Some Facts on Permanents
in Finite Characteristics

Abstract:

The permanent’s polynomial-time computability over fields of characteristic 3 for k-semi-unitary matrices (i.e. n×n-matrices A such that rank(AA^T - I_n) = k) in the case k ≤ 1 and its #_3-P-completeness for any k > 1 (Ref. 9) is a result that essentially widens our understanding of the computational complexity boundaries for the permanent modulo 3. Now we extend this result to study more closely the case k > 1 regarding the (n-k)x(n-k)-sub-permanents (or permanent-minors) of a unitary nxn-matrix and their possible relations, because an (n-k)x(n-k)-sub-matrix of a unitary nxn-matrix is generically a k-semi-unitary (n-k)x(n-k)-matrix.

The following paper offers a way to receive a variety of such equations of different sorts, in the meantime also extending (in the second chapter that is divided onto subchapters) this direction of research to reviewing all the set of polynomial-time permanent-preserving reductions and equations for a generic matrix’s sub-permanents they might yield, including a number of generalizations and formulae (valid in an arbitrary prime characteristic) analogical to the classical identities relating the minors of a matrix and its inverse.

As an auxiliary algebraic tool supposed for application when needed in all the constructions we’re going to discuss in the present article, we’ll introduce and utilize a special principle involving a field’s extension by a formal infinitesimal and allowing, provided a number of conditions are fulfilled, to reduce the computation of a polynomial over a field to solving, in a polynomial time, a system of algebraic equations.
The neighboring computation principle (for any characteristic):

Let’s denote by $\delta(q)$ the natural function in the natural variable $q$ that equals unity if $q$ is zero and equals zero otherwise, and by $\mathcal{J}(b(t), g)$ the Jacobian matrix of the vector-function $b(t)$ computed in the point $t=g$.

Let $f(u)$ be a polynomial in $u_1, \ldots, u_{\dim(u)}$ of degree $d$ over a field $F$,

$$u = u(h_1, \ldots, h_{\dim(h)}) , \; u \text{ exists in } h^{[0]} ;$$

$$v = v(h_1, \ldots, h_{\dim(h)}) , \; v(h^{[0]}) = \overline{0}_{\dim(v)}$$

(hence $u, v$ are two vector-functions (of generically different dimensions) in the parameter vector-variable $h$ and $h^{[0]}$ is a value of this variable);

$\mathcal{J}(\begin{pmatrix} u \\ v \end{pmatrix}, h^{[0]})$ exists and is nonsingular.

Let $\varepsilon$ be a formal infinitesimal variable and

$$F(\varepsilon) = \{ \sum_{k=n}^{\infty} \alpha_k \varepsilon^k , \; \alpha_k \in F, \; \alpha_n \neq 0, \; n \in \mathbb{Z} \}$$

be its extension containing $\varepsilon$.

Then, given $\upsilon$ as the value of $u$, over $F(\varepsilon)$

$$f(\upsilon) = \sum_{i=0}^{d} \text{coef}_{\varepsilon^i}(f(u(\sum_{k=0}^{d} \varepsilon^k h^{[k]}))) .$$

where:

$$\mathcal{J}(\begin{pmatrix} u \\ v \end{pmatrix}, h^{[0]})h^{[k]} = \begin{cases} 
\delta(k-1)(u(h^{[0]}) - \upsilon) - \text{coef}_{\varepsilon^i}(u(\sum_{i=0}^{k-1} \varepsilon^i h^{[i]})), & k = 1, \ldots, d \\
\overline{0}_{\dim(v)} & \text{otherwise}
\end{cases}$$

(and thus $u(\sum_{k=0}^{d} \varepsilon^k h^{[k]}) = u(h^{[0]}) + \varepsilon(-u(h^{[0]}) + \upsilon) + O(\varepsilon^{d+1})$)

This method will be called the neighboring computation of the function $f(\upsilon)$ by the parameterization $u(h)$ in the region $\upsilon(h) = \overline{0}_{\dim(\upsilon)}$ from the bearing point
Therefore if \( f(u(h)) \) is computable in a polynomial time for any \( h \) in the region \( v(h) = \Theta_{\dim(v)} \) and there exists a bearing point \( h^{[0]} \) then \( f(v) \) is computable in a polynomial time for any \( v \) too.

In the further, for the purpose of simplicity, we’ll call a system of functions \( S \) algebraically absolutely independent in a region \( R \) (given by a system of equations with a zero right part) iff the joint system of functions consisting of \( S \) and the left part of the system representing \( R \) is algebraically independent at some point of \( R \).

The above principle hence tells us that we can polynomial-time compute a polynomial over a field if we’re able to polynomial-time reduce its calculation to solving a system of algebraic equations having polynomial (in the initial polynomial’s number of variables) numbers of variables and equations (represented by polynomial-time computable and analytical (over the basic field) functions in these variables).

I. Equalities for the sub-permanents of a unitary matrix over fields of characteristic 3

Definitions:

Let \( A \) be an \( nxn \)-matrix, \( I, J \) be two subsets of \( \{1, \ldots, n\} \) of an equal cardinality. Then we define its \( I \rightarrow J \)-replacement matrix \( A^{[I \rightarrow J]} \) as the matrix received from \( A \) through replacing its rows with indexes from \( J \) by those with indexes from \( I \), i.e. through replacing its \( i_k \)-th row by its \( j_k \)-th one for \( s = 1, \ldots, |I| \).

Analogically, given two pairs \( I,J \) and \( K,L \) of subsets of \( \{1, \ldots, n\} \) such that \( |I| = |J| \) and \( |K| = |L| \), we define its \( I \rightarrow J, K \rightarrow L \)-double-replacement matrix \( A^{[I \rightarrow J, K \rightarrow L]} \) as the matrix received from \( A \) through replacing its rows with indexes from \( J \) by those with indexes from \( I \) and its columns with indexes from \( L \) by those with indexes from \( K \).
We also define its \( I,J \)-repeat matrix \( A^{[I,J]} \) as the matrix received from \( A \) through repeating twice its rows with indexes from \( I \) and its columns with indexes from \( J \) (while the pairs of doubled rows or columns receive neighboring indexes. i.e. the doubled rows and columns follow each other).

By \( A^{(I,J)} \) we’ll denote the matrix lying on the intersection of the rows with indexes from \( I \) and the columns with indexes from \( J \), and by \( A^{(I\setminus J)} \) we’ll denote the matrix received from \( A \) through removing its rows with indexes from \( I \) and its columns with indexes from \( J \).

For the purpose of simplicity, for a 1-set \( \{i\} \) we’ll omit the brackets \( {} \) and write just \( i \) instead.

**Theorem 1:**

Let \( U \) be a unitary nxn-matrix, \( I, J \) be two disjoint subsets of \( \{1,\ldots,n\} \) of an equal cardinality.

Then \( \text{per}(U^{[I\rightarrow J]}) = (-1)^{|I|} \text{per}(U^{[J\rightarrow I]}) \)

**Proof:**

To prove this theorem, we should effectively apply the principal equality expressing the permanent of an nxn-matrix through its “central minor convolution”, i.e.

\[
\text{per}(A) = (-1)^n \sum_{L,L \subseteq \{1,\ldots,n\}} \det(A^{(L,L)}) \det(A^{(L\setminus L)})
\]

First of all, as the permanent of a square matrix doesn’t change after any permutation of its rows and a unitary matrix remains unitary after any permutation of its rows, we can assume \( I=\{1,3,\ldots,2k-1\} \), \( J=\{2,4,\ldots,2k\} \) because we always can permute the rows of \( U \) so that the latter condition is fulfilled. Therefore, proving the theorem for this pair of sets \( I,J \) is equivalent to proving it for the generic case. Hence, each of the two rows of the matrix \( U^{[I\rightarrow J]} \) with the indexes \( 2q-1, 2q \) are the \( (2q-1) \)-th row of \( U \), \( q=1,\ldots,k \).

Since the matrix \( U^{[I\rightarrow J]} \) for \( |I|=k \) has \( k \) doubled rows, the sum over \( T \) in the above equality (1) can be replaced by the sum over those \( T \) that contain exactly one element from each pair \( 2q-1, 2q \) for \( q=1,\ldots,k \).

And now we apply the equality expressing a minor of a square matrix \( A \) through a minor of its inverse (for \( L,M \) being subsets of \( \{1,\ldots,n\} \) of an equal cardinality):
\[(2) \quad \det(A^{(L,M)}) = \det(A)\det((A^{-1})^{(\setminus L, \setminus M)})(-1)^{\sum_{l \in L} l + \sum_{m \in M} m}\]

For a unitary \(U\) this formula just takes the form
\[(3) \quad \det(U^{(L,M)}) = \det(U)\det(U^{(\setminus L, \setminus M)})(-1)^{\sum_{l \in L} l + \sum_{m \in M} m}\]

while in such a case the convolution equality (1) for the matrix \(U^{[I \to J]}\) yields:
\[
\per(U^{[I \to J]}) = (-1)^n \sum_{R, R \subseteq \{1, \ldots, n\} \setminus \{I \cup J\}} \sum_{h \in \{0, 1\}}^k \det(U^{(R \cup I \cup U \cap G(h))}) \det(U^{(\setminus \{R \cup J\}, \setminus \{R \cup U \cap G(h)\}))
\]
where \(G(h) = \{2 - h_1 \cup \ldots \cup 2k - h_k\}\).

After the application of the formula (3) to the latter equality, we receive
\[
\per(U^{[I \to J]}) = (-1)^n \sum_{R, R \subseteq \{1, \ldots, n\} \setminus \{I \cup J\}} \sum_{h \in \{0, 1\}}^k \det(U^{(\setminus \{R \cup I\}, \{R \cup U \cup G(h)\})) \det(U^{(R \cup J, R \cup U \cap G(h))})
\]
as all the indexes of the involved minors are doubled except 1, \ldots, 2k each of whom appears exactly once in the corresponding sum of indexes (according to the formula (3)) and their sum is equal to \(k\) modulo 2. Hence, we get the theorem.

**Theorem 2:**

Let \(U\) be a unitary \(n \times n\)-matrix, \(I, J\) be two subsets of \(\{1, \ldots, n\}\) of an equal cardinality.

Then \(\per(U^{[I \cup J]}) = (-1)^{|I|} \per(U^{(\setminus I \cup J)})\)

**Proof:**

The proof of this theorem virtually repeats the proof of Theorem 1, including the preliminary permutations of repeated rows and repeated columns that make their indexes belong to the set \(\{1, \ldots, 2k\}\), where \(|I| = |J| = k\). I.e. we can assume, beforehand, that \(I = J = \{1, \ldots, k\}\) – for the same reason as in the proof of Theorem 1, while preserving the degree of commonness. In such a case in the corresponding convolution sum all the indexes would be repeated twice when passing to the inverse’s minors, while each product of central minors will have the coefficient \(2^{|I|} = (-1)^{|I|}\)

**Theorem 3:** given two pairs \(I, J\) and \(K, L\) of subsets of \(\{1, \ldots, n\}\) such that
\[|I| = |J| = |K| = |L|, I \cap J = K \cap L = \emptyset,\]

Proof:

Once again, this theorem can be easily proven in the same way as Theorems 1, 2, while assuming \( I = K = \{1,3,...,2k-1\}, \ J = L = \{2,4,...,2k\} \).

Definition:

For an \( nxn \)-matrix \( A \) and \( k \leq n \), let’s define its \( k \)-th permanent-minor matrix \( P(A,k) \) as a \( C_n^k \times C_n^k \)-matrix whose rows and columns are indexed by \( k \)-subsets of \( \{1,...,n\} \) and whose \( I,J \)-entry \( p_{I,J}(A,k) = \text{per}(A_{(I,J)}) \) for a pair of \( k \)-subsets \( I,J \).

Let’s also define its \( k \)-th permanent-complement matrix \( F(A,k) \) as a \( C_n^k \times C_n^k \)-matrix whose rows and columns are indexed by \( k \)-subsets of \( \{1,...,n\} \) and whose \( I,J \)-entry \( f_{I,J}(A,k) = \text{per}(A_{(\setminus I,\setminus J)}) \) for a pair of \( k \)-subsets \( I,J \).

Obviously, \( P(U^T,k) = P^T(U,k) \) and \( F(U^T,k) = F^T(U,k) \).

Corollary 1: let \( U \) be unitary. Then

\[
(*) \quad F(U,k)P^T(U,k) = (-1)^kP(U,k)F^T(U,k) \star \{(−1)^{|I\cap J|}\}_{C_n^k \times C_n^k}
\]

where \( \star \) denotes the Hadamard (i.e. entry-wise) product of matrices.

Corollary 2:

\[
(**) \quad (-1)^{k+1}F(U,k) + P(U,k)P^T(U,k) = 0
\]

Both the above corollaries follow from Theorems 1 and 2 correspondingly and the Laplace expansions of the permanent for a set of rows and for a set of rows and a set of columns.

The equalities (*) and (**) are actually linear equations expressing the entries of \( F(U,k) \) through the entries of \( F(U,s) \) for \( s<k \).

We can also notice that for a unitary \( U \) its replacement matrix for \( |I|=|J|=1 \) is 1-semi-unitary and, therefore, we can compute its permanent in a polynomial time, while for a unitary \( U \) and four pair-wise distinct indexes \( i, j, s, r \) (where \( s < r \)
(*** \( \text{per}(U^{[i,s] \rightarrow [j,r]}) - \text{per}(U^{[i,r] \rightarrow [i,s]}) = \text{per}(M_{s,r} U^{[i,j]}) \))

where \( M_{s,r} \) is the identity matrix \( \mathbb{I}_n \) where the \( s \)-th and \( r \)-th rows were left-multiplied by the unitary matrix \( \left( \frac{-1}{\sqrt{-1}} \right) \) (hence \( M_{s,r} U^{[i,j]} \) is also 1-semi-unitary as a unitary row-transformation of the 1-semi-unitary matrix \( U^{[i,j]} \)).

**Lemma 1.**

Let \( U \) be unitary, \( i < j \). Then \( \text{per}(U^{[i,j]}) = \text{per}(M_{i,j} U) \)

**Lemma 2.**

Let \( U \) be unitary, \( i < j, s < r \), \( |\{i,j,r,s\}| = 4 \). Then

\[
\text{per}(U^{[[i,s] \rightarrow [j,r]]}) - \text{per}(U^{[[i,r] \rightarrow [i,s]]}) = \text{per}(M_{s,r} M_{i,j} U)
\]

Since, by the Laplace expansion of the permanent for a set of rows, the \( I,J \)-entry of the matrix \( P(U, 2) F^T(U, 2) \) equals \( \text{per}(U^{[I \rightarrow J]}) \), i.e \( (P(U, 2) F^T(U, 2))_{I,J} = \text{per}(U^{[I \rightarrow J]}) \), the equalities (*** \( \)) (together with the fact that if \( |I \cap J| > 0 \) then \( U^{[I \rightarrow J]} \) has either precisely one replaced row or no replaced rows and, accordingly, is 1-semi-unitary or unitary correspondingly) signify that the matrix \( F(U, 2) P^T(U, 2) = (P(U, 2) F^T(U, 2))^T \) can be polynomial-time expressed as the sum of a known matrix and a matrix \( X(U) \) with the following properties: \( x_{I,J}(U) = x_{K,L}(U) \) if \( I \cup J = K \cup L \) and \( x_{I,J}(U) = 0 \) if \( |I \cap J| > 0 \). We’ll call a matrix super-symmetric if its rows and columns are indexed by 2-subsets of \( \{1,...,n\} \) and it satisfies the two latter conditions. Hence, analogically, the matrix \( P^T(U, 2) F(U, 2) = P(U^T, 2) F^T(U^T, 2) \) can also be expressed as the sum of a known matrix and a super-symmetric \( Y(U) \). Accordingly, if in the generic case of a unitary \( U \) the homogeneous system of linear equations for two super-symmetric matrices \( X \) and \( Y \) \( P(U, 2) X - Y P(U, 2) = 0 \) is non-singular and, therefore, its only solution is zero, we can polynomial-time compute the entries of \( F(U, 2) \) because the two above-mentioned expressions yield a non-singular system of linear equations for \( X(U), Y(U) \) (via expressing \( F(U, 2) \) through \( X(U) \) and \( Y(U) \) correspondingly from these expressions). As an instrument for studying the
equation $P(U,2)X - YP(U,2) = 0$, we can apply, for $n \equiv 0 \pmod{m}$, the unitary matrix $U = \text{Diag}(\{W_q\}_{q=1}^{\frac{n}{m}})$ where $W_1, \ldots, W_{n/m}$ are unitary $m \times m$-matrices.

Analogically, we can polynomial-time compute the differences

\[ (***) \text{per}(U[i\rightarrow j, r\rightarrow s]) - \text{per}(U[i\rightarrow j, s\rightarrow r]) = \text{per}(U[i\rightarrow j])M_{s,r} \]

because $\text{per}(U[i\rightarrow j])M_{s,r}$ is also 1-semi-unitary for the same reason as $M_{s,r}U[i\rightarrow j]$.

It provides us with even more equations for the entries of the matrix $F(U,2)$. Similar unitary linear combinations of $k-1$ pair-wise disjoint pairs of rows in the matrix $U[i\rightarrow j]$ would lead to some linear equations relating the entries of the matrices $F(U,k), \ldots, F(U,1)$. And the following question arises accordingly: whether it may appear that all those equations form a non-singular system for finding those matrices for some $k > 1$ in the generic case of a unitary $U$. If it’s so, we may easily reduce their computation in any special case of our interest (particularly, significant for proving $P=NP$) to computing those matrices in the most generic case -- hence implying $P=NP$. As a necessary tool for such a research, we can offer the neighboring computation principle.

Let’s call the equation (***) the $(i,j;r,s)$-replacement-shift equation for the matrix $U$ and the equation (****) the $(i,j;r,s)$-double-replacement-shift equation for $U$.

Let’s also define the matrix $B(U, \alpha) = \begin{pmatrix} \alpha I_n & \sqrt{1-\alpha^2}U^T \\ \sqrt{1-\alpha^2}U & -\alpha I_n \end{pmatrix}$ which we’ll call the $\alpha$-block-composition of $U$ where $\alpha$ is an element of a field. It’s easy to see that $B(U, \alpha)$ is unitary when $U$ is unitary. We’ll now consider, for a basic field $H$ the entries of $U$ belong to, its $\alpha$-extension $H(\alpha)$ whose elements are formal power series in $\alpha$, i.e. having the form $h = \sum_{t=k}^{\infty} h_t \alpha^t$ where $k$ we’ll call the smallness-order of $h$ (or just the order of $h$) order($h$).

Conjecture.

For the generic case of a unitary $n \times n$-matrix $U$, the set of $(i,j;s,r)$-replacement-shift equations for $U$ and $U^T$ and $(i+n,j;r+n,s)$-replacement-shift equations (considered only for the power $\alpha^2$) for $B(U, \alpha)$ and $B(U^T, \alpha)$, where $i,j,s,r$ are from $\{1,\ldots,n\}$, form an algebraically complete (i.e. having a nonsingular Jacobian matrix) system of equations for the entries of $F(U,2)$. 


Actually, while proving the above conjecture looks yet too difficult at the present time, we can try to experimentally check it via a computer modeling on a random U.

II. Reviewing the permanent-minors and other permanents derived from a unitary matrix from a much wider point of view.

1. The permanent-analog of the inverse’s minor formula.

Let A be an n×n-matrix over a field of a prime characteristic p, α, β be two n-vectors with coordinates from the set {0,...,p−1}, i.e. α, β ∈ {0,..., p − 1}^n. Then let’s denote by A^{(α,β)} the matrix received from A through repeating α_i times its i-th row for i = 1,...,n and β_j times its j-th column for j=1,...,n (if some α_i or β_j equals zero it would mean we remove the i-th row or j-th column correspondingly). Then, in case if A^{(α,β)} is square, i.e. ∑_{i=1}^n α_i = ∑_{j=1}^n β_j, the following identity holds

\[ \text{per}(A^{(α,β)}) = \det^{p-1}(A)\text{per}((A^{-1})^{((p-1)\vec{1}_n-β,(p-1)\vec{1}_n-α)}) \prod_{i=1}^n (α_i !) \prod_{j=1}^n ((p - 1 - β_j) !) \]

where \( \vec{1}_n \) is the n-vector all whose coordinates are equal to 1.

The above identity can be also written as

\[ (*) \quad \text{per}(A^{(α,β)}) = \det^{p-1}(A)\text{per}((A^{-1})^{((p-1)\vec{1}_n-β,(p-1)\vec{1}_n-α)(\prod_{i=1}^n α_i !)(\prod_{j=1}^n β_j !)(-1)^n+\sum_{i=1}^n α_i} \]

Proof:

First of all, let’s prove that

\[ (1) \quad \left( \prod_{i=1}^n \frac{(p-1)!}{α_i !} \right)\text{per}(A^{(α,β)}) = \text{per}(1_n((p-1)\vec{1}_n,(p-1)\vec{1}_n-α) A^{((p-1)\vec{1}_n,β)}) \]

where in the right side is the permanent of a matrix composed of two blocks, the first block \( 1_n^{((p-1)\vec{1}_n,(p-1)\vec{1}_n-α)} \) being block-diagonal itself with diagonal blocks of
(p − 1) \times (p − 1 − \alpha_i), i=1,...,n. The identity (1) follows from the Laplace expansion of the right permanent by the columns corresponding to the first block (this expansion is the direct product of the Laplace expansions for its diagonal blocks).

Secondly, if \( B \) is an \( m \times ((p-1)m) \)-matrix and \( G \) is an \( m \times m \)-matrix then

\[
(2) \quad \text{per}\left( (GB)^{(p-1)i_m,i_{(p-1)m}} \right) = \det^{p-1}(G)\text{per}\left( B^{(p-1)i_m,i_{(p-1)m}} \right)
\]

as in characteristic \( p \) the permanent doesn’t change if each row of a matrix is repeated \( p-1 \) times and we add one of its \( (p-1) \)-tuples of equal rows to another \( (p-1) \)-tuple of equal rows, and is multiplied by \( d^{p-1} \) if we multiply a \( (p-1) \)-tuple of equal rows by \( d \).

Upon applying the formula (2) to the case

\[
B = \left( (I_n^{(p-1)i_n,i_{(p-1)n}}) \ A^{(i_n,\beta)} \right),
\]

\( G = A^{-1} \), we’ll receive an identity involving a two-blocked matrix with the second block being block-diagonal itself (like in the identity (1)) and hence analogous to the identity (1) what will give us the initial identity.

This identity is, first of all, a generalization (for an arbitrary prime characteristic \( p \)) of all the repeat-removal identities we received in characteristic 3, and, secondly, the permanent-analog of the classical formula for the matrix inverse’s minor.

2. Permanent-preserving compressions over fields of characteristic 3

2.1 The basic compression

Let \( A \) be an \( n \times n \)-matrix over a field of characteristic 3 with at least one pair of equal rows. Let \( i,j \) (\( i<j \)) be the indexes of the lexicographical minimum (index-wise) of such pairs of rows. We’ll define the compression of \( A \) \( \text{Comp}(A) \) as the \( (n-1) \times (n-1) \)-matrix received from \( A \) through making zero (via the Gauss algorithm) all the entries of the first column of \( A \) by its \( i \)-th row (having \( a_{i,1} \) as the leading entry for the column elimination) and then removing the first column and the \( j \)-th row of the received matrix. Then

\[
\text{per}(A) = -a_{i,1}\text{per}(\text{Comp}(A))
\]
We’ll also define the compression-closure of $A$, $\overline{\text{Comp}(A)}$, as the limit of the sequential application of the compression operator to $A$ or, if at some stage the received matrix is incompressible, to its transpose (i.e. the limit of actions when we compress the matrix and transpose it if no rows are equal any more but there are equal columns, until it would have no equal rows or equal columns). We can also talk about applying the compression and compression-closure operators to sets of matrices that would map them into another sets of matrices. It’s obvious that, if we denote by $\mathbb{U}_k$ the set of $k$-semi-unitary matrices, $\overline{\text{Comp}(\mathbb{U}_0)} = \mathbb{U}_0$, i.e. unitary matrices are incompressible because they are non-singular and can’t have equal rows.

But, if we take a unitary matrix with one row replaced by another one (whose permanent we can polynomial-time compute) and multiply both copies of the repeated row by $\sqrt{-1}$, then such a matrix will be both 1-semi-unitary and compressible, and, though strange, its compression won’t be 1-semi-unitary but will be 2-semi unitary instead. Hence $\overline{\text{Comp}(\mathbb{U}_1)} \subset \mathbb{U}_2$ and the latter fact raises somewhat a hope that $\overline{\text{Comp}(\mathbb{U}_1)}$ is a set of matrices that is $\#_3$-$P$ complete and, in such a case, we can use the neighboring computation principle to prove $\#_3$-$P = P$ and, therefore, $P = NP$.

### 2.2 The generalized compression.

Let $A$ be an $n \times n$-matrix over a field of characteristic 3 having at least one linearly dependent triple of rows, i.e. a triple of rows with pair-wise distinct indexes $i,j,k$ such that $a_k = g a_i + ha_j$ where $g,h$ are some elements of the field (we also assume $a_i$ and $a_j$ are linearly independent). Then adding the row $g a_i - h a_j$ multiplied by any element of the field to any row of $A$ except the $i$-th, $j$-th and $k$-th ones doesn’t change the permanent because of its row-wise multi-linearity and the fact that the permanent of a matrix having four rows $a_i, a_j, g a_i + h a_j, g a_j - h a_j$ is zero in characteristic 3. Hence we can eliminate, while assuming that the first entry of the row $g a_i - h a_j$ is non-zero (or permuting $A$’s columns for to fulfill this condition otherwise) and having it as the Gaussian column-elimination’s leading entry, the first column of $A$ except the entries $a_{i1}, a_{j1}, a_{k1}$. Then $\text{per}(A)$ equals the permanent of the matrix received from $A$ through replacing its $i$-th, $j$-th and $k$-th rows by the pair of rows $a_{j1} a_i - a_{i1} a_j, g a_i - h a_j$ and removing its first column. We’ll call such a compression a triple-compression (as it involves a triple of linearly dependent rows), while the case of two linearly dependent rows $a_j =$
\[ da_i \], where d is some element of the field, we’ll call a pair-compression (i.e. we can divide the j-th row by d while the permanent will also be divided by d and hence we’ll receive the above-described case of equal rows). In fact, the pair-compression is a partial case of the triple-compression by putting \( d=g, h=0 \), but, nevertheless, these are two cases of permanent-preserving matrix compressions we’ll distinguish and in the further let’s understand by \( \text{Comp}(A) \) the lexicographically least (index-wise) pair- or triple-compression of A. In the meantime, the compression-closure operator’s definition won’t change in this generalization of the compression-operator.

Thus the question of determining the structure of the matrix class \( \text{Comp}(U_1) \) becomes even more intriguing and challenging towards the chief mystery P versus NP. Actually we can even consider, instead of \( U_1 \), the wider class \( U_{(1)} \subset U_2 \) of matrices each of whom can be received from a unitary matrix by replacing one of its rows by an arbitrary vector-row (if this vector-row is a linear combination of its two other rows then such a matrix is triple-compressible) and, accordingly, study the class \( \text{Comp}(U_{(1)}) \).

It would be also useful to notice that the identity given and proven in the first section of this document that links the generalized permanent-minors of a matrix and its inverse is, if considered only for characteristic 3, merely an application of the pair-compression operator to certain matrices. Accordingly, the following questions could be raised: what family of identities may we receive in characteristic 3 when applying the most general compression, i.e. including the triple case, and, actually, what are the possible analogs of the permanent-preserving compressions we found in char 3 in other prime characteristics?

An answer to the former of these two questions might be gotten via studying an arbitrary \((3n)\times(3n)\)-matrix consisting of n linearly dependent triples of rows whose compression-closure would be of size at most \((2n)\times(2n)\). It could also provide us, upon permuting the matrix’s columns so that a chosen n-subset of its column set will turn into \( \{1,\ldots,n\} \), with an opportunity to determine a relation between all the \((2n)\times(2n)\) matrices (thus having equal permanents) we may receive in this way. Let’s call two \((2n)\times(2n)\)-matrices triple-conjugate if they can be received via such a procedure from one initial \((3n)\times(3n)\)-matrix consisting of n linearly dependent triples of rows. By the way, if we apply the same scheme for a \((2n)\times(2n)\)-matrix consisting of n pairs of equal rows and the pair-compression operator then we’ll receive \( n\times n \)-matrices that are partial inverses to each other.
Hence, while computing the permanent in char 3, we can transfer not only to the matrix’s partial inverse, but to its triple-conjugate as well (however, beforehand we should actually verify that, in fact, a triple-conjugate is (generically) not a partial inverse but its genuine generalization).

2.3 A wider generalization of permanent-preserving compressions.

Let $A$ be a square matrix such that its first $2k$ rows form a matrix of rank $k$, i.e., generically, its rows with the indexes $k+1,\ldots,2k$ are linear combinations of its first $k$ rows with the coefficient $k\times k$-matrix $B$. Then $\text{per}(A)$ is equal to the product of $\text{per}(B)$ and the permanent of the matrix received from $A$ through removing its rows with the indexes $k+1,\ldots,2k$ and doubling its rows with the indexes $1,\ldots,k$. In such a case we’ll receive a matrix with $k$ pairs of equal rows to which we can apply ($k$ times) the pair-compression operator in order to reduce its size by $k$. We’ll call such a compression an even compression.

Let $A$ be a square matrix such that its first $2k-1$ (for $k>1$) rows form a matrix of rank $k$, i.e., generically, its rows with the indexes $k+1,\ldots,2k-1$ are linear combinations of its first $k$ rows with the coefficient $(k-1)\times k$-matrix $B$. Then $\text{per}(A)$ is equal to the permanent of the matrix received from $A$ through removing its rows with the indexes $k+1,\ldots,2k-1$, doubling its rows with the indexes $1,\ldots,k$, and, afterwards, adding one new column whose entries corresponding to both copies of the $q$-th row are $-\text{per}(B(\{1,\ldots,k-1\}\cup\{1,\ldots,k\}\setminus\{q\}))$ for $q=1,\ldots,k$ and all the other entries are zeros. (Please notice that the added column ensures the matrix remains square). In such a case we’ll receive a matrix with $k$ pairs of equal rows to which we can apply ($k$ times) the pair-compression operator in order to reduce its size by $k$. We’ll call such a compression an odd compression.

In both the above cases of even and odd compressions, we just should suppose, naturally, that $k$ is fixed so that $\text{per}(B)$ or $\text{per}(B(\{1,\ldots,k-1\}\cup\{1,\ldots,k\}\setminus\{q\}))$ correspondingly could be computed in a polynomial time, or that we, at least, can polynomial-time calculate these values in some way otherwise. And, apparently, we may speak about applying to a $2k$- or $(2k-1)$-set of rows of rank $k$ the $2k$- or $(2k-1)$-compression operator correspondingly (as stated above) upon an appropriate permutation of the matrix’s rows turning the set into $\{1,\ldots,2k\}$ or $\{1,\ldots,2k-1\}$. We’ll call $k$ and $k-1$ the compression’s velocity for an even and odd compression correspondingly as they lessen the matrix’s size by $k$ and $k-1$ correspondingly. We can also prove that a compression transformation doesn’t
change the matrix’s rank (although changing, possibly, its semi-unitarity class),
while transferring to a partial inverse doesn’t change the matrix’s semi-unitarity
but, nevertheless, may change its rank. Hence, coupled together, the compression
operator and all the partial inversions form a yet more perfect instrument for
permanent-preservingly compressing matrix classes, first of all $\mathbb{U}(1)$. If we define
transferring to a partial inverse as a compression of velocity 0, we might be able
to compute the permanent on a yet more reach class $\widehat{\text{Comp}}(\mathbb{U}(1))$.

By the way, actually, it’s easy to notice that the earlier mentioned pair- and triple-
compressions are merely partial cases of even and odd compressions correspondingly (that are, in fact, their generalizations), and, though strange, the
triple-compression itself can be expressed as a double pair-compression (in a
beforehand modified matrix, though). Hence since now we can start defining the
compression of a matrix as its lexicographically least (index-wise) even or odd
compression, with the same notion of the matrix’s compression-closure.

### 2.4 The criterion of the permanent’s equality to zero

Let $A$ be a square matrix such that its rows with the indexes $k+1,\ldots,k+m$ are linear
combinations of its first $k$ rows with the coefficient $m\times k$-matrix $B$ such that all its
$m\times m$-subermanents (or permanent-minors) are zero. Then $\text{per}(A) = 0$. In
characteristic 3, an example of such a matrix $B$ is the matrix $C(x,y)$ where $\dim(y) <
2\dim(x)$ and the joint vector $(x,y)$ is the root vector of a polynomial that is the
derivative of another polynomial.

### 2.5 The partial inverse equivalence and classification

of permanent-preserving compressions.

**Lemma** (on the permanent of a partial inverse):

over a field of characteristic 3, for $A_{11}, A_{22}$ being square,

\[
(**) \text{ per } \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} = \det^2(A_{11}) \text{ per } \begin{pmatrix} A_{11}^{-1} & A_{11}^{-1} A_{12} \\ A_{21} A_{11}^{-1} & A_{22} - A_{21} A_{11}^{-1} A_{12} \end{pmatrix}
\]

The proof of the above formula can be received via the technique applied in
proving the analog of the inverse’s minor formula for permanent-minors in Part 1
of this article.
Apparently, the latter formula is a generalization of the formula for the permanent of a matrix’s inverse in characteristic 3, i.e., for a square non-singular \( A \), \( \text{per}(A) = \det^2(A)\text{per}(A^{-1}) \). In the meantime, in a generic prime characteristic \( p \) and with the same technique’s usage, we can even similarly generalize the formula (*) for permanent-minors via giving to both parts of the formula (**) their row/column multiplicity degrees:

\[
(**) \quad \text{per}\left(\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}\right) = \\
= \det^{b-1}\left( A_{11}^{(\alpha, \beta)} \right) \text{per}\left( \begin{bmatrix} A_{11}^{-1} & A_{11}^{-1}A_{12} \\ A_{21}A_{11}^{-1} & A_{22} - A_{21}A_{11}^{-1}A_{12} \end{bmatrix} \right)_{(p-1)\overline{1}_n - \beta, (p-1)\overline{1}_n - \alpha} \\
\cdot \left( \prod_{i=1}^{n} \alpha_{1,i}! \right) \left( \prod_{j=1}^{n} \beta_{1,j}! \right) (-1)^{n_1 + \sum_{i=1}^{n} \alpha_{1,i}}
\]

where \( \left( A_{11}^{(\alpha, \beta)} \right) = \left( \begin{bmatrix} A_{11}^{(\alpha_1, \beta_1)} & A_{12}^{(\alpha_1, \beta_2)} \\ A_{21}^{(\alpha_2, \beta_1)} & A_{22}^{(\alpha_2, \beta_2)} \end{bmatrix} \right) \), \( A_{11} \) is of size \( n_1 \times n_1 \) and in the right part of the equality (***), each block-matrix is multiplicity-degreed correspondingly (while \( A_{11} \) and \( A^{(\alpha, \beta)} = \left( \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}^{(\alpha, \beta)} \right) \) are square again).

**Corollary** (in characteristic 3): over a field of characteristic 3 and for square \( A_{11}, A_{22}, \) let \( A_{22} - A_{21}A_{11}^{-1}A_{12} = 0 \). Then

\[
\text{per}\left(\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}\right) = \det^2(A_{11})\text{per}\left( \begin{bmatrix} A_{11}^{-1} & A_{11}^{-1}A_{12} \\ A_{21}A_{11}^{-1} & 0 \end{bmatrix} \right)
\]

The above corollary can be used for another interpretation of the earlier introduced even or odd compressions: if we permute \( A \)'s rows so that all the linearly dependent rows we refer to in the corresponding definitions would form the second block-row in the received matrix’s 2x2-block-decomposition then its corresponding (to the block-decomposition) partial inverse will have the form

\[
\left( \begin{bmatrix} A_{11}^{-1} & A_{11}^{-1}A_{12} \\ B & 0_{k \times (n_1 - k)} \end{bmatrix} \right) \text{ or } \left( \begin{bmatrix} A_{11}^{-1} & A_{11}^{-1}A_{12} \\ B & 0_{(k-1) \times (n_1 - k)} \end{bmatrix} \right)
\]

and, due to \( B \) being of size either \( k \times k \) or \( (k-1) \times k \) correspondingly, we can permanent-preservingly reduce this matrix via the Laplace-expansion for the second block-row (we’ll call such compressions *primitive*). If there are several
pair-wise disjoint sets of such linear dependencies we refer to by the definitions, they’ll yield the direct product of corresponding primitive compressions. Hence even and odd compressions are equivalent to primitive ones via partial inverse reductions.

But there are yet compressions that are not (at least, so obviously) equivalent to primitive ones. For instance,

\[
\text{per} \left( \begin{pmatrix} \alpha & \beta & \alpha + \beta \\ c_1 & c_2 & c_3 \\ b_1 & b_2 & b_3 \end{pmatrix} A_{12} \right) = \text{per} \left( \begin{pmatrix} r_{11} \alpha + r_{12} \beta & r_{21} \alpha + r_{22} \beta \\ d & e \end{pmatrix} A_{12} \right)
\]

where \( r_{11} r_{21} = b_2, r_{12} r_{22} = b_1, r_{11} r_{22} + r_{12} r_{21} = b_1 + b_2 + b_3 \),

\[
\begin{align*}
\text{per} \left( \begin{pmatrix} 1 & 0 & 1 \\ c_1 & c_2 & c_3 \\ b_1 & b_2 & b_3 \end{pmatrix} \right) & = r_{11} e + r_{21} d \\
\text{per} \left( \begin{pmatrix} 0 & 1 & 1 \\ c_1 & c_2 & c_3 \\ b_1 & b_2 & b_3 \end{pmatrix} \right) & = r_{12} e + r_{22} d
\end{align*}
\]

\( \alpha, \beta \) are vector-columns, \( A_{12} \) is a matrix (of appropriate sizes), all the other values are elements of the basic field.

All the types of compression we discussed in Chapter 2 of the present article we’ll call elementary. To summarize, we may, hence, conclude that in characteristic 3 there exists a whole variety of permanent-preserving compressions of a square matrix which, together with the set of partial inverse transformations, form the set of permanent-preserving and polynomial-time calculated elementary transformations of a matrix. The problem of finding and classifying all of them is yet to be solved. And, accordingly, the compression-closure operator (understood as the closure-limit of those elementary compressions) is a pretty rich opportunity to reduce the size of a matrix whose permanent we need to know. Therefore the question of studying the compression-closure of important matrix classes we can polynomial-time compute the permanent on like \( \mathbb{U}_{(1)} \) still arises as one of the chief mysteries related to the ever mysterious indefiniteness of P versus NP.

Besides, the formulae (\( \ast \)), (\( \ast \ast \)), (\( \ast \ast \ast \)) provide us, when applied to a unitary matrix in characteristic 3, with another variety of linear equations for a unitary matrix’s permanent-minors of a bounded depth (i.e its sub-permanents received via
removing k-sets of their rows and columns, with a bounded k) whose non-
singularity (for a given maximum of k) is to be researched as well.

3. Some formulae for the hafnian of a symmetric matrix in characteristic 3.

The approaches demonstrated and applied in the present article’s first chapter for proving (in characteristic 3 only) a number of dependencies between the permanents of matrices received from a unitary one via certain row/column repeat/replacement modifications were in fact overlapped by the compression techniques and associated formulas that appeared in the second chapter. Nevertheless, the first chapter’s methods of proof aren’t yet deprived of some independent meaning as we can also use them (in characteristic 3 only as well) for proving various facts on the hafnian of a symmetric $(2n) \times (2n)$-matrix that is a generalization of the permanent of a square matrix. For this purpose, first of all let’s define for an $(2n) \times (2n)$-matrix $A$ its even-permanent as

$$\text{per}_{\text{even}}(A) = \sum_{\pi \in S_{2n}^{(\text{even})}} \prod_{i=1}^{2n} a_{i,\pi(i)}$$

where $S_{2n}^{(\text{even})}$ is the set of 2n-permutations having only cycles of even lengths.

**Theorem:** let $A$ be a $(2n) \times (2n)$-matrix. Then, in characteristic 3,

$$\text{per}_{\text{even}}(A) = \sum_{L,L \subseteq \{1,\ldots,2n\}} (-1)^{|L|} \det(A^{(L,L)}) \det(A^{(\setminus L \setminus L)})$$

Hence, analogically to the permanent,

$$\text{per}_{\text{even}}(A) = \det^2(A) \text{per}_{\text{even}}(A^{-1})$$

**Lemma:** let $A$ be a symmetric $(2n) \times (2n)$-matrix. Then

$$\text{haf}^2(A) = \text{per}_{\text{even}}(A)$$
We may also notice that the even-permanent of $A$ doesn’t depend on its diagonal entries. Secondly, in characteristic 3, if we represent a symmetric matrix in the form $\begin{pmatrix} d & b^T \\ b & M \end{pmatrix}$ where $d$ is an element of the basic field and $b$ is an $(2n-1)$-vector then $\text{haf}\left( \begin{pmatrix} d & b^T \\ b & M \end{pmatrix} \right) = \text{haf}\left( \begin{pmatrix} d & b^T \\ b & M + \alpha bb^T \end{pmatrix} \right)$ for any scalar coefficient $\alpha$. The latter fact implies the analogical (to the permanent) relation between the hafnians and even-permanents of a symmetric matrix $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ and its symmetric partial inverse:

$$\text{haf}\left( \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \right) = \det(A_{11}) \text{haf}\left( \begin{pmatrix} A_{11}^{-1} & A_{12}^{-1}A_{12} \\ A_{21}^{-1}A_{11} & A_{22} - A_{21}^{-1}A_{11}A_{12} \end{pmatrix} \right)$$

and

$$\text{per}_{\text{even}}\left( \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \right) = \det^2(A_{11}) \text{per}_{\text{even}}\left( \begin{pmatrix} A_{11}^{-1} & A_{12}^{-1}A_{12} \\ A_{21}^{-1}A_{11} & A_{22} - A_{21}^{-1}A_{11}A_{12} \end{pmatrix} \right)$$

We can expect that, as a generalization of the permanent, the hafnian apparently does possess its own types of compression, some of them being analogical to certain compression-types we’ve earlier found for the permanent, while others, perhaps, not. The one we would call primitive is to be applied to a symmetric matrix having the form $\begin{pmatrix} 0_{m,m} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ where $A_{12}$’s number of non-zero columns equals $m$ or $m+1$.

References

1. Allender, Eric; Gore, Vivec (1994), "A uniform circuit lower bound for the permanent", *SIAM Journal on Computing*, 23 (5): 1026–1049, doi:10.1137/s0097539792233907
2. Balasubramanian, K. (1980), Combinatorics and Diagonals of Matrices, Ph.D. Thesis, Department of Statistics, Loyola College, Madras, India, T073, Indian Statistical Institute, Calcutta
3. Bax, Eric (1998), Finite-difference Algorithms for Counting Problems, Ph.D. Dissertation, 223, California Institute of Technology
4. Bax, Eric; Franklin, J. (1996), A finite-difference sieve to compute the permanent, Caltech-CS-TR-96-04, California Institute of Technology
5. Glynn, David G. (2010), "The permanent of a square matrix", *European Journal of Combinatorics*, 31 (7): 1887–1891, doi:10.1016/j.ejc.2010.01.010
6. Glynn, David G. (2013), "Permanental formulae from the Veronesean", *Designs, Codes and Cryptography*, 68 (1-3): 39–47, doi:10.1007/s10623-012-9618-1
7. Jerrum, M.; Sinclair, A.; Vigoda, E. (2001), "A polynomial-time approximation algorithm for the permanent of a matrix with non-negative entries", *Proc. 33rd Symposium on Theory of Computing*, pp. 712–721, doi:10.1145/380752.380877, ECCC TR00-079
8. Mark Jerrum; Leslie Valiant; Vijay Vazirani (1986), "Random generation of combinatorial structures from a uniform distribution", *Theoretical Computer Science*, 43: 169–188, doi:10.1016/0304-3975(86)90174-X
9. Kogan, Grigory (1996), "Computing permanents over fields of characteristic 3: where and why it becomes difficult", *37th Annual Symposium on Foundations of Computer Science (FOCS ’96)*
10. van Lint, Jacobus Hendricus; Wilson, Richard Michale (2001), A Course in Combinatorics, ISBN 0-521-00601-5
11. Little, C. H. C. (1974), "An extension of Kasteleyn's method of enumerating the 1-factors of planar graphs"; in Holton, D., Proc. 2nd Australian Conf. Combinatorial Mathematics, Lecture Notes in Mathematics, 403, Springer-Verlag, pp. 63–72
12. Little, C. H. C. (1975), "A characterization of convertible (0, 1)-matrices", Journal of Combinatorial Theory, Series B, 18 (3): 187–208, doi:10.1016/0095-8956(75)90048-9
13. Marcus, M.; Minc, H. (1961), "On the relation between the determinant and the permanent", Illinois Journal of Mathematics, 5, 376–381
14. Pólya, G. (1913), "Aufgabe 424", Arch. Math. Phys., 20 (3): 27
15. Reich, Simeon (1971), "Another solution of an old problem of pólya", American Mathematical Monthly, 78 (6): 649–650, JSTOR 2316574, doi:10.2307/2316574
16. Rempala, Grzegorz A.; Wesolowski, Jacek (2008), Symmetric Functionals on Random Matrices and Random Matchings Problems, p. 4, ISBN 0-387-75145-9
17. Ryser, Herbert John (1963), Combinatorial Mathematics, The Carus mathematical monographs, Mathematical Association of America
18. Vazirani, Vijay V. (1988), "NC algorithms for computing the number of perfect matchings in K3,3-free graphs and related problems", Proc. 1st Scandinavian Workshop on Algorithm Theory (SWAT '88), Lecture Notes in Computer Science, 318, Springer-Verlag, pp. 233–242, doi:10.1007/3-540-19487-8_27
19. Valiant, Leslie G. (1979), "The Complexity of Computing the Permanent", Theoretical Computer Science, Elsevier, 8 (2): 189–201, doi:10.1016/0304-3975(79)90044-6
20. "Permanent", CRC Concise Encyclopedia of Mathematics, Chapman & Hall/CRC, 2002