Towards a Better Understanding of One-Wayness: Facing Linear Permutations

Alain P. Hiltgen

UBS – Corporate IT Security
P.O. Box, CH-8021 Zurich, Switzerland
E-mail: alain.hiltgen@ubs.com

Abstract. The one-wayness of linear permutations, i.e., invertible linear Boolean functions F: $\{0,1\}^n \rightarrow \{0,1\}^n$, is investigated. For linear permutations with a triangular matrix description (*t-linear* permutations), we prove that one-wayness, $C(F^{-1})/C(F)$, is non-trivially upperbounded by $16\sqrt{n}$, where $C(.)$ denotes unrestricted circuit complexity. We also prove that this upper bound strengthens as the complexity of the inverse function increases, limiting the one-wayness of t-linear permutations with $C(F^{-1}) = n^2/(c \log_2(n))$ to a constant, i.e., a value that is independent of n. Direct implications for linear and also non-linear permutations are discussed. Moreover, and for the first time ever, a description is given about where, in the case of linear permutations, practical one-wayness would have to come from, if it exists.

1 Introduction

One-wayness in a very intuitive sense describes the property that, for a function $F(.)$, it is much easier, given X, to *compute* $Z = F(X)$ than it is, given Z, to *find* X such that $Z = F(X)$. The fundamental importance of the existence of one-wayness, both for public-key and secret-key cryptography, has been pointed out at numerous occasions; see for example [5] [10] [6]. Menezes *et al.* [12] give a detailed survey of the research in this field, which essentially resumes to: (i) relating the existence of one-way functions to the existence of other cryptographic primitives or to the truth of certain well-founded complexity-theoretic assumptions; (ii) adapting the complexity-theoretic definition of a one-way function, to make it best captures the real needs of practical cryptography; (iii) searching for potential candidate one-way functions that can be used in practical applications. All these investigations largely contributed in clarifying and in satisfying our primary needs and in positioning the provability of one-wayness with respect to other complexity-theoretic problems of interest. Unfortunately, however, they also forged the now widely spread opinion that the provability of one-wayness is a today unsolvable problem.

The approach in this paper is a completely different one. It primarily aims at *understanding the mechanisms* that could generate or limit any sort of one-wayness that would be suitable for practical applications. With this objective in mind, special attention is paid to the very details, essentially forgetting about

infinite problems (or infinite families of Boolean functions) and concentrating on finite collections of finite subproblems (or Boolean 'vector' functions). The types of functions under consideration are restricted (permutations, linear functions), and weaker notions [7] of non-uniform one-wayness [2] [15] are investigated.

Only very few people took this latter approach, which somehow naturally leads to Boolean functions and unrestricted circuit complexity (c.f. [8] [6]). Boyack [3] proved that, in memoryless circuits, every linear permutation has exactly the same complexity as its inverse (memoryless circuits being circuits whose width never exceeds their input size). This emphasises the importance of circuit-width or 'lasting' redundancy for one-wayness, an implication that has never been pointed out explicitly (see also [11], for a different result supporting this same implication). Boyack also constructed the first examples of permutations F that provably satisfy $C(F^{-1}) \neq C(F)$, where $C(.)$ denotes unrestricted circuit complexity (for a precise definition of $C(.)$ we refer to the next section). Later, Hiltgen *et al.* [9] determined the smallest example of a permutation that provably satisfies $C(F^{-1}) \neq C(F)$ and, in [7] [8], constructed the first families $\{F_n\}$ of linear and non-linear permutations that are *feebly one-way of order* 2, i.e., that provably satisfy $\lim_{n\to\infty}[C(F_n^{-1})/C(F_n)] = 2$. Although this feeble one-wayness is much too weak to be relevant to practice, Hiltgen defined *practical one-wayness of order* $\lim_{n\to\infty}[\log_2(C(F^{-1}))/\log_2(C(F))]$ and pointed out that practical one-wayness of a small order (say 4) would suffice for practical applications, that practical one-wayness of order infinity, however, is what people usually look after. Finally, Massey [11] pointed out that, because virtually all permutations have nearly the same complexity, also for practical input sizes n, permutations with more than feeble one-wayness must be very rare.

In this paper we continue research along these lines. In doing so, we focus on permutations and more specifically on t-linear permutations, i.e., linear permutations with a triangular matrix description (for a more precise definition, we refer to the next section). T-linear permutations are very easy to handle, under various aspects, and give interesting insights into some questions of fundamental importance. In Section 2, unrestricted circuit complexity is defined and a direct relation between linear and t-linear permutations is recalled. We also upperbound the complexity of t-linear permutations which can be almost quadratic in the number of input variables. Section 3 addresses the one-wayness of t-linear permutations. By a novel approach, we first show that every single t-linear permutation can be characterised by a finite-length sequence of t-linear permutations. Then, based on this sequence we establish the existence of a particular trade-off between the one-wayness and the complexity of these permutations. This enables us to prove that $C(F^{-1})/C(F)$ is upperbounded by $16\sqrt{n}$ and that this upper bound strengthens to a constant, as the complexity of the inverse permutation increases. Because of Lemma 4, this actually implies that the order of practical one-wayness, for any family of t-linear permutations, is upperbounded by $\frac{3}{2}$. In Section 4, direct implications for linear and non-linear permutations are discussed. Section 5, comments on the only possible origins of one-wayness, in the case of t-linear permutations and in the case of linear permutations. This yields necessary and sufficient conditions for the construc-

tion of linear permutations with practical one-wayness [7] [8], leaving open the satisfiability of these conditions. Section 6 finally concludes by resuming some results and open problems and by commenting their relevance to cryptography.

2 Definitions and Preliminaries

Let $B_{n,m}$ denote the set of Boolean functions $F : \{0,1\}^n \to \{0,1\}^m$. B_n is used as shorthand notation for $B_{n,1}$. We consider realisations of Boolean functions by B_2-circuits [17, Section 1.3], i.e., by acyclic logical gate circuits, where the n Boolean input variables X_i and the two constants **0** and **1** are the only valid inputs to the circuit, and where each gate may compute any 1-output operation from the *basis* B_2 (operation set). The *size* or complexity of a B_2-circuit is the number of its gates and the *unrestricted circuit complexity* $C(F)$ of a function F is the smallest number of gates in a B_2-circuit computing F. It will be called simply complexity in what follows. The direct product $F \times G$, where $F \in B_{n,n}$ and $G \in B_{n,n}$ are functions that depend on disjoint sets of input variables, is used also in Section 5 as a shorthand notation for $[F(X), G(Y)] \in B_{2n,2n}$.

A function $F \in B_{n,n}$ is said now to be *linear* if each of its n component functions in $B_{n,1}$ is defined by an exor-sum of input variables, i.e., an exor-sum of linear terms only. There is a one-to-one correspondence between linear functions $F \in B_{n,n}$ and binary $n \times n$ matrices $[F]$ that issues from the following matrix description for F,

$$Z = [F] \cdot X,$$

where X and Z denote input and output (column) vectors, respectively, and '$\cdot$' denotes matrix multiplication in the Galois field $GF(2)$. In what follows, we will omit the '$\cdot$' whenever the context allows it, and we will interchangeably work with F and $[F]$, using F when dealing with complexities and $[F]$ when exploiting matrix properties. The *inverse* of F, when it exists, will be denoted by F^{-1} or $[F^{-1}]$, accordingly.

It is a fact, that F is invertible if and only if $\det[F] \equiv 1 \pmod 2$, i.e., if the determinant of $[F]$ is odd. It is a fact also that every $[F]$ decomposes, in a usually non-unique way, by Gaussian elimination into a product of four binary matrices

$$[F] = [P_a][L][U][P_b],$$

where $[L]$ is a lower triangular matrix, $[U]$ is an upper triangular matrix and $[P_a]$, $[P_b]$ are variable-permuting matrices. Obviously, P_a and P_b have zero complexity. The complexities of F, L and U are related as follows.

Lemma 1. *For any F, L and U defined as above,*

$$(i) \quad C(F) \leq C(L) + C(U) \qquad (ii) \quad C(F^{-1}) \leq C(L^{-1}) + C(U^{-1})$$

Proof. Let D be defined by $[D] = [P_a^{-1}][F][P_b^{-1}] = [L][U]$. Then obviously, $C(D) = C(F)$. (i) now follows from the fact that cascading circuits for $[L]$ and $[U]$ yields a circuit for $[D]$. The proof for (ii) is analogous. □

Although the explicit characterisation of invertible functions appears to be a rather challenging problem in the general case of linear functions F, it is known to be very easy in the particular case of *t-linear functions* T, i.e., in the case of linear functions with a triangular matrix description $[T]$. The determinant of a triangular matrix indeed corresponds to the product of its diagonal elements, so that a binary triangular matrix is invertible if and only if its diagonal elements are all equal to 1. The functions corresponding to such invertible triangular matrices will be called *t-linear permutations* in what follows.

Every 'lower' triangular matrix maps to an 'upper' triangular matrix by reversing the order of its rows and columns. As this does not affect the complexity of the associated t-linear function, we restrict our further complexity investigations to (upper) t-linear permutations only. The following upper bound on the complexity of a t-linear permutation is also of interest.

Lemma 2. *For any t-linear permutation* $T \in B_{n,n}$, $n \geq 4$,

$$C(T) < \frac{n^2}{\lfloor \log_2(n) - 1 \rfloor}$$

A proof for this result is given in the appendix. From a standard counting argument, it follows that the bound is asymptotically optimal up to constant factor 2. T-linear as well as linear permutations therefore bear the potential for practical one-wayness, as introduced in [7] [8].

3 Limits on One-Wayness

We start by extending our notation for linear functions from F and $[F]$ to F_μ and $[F_\mu]$, respectively, so that an additional index $\mu \geq 1$ refers to F_μ being a linear function in $B_{2^\mu,2^\mu}$. This is not a real restriction, as any function $F \in B_{n,n}$, $n \geq 2$, can be mapped to a function $F_\mu \in B_{2^\mu,2^\mu}$, with $\mu = \lceil \log_2(n) \rceil$, $C(F_\mu) = C(F)$ and $C(F_\mu^{-1}) = C(F^{-1})$, by adding only *futile* component functions, i.e., component functions that are equal to an input variable not occurring in the definition of any other component function. The *one-wayness* ow_{F_μ} of a permutation F_μ is defined then by

$$\mathrm{ow}_{F_\mu} = \begin{cases} C(F_\mu^{-1})/C(F_\mu) & \text{if } C(F_\mu) > 0, \\ 1 & \text{if } C(F_\mu) = 0 \quad (\Rightarrow C(F_\mu^{-1}) = 0). \end{cases}$$

Observe now that the matrix corresponding to an (upper) t-linear permutation T_μ decomposes as follows

$$[T_\mu] = \begin{bmatrix} [\vartheta_{\mu-1}] & [\lambda_{\mu-1}] \\ [0_{\mu-1}] & [\tau_{\mu-1}] \end{bmatrix}, \tag{1}$$

where $\vartheta_{\mu-1}$ and $\tau_{\mu-1}$ are (upper) t-linear permutations, $\lambda_{\mu-1}$ is a linear function and $0_{\mu-1}$ is the zero function. The matrix corresponding to the inverse permutation therefore allows for the following description

$$[T_\mu^{-1}] = \begin{bmatrix} [\vartheta_{\mu-1}^{-1}] & [\vartheta_{\mu-1}^{-1}][\lambda_{\mu-1}][\tau_{\mu-1}^{-1}] \\ [0_{\mu-1}] & [\tau_{\mu-1}^{-1}] \end{bmatrix}.$$

Two preliminary results about t-linear permutations are resumed in the following lemmas. They will be helpful for what follows.

Lemma 3. *Let T_μ be any t-linear permutation, with a decomposition as defined in (1). Then*

$$C(T_\mu) \geq \max[C(\vartheta_{\mu-1}),\ C(\tau_{\mu-1}),\ C(\lambda_{\mu-1})],$$
$$C(T_\mu^{-1}) \leq C(\vartheta_{\mu-1}^{-1}) + C(\tau_{\mu-1}^{-1}) + C(\lambda_{\mu-1}) + 2^{\mu-1}.$$

Proof. Any circuit for T_μ can be used as a circuit for $\vartheta_{\mu-1}$, $\tau_{\mu-1}$ or $\lambda_{\mu-1}$ simply by discarding extra outputs and by fixing extra input variables to zero. This can only reduce complexity and therefore yields the first inequality.

The second inequality follows from the fact that the combination of the next four circuits always yields a circuit for $Z = [T_\mu^{-1}] \cdot X$:

$$Z2 = [\tau_{\mu-1}^{-1}] \cdot X2, \qquad I2 = X1 \oplus_{\mu-1} I1,$$
$$I1 = [\lambda_{\mu-1}] \cdot Z2, \qquad Z1 = [\vartheta_{\mu-1}^{-1}] \cdot I2,$$

$X1, X2$ and $Z1, Z2$ denoting the upper and lower halves of X and Z, respectively, $I1, I2$ denoting intermediate results and '$\oplus_{\mu-1}$' denoting component wise exor-addition of two length $2^{\mu-1}$ vectors, so that $C(\oplus_{\mu-1}) = 2^{\mu-1}$. □

Lemma 4. *From every t-linear permutation T_μ, with $C(T_\mu) \leq 2^{\mu-2}$, it is possible to obtain a unique t-linear permutation $T_{\mu-1}$, with*

$$C(T_{\mu-1}) = C(T_\mu) \quad \text{and} \quad C(T_{\mu-1}^{-1}) = C(T_\mu^{-1}),$$

by discarding the first $2^{\mu-1}$ of its futile component functions.

Proof. Eliminating a futile component function does not change the complexities of T_μ and T_μ^{-1}. We therefore only need to prove that there are sufficiently many of these component functions. From the upper bound $C(T_\mu) \leq 2^{\mu-2}$ it follows that at most half of the 2^μ input variables can be an input to one of the at most $2^{\mu-2}$ 2-input/1-output gates in the circuit. Moreover, from the invertibility of T_μ, every input variable has to affect at least one output. Therefore, at least $2^{\mu-1}$ input variables only affect the single output to which they are directly fed through. □

The next definition is at the very origin of our new approach. It allows us to convert a single permutation into a finite sequence of permutations, from which surprising limits and observations on the one-wayness of these permutations can be deduced.

Definition 5. Let T_μ be any t-linear permutation, with a decomposition as defined in (1). We define the *most-complex-inverse decomposition sequence of* T_μ, MCIDS_{T_μ}, to be the unique finite-length sequence $\{T_\mu, T_{\mu-1}, \ldots, T_1\}$ of t-linear permutations T_ν satisfying: For $\nu = \mu \ldots 2$,

if $C(T_\nu) \leq 2^{\nu-2}$, then $T_{\nu-1}$ is obtained according to Lemma 4,

if $C(T_\nu) > 2^{\nu-2}$, then, if $C(\vartheta_{\nu-1}^{-1}) > C(\tau_{\nu-1}^{-1})$, then $T_{\nu-1} = \vartheta_{\nu-1}$, else $T_{\nu-1} = \tau_{\nu-1}$.

This essentially corresponds to recursively defining $T_{\nu-1}$ to be the t-linear component, $\vartheta_{\nu-1}$ or $\tau_{\nu-1}$, of T_ν that has the most complex inverse. Two immediate implications from that definition, that will be used in the following, are $C(T_{\nu-k}) \leq C(T_\nu)$, for $0 < k < \nu$, and $\max[C(\vartheta_{\nu-1}^{-1}),\ C(\tau_{\nu-1}^{-1})] = C(T_{\nu-1}^{-1})$.

Lemma 6. *Let T_μ be any t-linear permutation, with $C(T_\mu) > 2^{\mu-2}$ and with a decomposition as defined in (1). Then,*

$$C(\lambda_{\mu-1}) \geq \max[C(\vartheta_{\mu-1}^{-1}),\ C(\tau_{\mu-1}^{-1})] \quad \Rightarrow \quad \mathrm{ow}_{T_\mu} < 5.$$

Proof. For $C(T_\mu) > 2^{\mu-2}$, the above assumption, together with Lemma 3, yields $C(T_\mu^{-1}) < 3C(\lambda_{\mu-1}) + 2C(T_\mu)$. From Lemma 3, we further know that $C(T_\mu) \geq C(\lambda_{\mu-1})$, so that $\mathrm{ow}_{T_\mu} = C(T_\mu^{-1})/C(T_\mu) < 5$. □

The case of real interest therefore only occurs when $C(\lambda_{\mu-1}) < \max[C(\vartheta_{\mu-1}^{-1}), C(\tau_{\mu-1}^{-1})]$. Note that Lemma 6 holds independently of the possible one-wayness of any of the component permutations $\vartheta_{\mu-1}$, $\tau_{\mu-1}$ of T_μ. This clearly demonstrates how easily one-wayness can be destroyed. It also indicates that any t-linear permutation T_μ, whose inverse T_μ^{-1} has near maximum complexity, cannot be very one-way, as T_μ^{-1} can only have near maximum complexity if $\lambda_{\mu-1}$ has near maximum complexity as well. A proof for this and other implications follows from the next theorem and corollary which state our main result.

Theorem 7. *Let T_ν and $T_{\nu-k}$ be two t-linear permutations from any* MCIDS_{T_μ}, *with $1 < \nu \leq \mu$, $0 < k < \nu$ and $C(T_\nu) > 0$. Then,*

$$\begin{aligned} C(T_{\nu-1}^{-1}) &> \tfrac{1}{2}C(T_\nu^{-1}) - \tfrac{3}{2}C(T_\nu) = (\tfrac{1}{2}\mathrm{ow}_{T_\nu} - \tfrac{3}{2}) \cdot C(T_\nu), \\ C(T_{\nu-k}^{-1}) &> \tfrac{1}{2^k}C(T_\nu^{-1}) - 3C(T_\nu) = (\tfrac{1}{2^k}\mathrm{ow}_{T_\nu} - 3) \cdot C(T_\nu). \end{aligned}$$

Proof. If $C(T_\nu) \leq 2^{\nu-2}$, it follows from Lemma 4 and Definition 5 that $C(T_{\nu-1}^{-1}) = C(T_\nu^{-1})$. On the other hand, if $C(T_\nu) > 2^{\nu-2}$, it follows from Lemma 3 and Definition 5 that

$$\begin{aligned} C(T_\nu^{-1}) &< 2\ C(T_{\nu-1}^{-1}) + C(\lambda_{\nu-1}) + 2\ C(T_\nu) \\ &\leq 2\ C(T_{\nu-1}^{-1}) + 3\ C(T_\nu). \end{aligned}$$

It is true therefore, in general, that

$$\begin{aligned} C(T_{\nu-1}^{-1}) &> \tfrac{1}{2}C(T_\nu^{-1}) - \tfrac{3}{2}C(T_\nu) \\ &= (\tfrac{1}{2}\mathrm{ow}_{T_\nu} - \tfrac{3}{2}) \cdot C(T_\nu). \end{aligned}$$

From the recursive nature of Definition 5, we further deduce that

$$\begin{aligned} C(T_{\nu-k}^{-1}) &> \tfrac{1}{2^k}C(T_\nu^{-1}) - 3\,(\tfrac{C(T_{\nu-k+1})}{2} + \tfrac{C(T_{\nu-k+2})}{4} + \ldots + \tfrac{C(T_\nu)}{2^k}) \\ &> \tfrac{1}{2^k}C(T_\nu^{-1}) - 3C(T_\nu) \\ &= (\tfrac{1}{2^k}\mathrm{ow}_{T_\nu} - 3) \cdot C(T_\nu). \end{aligned}$$

□

Note that, because $C(T_{\nu-k}) \leq C(T_\nu)$, for $0 < k < \nu$ (c.f. Definition 5), the inequalities of Theorem 7 remain valid also if we divide their right sides by $C(T_\nu)$ and their left sides by $C(T_{\nu-1})$ and $C(T_{\nu-k})$, respectively. This yields the following corollary.

Corollary 8. *Let T_ν and $T_{\nu-k}$ be two t-linear permutations from any* MCIDS_{T_μ}, *with $1 < \nu \leq \mu$, $0 < k < \nu$ and $C(T_\nu) > 0$. Then,*

$$\begin{aligned} \mathrm{ow}_{T_{\nu-1}} &> \tfrac{1}{2}\mathrm{ow}_{T_\nu} - \tfrac{3}{2} \\ \mathrm{ow}_{T_{\nu-k}} &> \tfrac{1}{2^k}\mathrm{ow}_{T_\nu} - 3. \end{aligned}$$

Two fundamental restrictions, both with regard to most-complex-inverse decomposition sequences MCIDS_{T_μ}, therefore hold: firstly, one-wayness can decrease at most linearly with the number of input variables; secondly, the complexity of the inverse permutations can decrease at most linearly with the number of input variables, as long as one-wayness is larger than or equal to 5. The next two theorems are direct consequences of these restrictions and Lemma 2.

Theorem 9. *Let T_μ be any t-linear permutation and let $n = 2^\mu$ denote the number of input variables on which it depends. Then,*

$$ow_{T_\mu} < 16\sqrt{n}/\Delta_n,$$

with $\Delta_n = \max[1, \sqrt{\tfrac{1}{2}\log_2(n) - 2}\,]$.

Proof. Let ow_{T_μ} be described by $2^{\alpha\mu+3}$. For $\mu = 1$, only $\alpha < 0$ is possible (all t-linear permutations T_1 being involutions), and for $\alpha \leq 0$, $\mu \geq 1$, the theorem holds trivially. We may therefore assume in the following that $\mu \geq 2$ and $\alpha \geq 0$.

Suppose now first that $C(T_\mu) > 2^{\mu-2}$. It follows then from Corollary 8, that $k_o = \lfloor \alpha\mu+1 \rfloor \leq \alpha\mu+1$ steps in MCIDS_{T_μ} are insufficient to completely eliminate one-wayness, so that $\mu - k_o \geq 2$; all T_1 being involutions. From Theorem 7 and the lower bound on $C(T_\mu)$, we further deduce that

$$C(T^{-1}_{\mu-k_o}) > C(T_\mu) > 2^{\mu-2},$$

while the monotonicity, for $\mu - k_o \geq 2$, of the upper bound obtained from Lemma 2, together with the fact that $k_o > \alpha\mu$, implies that

$$C(T^{-1}_{\mu-k_o}) < \tfrac{2^{2\mu-2k_o}}{\mu-k_o-1} < 2^{2\mu-2\alpha\mu-\log_2(\mu-\alpha\mu-1)}.$$

Both inequalities together yield

$$\begin{aligned} 2\alpha\mu &< \mu + 2 - \log_2(\mu - \alpha\mu - 1) \\ &< \mu + 2 - \log_2(\max[1, \tfrac{1}{2}\mu - 2]), \end{aligned}$$

where the max[.]-expression results from either directly substituting $\mu - \alpha\mu > \mu - k_o \geq 2$, or first using this bound to obtain $\alpha\mu < \frac{1}{2}\mu + 1$ from the next to last inequality and then substituting this latter bound. This proves that

$$\alpha\mu < 1 + \tfrac{1}{2}(\mu - \log_2(\max[1, \tfrac{1}{2}\mu - 2])),$$

and consequently, that

$$\mathrm{ow}_{T_\mu} = 2^{\alpha\mu+3} < 16\sqrt{n}/\max[1,\ \sqrt{\tfrac{1}{2}\log_2(n) - 2}\,]. \tag{2}$$

The case $C(T_\mu) \leq 2^{\mu-2}$ is dealt with analogously. From Lemma 4, we know that we can reduce μ until, for some $\nu < \mu$, either $C(T_\nu) > 2^{\nu-2}$ and $\nu \geq 2$, so that

$$\mathrm{ow}_{T_\mu} = \mathrm{ow}_{T_\nu} = 2^{\alpha\nu+3} < 16\sqrt{n'}/\max[1,\ \sqrt{\tfrac{1}{2}\log_2(n') - 2}\,], \qquad n' = 2^\nu < n,$$

or $\nu = 1$, in which case $\mathrm{ow}_{T_\mu} = \mathrm{ow}_{T_1} = 1$. The monotonicity, with regard to n, of the upper bound in (2) finally implies that the result holds in general. □

Theorem 10. *Let T_μ be any t-linear permutation, and let $n = 2^\mu$ denote the number of input variables on which it depends. Then, for any possible α,*

$$\mathrm{ow}_{T_\mu} \geq 8n^\alpha \quad \Rightarrow \quad \begin{cases} C(T_\mu) & < \dfrac{n^{2-2\alpha}}{\log_2(n^{1-\alpha}) - 1} & < n^{2-2\alpha}/\Delta_n^2, \\ C(T_\mu^{-1}) & < \dfrac{8n^{2-\alpha}}{\log_2(n^{1-\alpha}) - 1} & < 8n^{2-\alpha}/\Delta_n^2, \end{cases}$$

with $\Delta_n = \max[1,\ \sqrt{\tfrac{1}{2}\log_2(n) - 2}\,]$.

Proof. Let ow_{T_μ} be described by $2^{\alpha\mu+3}$. For $\mu = 1$, only $\alpha < 0$ is possible (all t-linear permutations T_1 being involutions), and for $\alpha \leq 0$, $\mu \geq 1$, the theorem holds trivially. We may therefore assume in the following that $\mu \geq 2$ and $\alpha \geq 0$.

Suppose now first that $C(T_\mu) > 2^{\mu-2}$. Then, by exactly the same derivations as in the proof of the previous theorem, we get that

$$C(T_\mu) < C(T^{-1}_{\mu-k_o}) < \tfrac{2^{2\mu-2\alpha\mu}}{\mu-\alpha\mu-1} = \tfrac{n^{2-2\alpha}}{\log_2(n^{1-\alpha})-1}. \tag{3}$$

Theorem 7, the previous upper bounds on $C(T_\mu)$ and $C(T^{-1}_{\mu-k_o})$, and the fact that $k_o \leq \alpha\mu + 1$ further yield

$$\begin{aligned} C(T_\mu^{-1}) &< 2^{k_o} \cdot (C(T^{-1}_{\mu-k_o}) + 3C(T_\mu)) \\ &< 2^{k_o+2} \cdot C(T^{-1}_{\mu-k_o}) \\ &< 8n^\alpha \cdot \tfrac{n^{2-2\alpha}}{\log_2(n^{1-\alpha})-1}. \end{aligned} \tag{4}$$

The weaker bounds finally result from the fact that the derivations in the proof of Theorem 9 showed that $\alpha < \min[1 - \frac{2}{\mu},\ \frac{1}{2} + \frac{1}{\mu}]$, so that

$$\log_2(n^{1-\alpha}) - 1 > \max[1,\ \tfrac{1}{2}\log_2(n) - 2] = \Delta_n^2,$$

with Δ_n defined as in Theorem 9.

The case $C(T_\mu) \leq 2^{\mu-2}$ is dealt with analogously, yielding either the same upper bounds, for some $n' = 2^\nu < n$, $\nu \geq 2$, or $\mathrm{ow}_{T_\mu} = \mathrm{ow}_{T_1} = 1$, i.e., $\alpha < 0$. The monotonicity, with regard to n, of the upper bounds in (3) and (4) finally implies that the result holds in general. □

Here we observe that, for any t-linear permutation T_μ, not only its one-wayness ow_{T_μ} is non-trivially upper bounded, but, for any lower bound on that one-wayness, its complexity and the complexity of its inverse are non-trivially upper bounded as well. This shows, in particular, that any potential candidate for a t-linear permutation T_μ with near maximum one-wayness $\mathrm{ow}_{T_\mu} \geq 8\sqrt{n}/\Delta_n$ would have to satisfy $C(T_\mu) < n$ and $C(T_\mu^{-1}) < 8n^{3/2}/\Delta_n$. The following converse is therefore of interest as well.

Converse to Theorem 9 and Theorem 10. *Let T_μ be any t-linear permutation and let $n = 2^\mu$ denote the number of input variables on which it depends. Then, for any possible β,*

$$C(T_\mu) \geq n^\beta \quad \Rightarrow \quad \mathrm{ow}_{T_\mu} < \min[8n^{1-\beta/2}/\Delta_n,\ 16n^{1/2}/\Delta_n],$$

$$C(T_\mu^{-1}) \geq n^\beta \quad \Rightarrow \quad \mathrm{ow}_{T_\mu} < \min[64n^{2-\beta}/\Delta_n^2,\ 16n^{1/2}/\Delta_n],$$

with $\Delta_n = \max[1,\ \sqrt{\frac{1}{2}\log_2(n) - 2}\ ]$.

This essentially follows from the weaker bounds in Theorem 10, by using $\beta = 2-2\alpha-2\log_2(\Delta_n)/\log_2(n)$ and $\beta = 2-\alpha+(3-2\log_2(\Delta_n))/\log_2(n)$, respectively. It shows, in particular, that any t-linear permutation T_μ, $n = 2^\mu$, whose inverse has near maximum complexity $C(T_\mu^{-1}) = n^2/(c\log_2(n))$, c a constant, is forced to have one-wayness $\mathrm{ow}_{T_\mu} < 64c\log_2(n)/\Delta_n^2 < 384c$, i.e., one-wayness upperbounded by an expression that does not dependent on n.

We conclude this section by pointing out that, although linear permutations with $C(F) \neq C(F^{-1})$ have been demonstrated to exist [7], the existence of t-linear permutations with $C(T) \neq C(T^{-1})$ is still an open problem.

4 Implications for Linear and Non-linear Permutations

• The implications for *linear* permutations directly follow from the decomposition

$$[F] = [P_a][L][U][P_b], \tag{5}$$

described in Section 2 (P_a and P_b being variable-permuting matrices), and the complexity relations derived in Lemma 1. We here only introduce, for $C(L \circ U) \neq 0$,

$$\delta_{LU} = \frac{C(L)+C(U)}{C(L \circ U)} \quad \text{and} \quad \delta_{LU^-} = \frac{C(L^{-1})+C(U^{-1})}{C((L \circ U)^{-1})},$$

which we call the *decomposition-loss factors* of LU and LU^- ('$\circ$' denoting functional composition). These factors characterise the circuit inefficiencies that result when realising the linear permutations $L \circ U$ and $(L \circ U)^{-1}$ by cascading circuits for their t-linear components. Note that such realisations, once in between, force circuit-width to equal input size and redundancy to vanish.

Lemma 11. *Let F be any linear permutation, with $C(F) > 0$. Then, for every decomposition (5) of F,*

$$\mathrm{ow}_F = \left(\frac{C(L)}{C(F)} \cdot \mathrm{ow}_L + \frac{C(U)}{C(F)} \cdot \mathrm{ow}_U\right) / \delta_{LU^-}$$

with $\delta_{LU^-} \geq 1$.

Proof. Obviously, for $[D] = [P_a^{-1}][F][P_b^{-1}] = [L][U]$, the complexities of F and F^{-1} satisfy $C(F) = C(D)$ and $C(F^{-1}) = C(D^{-1})$, respectively. The result then follows from the definitions of ow_F and δ_{LU^-}, yielding

$$\mathrm{ow}_F = \frac{C(F^{-1})}{C(F)} = \left(\frac{C(L^{-1})}{C(F)} + \frac{C(U^{-1})}{C(F)}\right) / \delta_{LU^-}.$$

We only additionally substitute $C(L) \cdot \mathrm{ow}_L$ and $C(U) \cdot \mathrm{ow}_U$ for $C(L^{-1})$ and $C(U^{-1})$, respectively. The lower bound on δ_{LU^-} follows from Lemma 1 (ii). □

Lemma 12. *Let F be any linear permutation, with $C(F) > 0$. Then, for every decomposition (5) of F,*

$$\mathrm{R}_{LU} \cdot \min[\mathrm{ow}_L, \mathrm{ow}_U] \leq \mathrm{ow}_F \leq \mathrm{R}_{LU} \cdot \max[\mathrm{ow}_L, \mathrm{ow}_U],$$

where $\mathrm{R}_{LU} = \delta_{LU}/\delta_{LU^-}$, with $\delta_{LU} \geq 1$ and $\delta_{LU^-} \geq 1$.

Proof. This follows directly from the previous lemma. The lower bound on δ_{LU} is a consequence of Lemma 1 (i). □

The decomposition-loss factors thus play a fundamental role in relating the maximum one-wayness of linear permutations to the maximum one-wayness of t-linear permutations. Note that the one-wayness of a linear permutation can only become significantly larger than the one-wayness of a t-linear permutation, if the *decomposition-loss ratio*, $\mathrm{R}_{LU} = \delta_{LU}/\delta_{LU^-}$, can become significantly larger than 1, and that a necessary condition for this to happen is that the decomposition-loss factor δ_{LU} can become significantly larger than 1. An example where R_{LU} and δ_{LU} differ from 1 is given in the appendix. Whether they can be much larger than $\frac{3}{2}$, however, remains an open problem.

• The implications for *non-linear* permutations follow from a different observation, namely, that the existence of a most-complex-inverse decomposition sequence in fact does not require the permutation T_μ to be linear. As long as $Z = T_\mu(X)$ recursively decomposes as follows:

$$\begin{array}{lll} Z1 = \vartheta_{\mu-1}(X1) & \oplus_{\mu-1} & \lambda_{\mu-1}(X2) \\ Z2 = & & \tau_{\mu-1}(X2), \end{array}$$

with $X1, X2$ and $Z1, Z2$ denoting the upper and lower halves of X and Z, respectively, the MCIDS_{T_μ} exists and neither $\lambda_{\mu-1}(X2)$ nor $\tau_{\mu-1}(X2)$ (assuming $C(\vartheta_{\mu-1}^{-1}) > C(\tau_{\mu-1}^{-1})$ in this particular step) needs to satisfy any linearity or dependence requirements. Thus, if these functions were to be both non-linear (or non-t-linear) this would not affect the validity of Theorem 7, nor would it affect that of Corollary 8. The decomposition in itself limits one-wayness to $n/2+3$, whereby the complexity of T_μ^{-1} can be exponential in n (through $\lambda_{\mu-1}$). More involved generalisations to non-linear permutations are possible as well. They will be discussed in a separate paper.

5 Origins of One-Wayness

We know already from Section 3 that, within a most-complex-inverse decomposition sequence, one-wayness can decrease at most by a factor of 2, when the number of input variables decreases by a factor of 2. No evidence has been given, however, that any decrease at all can occur. The next discussion therefore emphasises the eventually unusual conditions that would have to be satisfied, for a decrease by a factor of 2 to occur. For simplicity reasons, we will assume that the component function $\lambda_{\nu-1}$, which needs to satisfy $C(\lambda_{\nu-1}) < 2\max[C(\vartheta_{\nu-1}),\ C(\tau_{\nu-1})]$ in order to allow for any decrease at all, equals the zero function $0_{\nu-1}$. Under this still rather general setting, the first inequality in Corollary 8 simplifies to

$$\mathrm{ow}_{T_{\nu-1}} \geq \tfrac{1}{2}\mathrm{ow}_{T_\nu},$$

with equality if and only if $C(T_\nu^{-1}) = 2\,C(T_{\nu-1}^{-1})$ and $C(T_\nu) = C(T_{\nu-1})$. This shows that one-wayness can only decrease by a factor of 2, if

$$C(\vartheta_{\nu-1}^{-1} \times \tau_{\nu-1}^{-1}) = 2\max[C(\vartheta_{\nu-1}^{-1}),\ C(\tau_{\nu-1}^{-1})],$$
$$C(\vartheta_{\nu-1} \times \tau_{\nu-1}) = \max[C(\vartheta_{\nu-1}),\ C(\tau_{\nu-1})] = C(T_{\nu-1}),$$

which implicitly requires $C(\vartheta_{\nu-1}^{-1}) = C(\tau_{\nu-1}^{-1})$ and $C(\vartheta_{\nu-1}) = C(\tau_{\nu-1})$. The case $\min[C(\vartheta_{\nu-1}),\ C(\tau_{\nu-1})] < \max[C(\vartheta_{\nu-1}),\ C(\tau_{\nu-1})]$ is indeed of no real interest, as it implies $\mathrm{ow}_{T_\nu} < \max[\mathrm{ow}_{\vartheta_{\nu-1}},\ \mathrm{ow}_{\tau_{\nu-1}}]$. We therefore observe that *a one-wayness decrease of interest (or increase of interest, from a constructive point of view) can only occur:* if $\vartheta_{\nu-1}$ and $\tau_{\nu-1}$ have almost the same complexity and almost the same one-wayness, and if their common realisation on disjoint sets of variables allows for extensive savings, while the common realisation of their inverses, also on disjoint sets of variables, does not allow for any significant savings at all. Whether this can be satisfied, simultaneously (and repeatedly), remains an open problem, although it suggests a negative conjecture.

It seems important here to briefly point out that a related problem, namely, whether for any function F it is possible to have $C(F \times F) < 2\,C(F)$, has been addressed by Paul [13] and also Uhlig [16], many years ago. Paul, in particular, describes how a result like the next one easily follows by contradiction.

Theorem 13. *For any $\epsilon > 0$, there are values of n, such that there exist t-linear permutations $T \in B_{n,n}$ that satisfy*

$$C(T \times T) < (1+\epsilon)\,2^{\omega-2} \cdot C(T),$$

where ω is the smallest exponent such that multiplication of two $N \times N$ matrices can be performed with $N^{\omega+o(1)}$ gates.

From a paper by Coppersmith *et al.* [4], we know that $\omega < 2.376$. Strassen [14] even expects much smaller $\omega \geq 2$ to be possible.

We conclude this section by recalling that, even if t-linear permutations could not be practically one-way, the decomposition-loss ratio introduced in the previous section remains another potential independent source of one-wayness for linear permutations. The example in the appendix, in particular, illustrates that this ratio can be greater than 1, even if $\mathrm{ow}_U = \mathrm{ow}_L = 1$.

6 Conclusions and Open Problems

The unrestricted-circuit-complexity approach to provable practical one-wayness bears certain advantages that should have become clear form the results achieved in [3] [7] [8] [11] and in this paper. It has enabled us to realise the importance of circuit-width or 'lasting' redundancy for one-wayness, as it has enabled us to construct the first examples of linear and non-linear permutations F, with $C(F^{-1}) \approx 2\,C(F)$. More specifically in this paper, it has allowed us to demonstrate the first non-trivial upper bounds on one-wayness and to describe necessary and sufficient conditions for the construction of linear permutations with practical one-wayness. Nevertheless, many open problems remain:

Open Problem 1. *Is there any t-linear permutation T with $C(T^{-1}) \neq C(T)$?*

Open Problem 2. *Is there any t-linear permutations T_μ with $\mathrm{ow}_{T_\mu}/\mathrm{ow}_{T_{\mu-1}} \approx 2$, or can this upper bound be strengthened in general?*

Open Problem 3. *Are there any t-linear permutations $L, U \in B_{n,n}$ for which $\mathrm{R}_{LU} \approx 4n/\log_2(n)$, or can this upper bound be strengthened in general?*

Open Problem 4. *What influence do permanent or temporary circuit-width (or redundancy) restrictions have on complexity and on one-wayness?*

Today, we perfectly understand to what extend cryptography relies on the existence of one-wayness. The relevance of the above questions to cryptography therefore should be clear. But, what about the relevance of the above approach? Despite our full recognition for the contributions of the classical Turing-Machine-complexity approach to the field, we are seriously concerned by the fact that this classical approach so far failed to produce concrete structural insight into the possible origins of one-wayness, and thus also failed to motivate research in this topic.

This yields the justification for the non-classical unrestricted-circuit-complexity approach taken in this paper. Unrestricted circuit complexity allows for the stronger (less restricted) type of cryptanalytic adversary. More important, its natural dealing with Boolean functions considerably facilitates structural investigations by means of subfunctions and/or component functions, an interesting technique that, to our opinion, bears the potential for significantly improving our understanding of one-wayness. We believe that our results and those in the referenced papers do support these reflections. Hopefully, they can also motivate further research.

Acknowledgements

The author is especially grateful to J. Ganz and X. Lai for the many helpful and clarifying discussions.

References

1. V. L. Arlazarov, E. A. Dinic, M. A. Kronrod, and I. A. Faradžev, "On economical construction of the transitive closure of an oriented graph," *Dokl. Akad. Nauk*, vol. 194, pp. 487–488, 1970. Engl. Transl.: Sov. Math. Dokl., vol. 11, pp. 1209–1210, 1970.
2. R. B. Boppana and J. C. Lagarias, "One-way functions and circuit complexity," *Information and Computation*, vol. 74, pp. 226–240, 1987. Conf. version: *Proc. 1st Ann. IEEE Symp. Structure in Complexity Th.*, pp. 51–65, 1986.
3. S. W. Boyack, *The Robustness of Combinatorial Measures of Boolean Matrix Complexity*. Ph.D. thesis, Massachusetts Inst. of Techn., 1985.
4. D. Coppersmith and S. Winograd, "Matrix multiplication via arithmetic progressions," *J. Symbolic Comput.*, vol. 9, pp. 251–280, 1990. Conf. version: *Proc. 19th Ann. ACM Symp. Theory of Comput.*, pp. 1–6, 1987.
5. W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 6, pp. 644–655, Nov. 1976.
6. S. Goldwasser, "The search for provably secure cryptosystems," in *Cryptology and Computational Number Theory: Proc. Symp. Appl. Math., vol. 42* (C. Pomerance, ed.), pp. 89–113, Providence, RI: Amer. Math. Soc., 1990.
7. A. P. Hiltgen, "Constructions of feebly-one-way families of permutations," *Advances in Cryptology: Proc. Auscrypt'92, Springer*, pp. 422–434, 1993.
8. A. P. Hiltgen, *Cryptographically Relevant Contributions to Combinational Complexity Theory*, vol. 3 of *ETH Series in Information Processing*, ed. J. L. Massey. Konstanz: Hartung-Gorre, 1994. Reprint of: Ph.D. thesis no. 10382, Swiss Federal Institute of Technology, ETH-Zürich, 1993.
9. A. P. Hiltgen and J. Ganz, "On the existence of specific complexity-asymmetric permutations," *Technical Report*, Signal and Inform. Proc. Lab, ETH-Zürich, 1992.
10. R. Impagliazzo and M. Luby, "One-way functions are essential for complexity based cryptography," *Proc. 30th Ann. IEEE Symp. Foundations of Computer Sci.*, pp. 230–235, 1989.
11. J. L. Massey, "The difficulty with difficulty," *A Guide to the Transparencies from the Eurocrypt '96 IACR Distinguished Lecture*, Signal and Inform. Proc. Lab., ETH Zürich, 1996. Available from http://www.iacr.org/conferences/ec96/massey.html.
12. A. Menezes, P. van Orschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC-Press Series on Discrete Mathematics and its Applications, CRC-Press: Boca Raton, 1997.
13. W. J. Paul, "Realizing Boolean functions on disjoint sets of variables," *Theoret. Comput. Sci.*, vol. 2, pp. 383–396, 1976.
14. V. Strassen, "Algebraic complexity theory," in *Handbook of Theoretical Computer Science, vol. A* (J. van Leeuwen, ed.), ch. 11, Amsterdam: Elsevier, 1990.
15. C. Sturtivant and Z. Zhang, "Efficiently inverting bijections given by straight line programs," *Proc. 31th Ann. IEEE Symp. Foundations of Computer Sci.*, pp. 327–334, 1990.
16. D. Uhlig, "On the synthesis of self-correcting schemes from functional elements with a small number of reliable elements," *Matemat. Zametki*, vol. 15, no. 6, pp. 937–944, June 1974. Engl. Transl.: Math. Notes Acad. Sci. USSR, vol. 15, pp. 558–562, 1974.
17. I. Wegener, *The Complexity of Boolean Functions*. New York: Wiley (Stuttgart: Teubner), 1987.

Appendix

Proof for Lemma 2

In order to prove that every t-linear permutation $T \in B_{n,n}$, $n \geq 4$ can be realised by using no more then $n^2/\lfloor \log_2(n) - 1 \rfloor$ gates, we proceed as follows.

First, we divide the n input variables into $\lceil \frac{n}{k} \rceil < \frac{n}{k} + 1$ disjoint sets of size k (a positive integer), so that the first set contains the first k input variables, the second set contains the second k input variables, ... and the last set contains the remaining input variables and possibly also some dummy variables. Then, for each of these sets, we precompute all possible 2^k linear functions in the respective k variables. Note that there exists a circuit that does this with complexity $C_k \leq 2^k - k - 1$, as the $k + 1$ weight-0 and weight-1 functions require no gates to be synthesised, and each weight-k function ($k > 1$) can be synthesised from a single addition of an input variable and a weight-$(k-1)$ function. Finally, for the n component functions, only precomputed functions have to be added. Due to the triangular form of the corresponding matrix, it follows that, there are at most k component functions whose synthesis requires at most $\lceil \frac{n}{k} \rceil - 1$ additional gates, k component functions whose synthesis requires at most $\lceil \frac{n}{k} \rceil - 2$ additional gates, ... and k component functions whose synthesis requires at most 1 additional gate.

Altogether, this describes a general realisation that needs no more than C_T gates, where

$$C_T \leq \lceil \tfrac{n}{k} \rceil \cdot C_k + k \cdot \sum_{i=1}^{\lceil \frac{n}{k} \rceil - 1} i \; < \; (\tfrac{n}{k} + 1) \cdot (2^k - k - 1 + \tfrac{n}{2}).$$

The result follows from substituting $k = \lfloor \log_2(n) - 1 \rfloor \geq 1$, for $n \geq 4$. This general realisation for t-linear functions derives from a general realisation for linear functions, also known as the 'Four Russians' algorithm [1]. □

Linear Permutation $T = L \circ U$ with $\mathbf{R}_{LU} \neq 1$ and $\delta_{LU} \neq 1$

As an example, we consider the function F with matrix description

$$[F] = \begin{bmatrix} 1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0 \\ 1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1 \\ 1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1 \end{bmatrix} \qquad [F^{-1}] = \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,0\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,0\,0\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1 \\ 1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1 \\ 1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,1 \end{bmatrix}$$

This function F, for which it has been proved in [7] that $C(F) = 12$ and $C(F^{-1}) = 15$, decomposes into a product of triangular matrices L and U, defined by

$$[L] = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0 \\ 1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,1 \end{bmatrix} \qquad [L^{-1}] = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0 \\ 1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0 \\ 1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,1 \end{bmatrix},$$

$$[U] = \begin{bmatrix} 1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1 \end{bmatrix} \qquad [U^{-1}] = \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1 \end{bmatrix}$$

It is straight-forward here to verify that $C(L) = C(L^{-1}) = 6$ and $C(U) = C(U^{-1}) = 10$, so that $\mathrm{ow}_L = \mathrm{ow}_U = 1$. Consequently, by Lemma 12, $\mathrm{ow}_F = \mathrm{R}_{LU} = \frac{15}{12} = \frac{5}{4}$, with decomposition-loss factors $\delta_{LU} = \frac{16}{12}$ and $\delta_{LU^-} = \frac{16}{15}$.

By letting n grow, this yields a family of linear permutations, also investigated in [7], for which $\mathrm{ow}_L = \mathrm{ow}_U = 1$ and $\mathrm{ow}_F = \mathrm{R}_{LU} \to \frac{3}{2}$; the respective decomposition-loss factors satisfying $\delta_{LU} \to \frac{3}{2}$ and $\delta_{LU^-} \to 1$. □