$ 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 minimum image requires. □

Thus, for any $n > 1$, the word w_{n-1} defined via (3) guarantees minimum image in T_n [32, Corollary 3.5]. Using (3) on can easily calculate 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 minimum image in T_5 results in a word of length 216 248; thus, we were not exaggerating as we said in the introduction that it would be rather hard to write down this word! Sauer and Stone have suggested the following open problem: for a given t-letter alphabet, 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 $\mu_k(t)$ which was known up to now was $\mu_2(2) = 8$—it is shown in [32, 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 such constructions in the two next sections.

2 A connection with the generalized Černý conjecture

Let $\mathcal{A} = \langle Q, \Sigma, \delta\rangle$ be a deterministic finite automaton (DFA), where Q denotes the state set, Σ stands for the input alphabet, and $\delta : Q \times \Sigma \to Q$ is the transition function defining an action of the letters in Σ on Q. The action extends in a unique way to an action $Q \times \Sigma^* \to Q$ of the free monoid Σ^* over Σ; the latter action is still denoted by δ. The automaton $\mathcal{A}$ is called *synchronizing* if there exists a word $w \in \Sigma^*$ whose action resets $\mathcal{A}$, that is, leaves the automaton in one particular state no matter which state

in Q it started at: $\delta(q,w)=\delta(q',w)$ for all $q,q'\in Q$. 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. Černý conjectured in [10]—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. [11,13–15,19,25], to mention a few most representative papers only), this conjecture still constitutes an open problem.

The second-named author of the present paper extended Černý's conjecture in the following way (see [26, 27]). Recall that the transition function $\delta: Q\times\Sigma^*\to Q$ of each DFA $\mathcal{A}=\langle Q,\Sigma,\delta\rangle$ defines a natural homomorphism $\varphi_{\mathcal{A}}:\Sigma^*\to T(Q)$ via the rule

$$\begin{array}{rcccccc} \varphi_{\mathcal{A}}: & v & \mapsto & v\varphi_{\mathcal{A}}: & Q & \to & Q \\ & & & v\varphi_{\mathcal{A}}: & q & \mapsto & \delta(q,v) \end{array} \tag{4}$$

Suppose that $\mathsf{df}(\varphi_{\mathcal{A}})\geq k$ where $1\leq k<|Q|$. Then the extended conjecture was that there exists a word $w\in\Sigma^*$ of length k^2 for which $\mathsf{df}(w\varphi_{\mathcal{A}})\geq k$. (Clearly, the original Černý conjecture corresponds to the case $k=|Q|-1$.) It was proved for some partial cases in [26, 27] but recently Kari [18] has found an automaton $\mathcal{K}$ with 6 states for which no word w of length 16 satisfies $\mathsf{df}(w\varphi_{\mathcal{K}})\geq 4$ and hence disproved the extended conjecture as it was formulated in [26, 27]. One can, however, observe that Kari's automaton is synchronizing (which means that in fact $\mathsf{df}(\varphi_{\mathcal{K}})=5$) and admits a reset word of length 25. This suggests that the right generalization of the Černý conjecture may look as follows: *if k is the deficiency of the homomorphism $\varphi_{\mathcal{A}}$ associated via* (4) *with a finite automaton $\mathcal{A}=\langle Q,\Sigma,\delta\rangle$, then there exists a word $w\in\Sigma^*$ of length k^2 for which $\mathsf{df}(w\varphi_{\mathcal{A}})=k$.* This new conjecture (which we will refer to as *the generalized Černý conjecture*) still contains the original Černý conjecture as a special case and is consistent with the current experimental material (including Kari's example).

For the purpose of the present paper it is important to relate the proposed generalization of the Černý conjecture to our initial problem of constructing words that guarantee minimum image in T_n. In fact, the similarity between the two situations is pretty obvious: in the former case we look for a shortest word of minimum rank for a specific homomorphism $\varphi_{\mathcal{A}}:\Sigma^*\to T_n$ (where $n=|Q|$) while in the latter case we are interested in a shortest word which has minimum rank with respect to every homomorphism from Σ^* to T_n. 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 of minimum rank for a DFA but in contrast with the generalized Černý conjecture situation, the automaton is a black-box about which we only know

that it has n states. Thus, from the point of view of automata theory the notion of a word guaranteeing minimum image appears to be fairly natural as it fits into the classic framework of Moore's "Gedanken-experiments" [22]. We notice in passing that, if thinking of a real computational device as a compound made from a number of finite automata, each with a relatively small number of states, a reasonable construction for an input signal that would simultaneously reset all those automata and that could be generated without analyzing the structure of each particular component of the device might be of some practical interest. For instance, recent experiments in biocomputing (see [7, 8]), in which DNA molecules have been used as both hardware and software for constructing finite automata of nanoscaling size, have resulted in a 'soup of automata', that is, a solution containing 3×10^{12} copies of a certain DFA per μl. All these copies can work in parallel on different inputs, thus ending up in different and unpredictable states. In contrast to an electronic computer, one cannot reset such a system by just pressing a button; instead, in order to synchronously bring each automaton to its "ready-to-restart" state, one could spice the soup with (sufficiently many copies of) a DNA molecule whose nucleotide sequence encodes a reset word for the automata. And if a molecular computer is built from several tubes containing soups with different underlying automata, one can reset it at once by adding to each tube molecules that encode a word guaranteeing minimum image in T_n (where n is the maximum number of states of the automata).

Returning back to the mainstream of the paper, we easily extract from the connection that we just discussed the following conclusion:

Theorem 2.1. *If the generalized Černý conjecture holds true, then, over each finite alphabet Σ and for each $n > 1$, there exists a word of length $|\Sigma|^{(n-1)^2} + n^2 - 2n$ that guarantees minimum image in T_n.*

Proof. By a well known result of DeBruijn [12], there is a cyclic sequence over Σ, of length $|\Sigma|^{(n-1)^2}$, such that each word over Σ of length $(n-1)^2$ appears as a factor of the sequence. Cut this cycle in an arbitrary place and make it a word u of the same length $|\Sigma|^{(n-1)^2}$. Since our cut goes through exactly $(n-1)^2 - 1$ factors of length $(n-1)^2$, the word u still contains all but $(n-1)^2 - 1$ words of length $(n-1)^2$ as factors. Now take in u the prefix v of length $(n-1)^2 - 1$ and put it on the back of u thus obtaining the word $w = uv$ of length $|\Sigma|^{(n-1)^2} + n^2 - 2n$. Clearly, this procedure restores all those factors of length k^2 that we have destroyed by cutting the initial DeBruijn sequence, and therefore, each word over Σ of length $(n-1)^2$ appears as a factor in w. We note that there is an efficient procedure that,

given Σ and n, builds DeBruijn's sequences so, if necessary, the word w may be explicitly written down.

Now suppose that the generalized Černý conjecture holds true. Then for any homomorphism $\varphi : \Sigma^* \to T_n$ with $\mathsf{df}(\varphi) = k \leq n-1$ there exists a word $w_\varphi \in \Sigma^*$ of length k^2 such that $\mathsf{df}(w_\varphi\varphi) = k$. Clearly, the word w_φ can be extended to a word of length $n-1$ and, by the above construction of the word w, w_φ must appear as a factor in w. Hence $\mathsf{df}(w\varphi) = k$ and thus w guarantees minimum image in T_n. □

It should be mentioned that the natural idea used in the above proof (of "gluing together" individual reset words in order to produce a "universal" reset word) first appeared in a paper by Ito and Duske [17].

Thus, we see that the validity of the generalized Černý conjecture would have as an immediate consequence an easy construction for words guaranteeing minimum image, and obviously the construction obtained this way would be (asymptotically) more economic than that by Sauer and Stone. We note that the conjecture has been proved to hold for $k = 1, 2, 3$ (see [26]); thus, for $n = 2, 3, 4$, the construction from Theorem 2.1 certainly works. However in the general case the conjecture is open. Therefore it appears to be reasonable to look for a slightly weaker, but non-conditional construction. We provide such a construction utilizing a result by the second-named author [28]. This result which is based on a combinatorial theorem conjectured by the second-named author and then proved by Frankl [16] yields the best approximation to the size of the shortest reset word known so far.

Proposition 2.2. *Suppose that the DFA $\mathcal{A} = (Q, \Sigma, \delta)$ is such that the deficiency of the homomorphism $\varphi_\mathcal{A} : \Sigma^* \to T(Q)$ defined via (4) is no less than k where $3 \leq k < |Q|$. Then there exists a word $w \in \Sigma^*$ of length $\frac{1}{6}k(k+1)(k+2) - 1$ verifying $\mathsf{df}(w\varphi_\mathcal{A}) \geq k$.*

Perhaps, it is a good place to note that for $k = |Q| - 1$ (the case that, we recall, corresponds to the original Černý conjecture), a result analogous to Proposition 2.2 has been rediscovered in the paper [21] whose authors were (and, as is their recent publications [30, 31] shows, still are) unaware of [28] and [16].

It should be clear that combining the reasoning from the proof of Theorem 2.1 with Proposition 2.2 leads to the following result:

Theorem 2.3. *Over each finite alphabet Σ and for each $n > 3$, there exists a word of length $|\Sigma|^{\frac{1}{6}(n^3-n)-1} + \frac{1}{6}(n^3 - n) - 2$ that guarantees minimum image in T_n.*

Obviously, the construction of Theorem 2.3 is asymptotically (that is, for sufficiently large values of 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? We answer this question in the negative in Section 4. Another natural question concerns the behavior of the constructions for small values of n and for small sizes of the alphabet Σ. Here the Sauer-Stone construction is often better as the following table shows. In the table, t denotes the size of the alphabet Σ and we omit some of the summands in the second column to fit into the page.

Table 1: The Sauer-Stone construction vs. Theorems 2.1 and 2.3

	The length of the word from:		
n	the Sauer-Stone construction	Thm 2.1	Thm 2.3
2	t	t	
3	t^3+3t^2+2t	t^4+3	
4	$t^7+4t^6+6t^5+10t^4+9t^3+7t^2+3t$	t^9+8	t^9+8
5	$t^{14}+5t^{13}+11t^{12}+21t^{11}+30t^{10}+37t^9+\cdots+4t$	$t^{16}+15$	$t^{19}+18$
6	$t^{27}+6t^{26}+17t^{25}+38t^{24}+68t^{23}+105t^{22}+\cdots+5t$	$t^{25}+24$	$t^{34}+33$
7	$t^{52}+7t^{51}+24t^{50}+62t^{49}+130t^{48}+\cdots+6t$	$t^{36}+35$	$t^{55}+54$
8	$t^{101}+8t^{100}+32t^{99}+94t^{98}+224t^{97}+\cdots+7t$	$t^{49}+48$	$t^{83}+82$

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 the generalized Černý conjecture for $n=3,4,5$ and does better than the construction based on Proposition 2.2 for $n=4,5,6,7$. 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 Sauer-Stone construction vs. Theorems 2.1 and 2.3 in the case of a two-letter alphabet

	The length of the word from:		
n	the Sauer-Stone construction	Theorem 2.1	Theorem 2.3
2	2	2	
3	24	19	
4	842	520	520
5	216 248	65 551	524 306
6	3 542 987 594	33 554 456	17 179 869 217
7	237 765 870 667 058 360	68 719 476 771	36 028 797 018 964 022

We see that, over a two-letter alphabet, the construction based on the generalized Černý conjecture always produces shorter word than the Sauer-

Stone construction. However, for $n = 5$ and $n = 6$ the Sauer-Stone construction is more economic than the one arising from Theorem 2.3. 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 [32], 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 $(n-1)^{th}$ member of the sequence guarantees minimum image in T_n for each $n \geq 2$ and is shorter than the word w_{n-1} arising from (3). A straightforward calculation shows that this produces words guaranteeing minimum image of length 346 for T_4, of length 89 768 for T_5, of length 1 470 865 754 for T_6, of length 98 708 129 987 190 440 for T_7, 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 constructions from Theorem 2.1 and Theorem 2.3 for $n = 3, 4$ and respectively $n = 4, 5, 6$.

Yet, having in mind the benchmark we mentioned in the Introduction, that is, of producing, over a two-letter alphabet, a word of reasonable size that guarantees minimum image in T_5, we can be satisfied with neither a word of length 89 768 nor even a (still hypothetical!) word of length 65 551. A more important motivation for further efforts is provided by the crucial question: must any "simultaneous" Černý word that resets all synchronizing automata with n states consist of all "individual" Černý words (one for each synchronizing automaton) somehow put together? In the next section we will answer this question by exhibiting a better construction than the one which we got almost for free 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.

3 Improving the Sauer-Stone construction

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

Lemma 3.1. *Let $f, g : Q \to Q$ 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 $\mathsf{Ker}(g)$.*

We use the following notational convention. For any sequence $a_1, \ldots, a_m$ of (not necessarily distinct) letters, the expression $a_i \cdots a_j$ denotes:

– the word of length $j-i+1$ such that the letter in position p (where $p \in \{1,\dots,j-i+1\}$) is a_{i+p-1} provided that $i \le j$;
– the empty word otherwise.
By an *r-set* (*r-partition*) we mean a set with r elements (respectively, a partition of a set into r parts).

Let $\varphi : \Sigma^* \to T(Q)$ be a homomorphism, $w \in \Sigma^*$ a word with $\mathsf{rk}(w\varphi) = r$. Suppose that there exists a word $v \in \Sigma^*$ such that $\mathsf{rk}(wvw\varphi) < r$ and let $u = a_1 a_2 \cdots a_m$ be a shortest word with this property. Setting for $0 \le i < m$

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

we have the following proposition:

Proposition 3.2.

(1) *π_0, π_1, …, π_{m-1} are pairwise distinct r-partitions of Q.*
(2) *C_0, C_1, …, C_{m-1} are pairwise distinct r-subsets of Q.*
(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 3.1, 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. Therefore the partitions π_i and π_j are different provided that $i \ne j$. Similarly, all the sets C_i for $0 \le i \le m-1$ are different. □

It is Proposition 3.2 that allows us to improve the Sauer-Stone construction. If we mimic the strategy of [32] 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 a bound

to the length of the shortest word v verifying $\mathsf{df}(vvw\varphi) < k$ for a given homomorphism φ of deficiency $> k$. Proposition 3.2 shows that the length of such a minimum word is tightly related to the size of a specific combinatorial configuration involving r-subsets of an n-set and its r-partitions. According to a well-known method in combinatorics, we now convert this combinatorial problem into a problem of linear algebra. (The second-named author's paper [24] was probably the first where an analogous approach was applied to Černý type problems. However, as the referee of the present paper pointed out, linear algebra methods were used in treating of certain problems of a similar flavor even before the Černý conjecture was formulated, see, e.g., the paper by Perles, Rabin and Shamir [23] on so-called definite automata.) Among notions from linear algebra we use, the notion of the rank of a system of vectors will appear. This should not cause any confusion for the notion of the rank of a transformation used before will not occur in our proof.

Let $Q = \{1, \cdots, n\}$. We identify each subset $C \subseteq Q$ with its characteristic vector 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, denoting by $C \cdot D$ the scalar product $\sum_{1 \le i \le n} C_i D_i$, we observe that

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

Therefore a subset C of Q is a cross-section of the partition $\{D_1, \ldots, D_r\}$ if and only if $C \cdot D_i = 1$ for $1 \le i \le r$.

With these notations in hand, Proposition 3.2 leads to the following result.

Proposition 3.3. *The relation $m \le n - r + 1$ holds.*

Proof. We first prove that the vectors C_0, C_1, …, 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, …, C_{j-1}, say

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

It follows, since the map $C \to |C|$ 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 $\sum_{0 \le i \le j-1} \lambda_i = 1$. 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.

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

$$C_i \cdot (B_j - B_k) = 0 \quad \text{for } 1 \le j, k \le r \tag{5}$$

Now the vectors $B_j - B_k$ for $1 \le j, k \le r$ generate a vector space of dimension $r-1$ and relation (5) 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 $m \le n - r + 1$. □

Proposition 3.3 yields

Corollary 3.4. *Let k be a positive integer, $\varphi : \Sigma^* \to T(Q)$ a homomorphism of deficiency $> k$. Then for any word $w \in \Sigma^*$ with $\mathsf{df}(w\varphi) = k$ there exists a word v of length $\le k+1$ such that $\mathsf{df}(wvw\varphi) > k$.*

Now suppose that $\Sigma = \{a_1, \ldots, a_t\}$ and let $u_1 = a_1 \cdots a_t$ and

$$u_{k+1} = u_k \prod_{\ell(v) \le k+1} (v u_k). \tag{6}$$

Theorem 3.5. *For any positive integer k, the word u_k defined via (6) witnesses for deficiency k.*

Proof. By induction on k. The case $k = 1$ is obvious (see the reasoning in the second paragraph of Section 1). Suppose that u_k witnesses for deficiency k and take any homomorphism $\varphi : \Sigma^* \to T(Q)$ of deficiency $> k$. We have 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 3.4 there exists a word v of length $\le k+1$ such that $\mathsf{df}(u_k v u_k \varphi) > k$. Since by (6) the word $u_k v u_k$ appears as a factor in u_{k+1}, we also have $\mathsf{df}(u_{k+1}\varphi) > k$, as required. □

From Theorem 3.5 and Lemma 1.1 we obtain

Corollary 3.6. *For each $n > 1$, the word u_{n-1} guarantees minimum image in T_n.*

A comparison between the definitions (3) and (6) 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 $t = |\Sigma|$ equals $t^{\frac{1}{2}(k^2-k)}$; this means that asymptotically the construction (6) is better than not only the construction from Theorem 2.3 but also the construction from Theorem 2.1 which, we recall, depends on the generalized Černý conjecture. The following table exhibits some data about the size of words arising from (6) for small n 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 in the second to last paragraph of Section 2. Namely, we can make the word aba^2b^2ab play the role of u_2 and proceed by (6) for $k \geq 3$.

Table 3: The length of the words defined via (6)

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

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 essential even for small deficiencies and alphabet sizes. As for our "benchmark", that is, a word over two letters that guarantees minimum 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 semigroup T_5 itself (which is 3125). In the rest of the paper we discuss to what extent the achieved results may be further improved.

4 A lower bound

Now we seek a lower bound for the length of a word guaranteeing minimum image in T_n. For this aim, we recall the construction of the minimal automaton of a language of the form $\Sigma^* w \Sigma^*$, where $w \in \Sigma^*$. This construction can be readily obtained from the well-known construction of the minimal automaton of $\Sigma^* w$, which is used, for instance, in pattern matching algorithms (implicitly in [20], and explicitly in [1, 6, 9]).

Given two words u and v words of Σ^*, we denote by $\mathrm{overlap}(u, v)$ the longest word $z \in \Sigma^*$ 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.

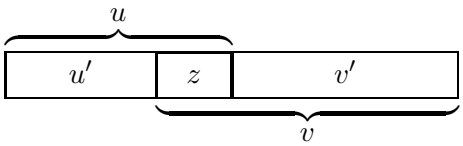

Figure 1: $z = \mathrm{overlap}(u, v)$

Given a word $w = a_1 \cdots a_m \in \Sigma^*$, the minimal automaton of $\Sigma^* w \Sigma^*$ is $\mathcal{A}(w) = \langle Q, \Sigma, \delta \rangle$ with the set of states $Q = \{a_1 \cdots a_i \mid 0 \leq i \leq m\}$, that is, the set of all prefixes of the word w, and the transition function $\delta : Q \times \Sigma \to Q$ defined as follows: for all $a \in \Sigma$

$$\delta(a_1 \cdots a_m, a) = a_1 \cdots a_m,$$
$$\delta(a_1 \cdots a_i, a) = \mathrm{overlap}(a_1 \cdots a_i a, w) \text{ for } 0 \leq i < m.$$

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

The following picture illustrates this construction by showing the automaton $\mathcal{A}(a^2bab)$ over the alphabet $\{a, b\}$.

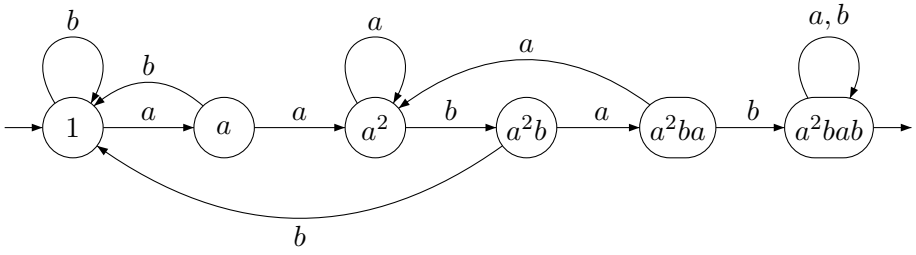

Figure 2: The automaton $\mathcal{A}(a^2bab)$

Proposition 4.1. *The automaton $\mathcal{A}(w)$ is synchronizing and $u \in \Sigma^*$ 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 a sink, any reset word u for $\mathcal{A}(w)$ necessarily sends every state to the final state. In particular, it sends the initial state to the final state and thus it is accepted by $\mathcal{A}(w)$. Therefore 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. Therefore the word xu is accepted by $\mathcal{A}(w)$ whence $\delta(x,u) = w$. Thus u is a reset word. □

Theorem 4.2. *Any word over a finite alphabet Σ guaranteeing minimum image in T_n contains every word over Σ of length $n-1$ as a factor and has length at least $|\Sigma|^{n-1} + n - 2$.*

Proof. Take an arbitrary word $v \in \Sigma^*$ of length $n-1$ and consider the automaton $\mathcal{A}(v) = \langle Q, \Sigma, \delta \rangle$. By Proposition 4.1, the homomorphism $\varphi_{\mathcal{A}(v)} : \Sigma^* \to T(Q) = T_n$ verifies $\mathsf{rk}(v\varphi_{\mathcal{A}(v)}) = 1$. Now take any word $w \in \Sigma^*$ that guarantees minimum image in T_n; by the definition, it should satisfy $\mathsf{rk}(w\varphi_{\mathcal{A}(v)}) \leq \mathsf{rk}(v\varphi_{\mathcal{A}(v)})$ whence $\mathsf{rk}(w\varphi_{\mathcal{A}(v)}) = 1$. Thus, w should be a reset word for automaton $\mathcal{A}(v)$. By Proposition 4.1, w then has the word v as a factor.

Since there are $|\Sigma|^{n-1}$ different words over Σ 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 Σ containing every word over Σ of length $n-1$ as a factor has the length at least $|\Sigma|^{n-1} + n - 2$. (This bound is, in fact, exact — see the reasoning with the DeBruijn sequences in the first paragraph of the proof of Theorem 2.1.) □

5 Numerical results

In the previous sections we have established some lower and some upper bounds for the minimum length of a word guaranteeing minimum image in T_n. Obviously, the gap between these bounds is rather wide. Which direction should one go next: increasing the lower bound or decreasing the upper one? In order to obtain at least a rough answer to this question we tried to explicitly construct shortest words guaranteeing minimum image in T_3 over 3 letters and respectively in T_4 over 2 letters. To this aim I. V. Petrov, a student of the third-named author, has implemented an exhaustive search algorithm in Visual C++ 6.0. Here is a brief account of the results obtained by Petrov's program; their more detailed description is published in [5].

It turns out that the minimum length of a word over 3 letters guaranteeing minimum image in T_3 is equal to 20. Up to renaming of the letters there exists 22 such words; the word

$$aba^2cacb^2cbabcba^2c^2b$$

is the first in their alphabetical list. Observe that the lower bound from Theorem 4.2 is $3^2 + 3 - 2 = 10$ while the upper bound from Corollary 3.6 is $3^3 + 3 \cdot 3^2 + 2 = 56$. We see that the real value is much closer to the lower theoretical bound. In fact, words constructed via Corollary 3.6 have a stronger property than that of guaranteeing minimum image in T_3: they witness for deficiency 2. Using the algorithm from [3, 4] that recognizes the latter property we have checked that none of the shortest words over 3 letters guaranteeing minimum image in T_3 witness for deficiency 2. In fact, the minimum length of a word over 3 letters that witnesses for deficiency 2 is 21; thus, in the notation introduced in Section 1, $\mu_2(3) = 21$.

The minimum length of a word over 2 letters guaranteeing minimum image in T_4 is equal to 33. Surprisingly enough, it turns out that (up to renaming of the letters) there is a unique such word, namely

$$ab^2aba^3b^2a^2babab^2a^2b^3aba^2ba^2b^2a.$$

The lower bound from Theorem 4.2 is $2^3 + 4 - 2 = 10$ while the theoretical upper bound presented in Table 3 is 154. Again we see that the lower bound is much closer to the real value. We may conclude that the results of computer experiments clearly indicate that there should exist more efficient constructions for words guaranteeing minimum image than those presently known.

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 identities for finite semigroups whose subgroups belong to a given pseudovariety*, J. Algebra and Appl. **2** (2003) 137–163.

[3] D. S. Ananichev, A. Cherubini, and M. V. Volkov, *An inverse automata algorithm for recognizing 2-collapsing words*, Developments in Language Theory, 6th Internat. Conf. DLT 2002, Lect. Notes Comp. Sci. **2450** (2003) 270–282.

[4] D. S. Ananichev, A. Cherubini, and M. V. Volkov, *Image reducing words and subgroups of free groups*, Theor. Comput. Sci. **307** (2003) 77–92.

[5] D. S. Ananichev and I. V. Petrov, *Quest for short synchronizing words and short collapsing words*, Proc. WORDS'03, 4th Internat. Conf. on Combinatorics on Words, Turku Centre Comp. Sci. General Publication **27** (2003) 411–418.

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

[7] Y. Benenson, T. Paz-Elizur, R. Adar, E. Keinan, Z. Livneh, and E. Shapiro, *Programmable and autonomous computing machine made of biomolecules*, Nature **414**, No.1 (November 22, 2001) 430–434.

[8] Y. Benenson, R. Adar, T. Paz-Elizur, Z. Livneh, and E. Shapiro, *DNA molecule provides a computing machine with both data and fuel*, Proc. National Acad. Sci. USA **100** (2003) 2191–2196.

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

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

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

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

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

[14] L. Dubuc, *Sur les automates circulaires et la conjecture de Černý*, RAIRO Inform. Theor. Appl. **32** (1998) 21–34 [in French].

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

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

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

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

[19] 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.

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

[21] A.A. Klyachko, I.K. Rystsov, and M.A. Spivak, *An extremal combinatorial problem associated with the bound of the length of a synchronizing word in an automaton*, Kibernetika (1987) No.2, 16–20, 25 [in Russian; Engl. translation: Cybernetics **23** (1987) 165–171].

[22] E. F. Moore, *Gedanken-experiments on sequential machines*, C. E. Shannon and J. McCarthy (eds.), Automata Studies, Priceton University Press, 1956, 129–153.

[23] M. Perles, M. O. Rabin, and E. Shamir, *The theory of definite automata*, IEEE Trans. Electron. Comput. **12** (1963) 233–243.

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

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

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

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

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

[29] 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.

[30] I. K. Rystsov, *Almost optimal bound of reccurent word length for regular automata*, Kibernetika i Sistemnyj Analiz (1995) No.5, 40–48 [in Russian; Engl. translation: Cybern. Syst. Anal. **31** (1995) 669–674].

[31] I. K. Rystsov, *Quasioptimal bound for the length of reset words for regular automata*, Acta Cybern. **12** (1995) 145–152.

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