International Journal of Algebra and Computation
Vol. 32, No. 2 (2022) 251–263

DOI: 10.1142/S0218196722500126

Decompositions of matrices into potent and square-zero matrices

Peter Danchev*
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria
danchev@math.bas.bg

Esther García
Departamento de Matemática Aplicada
Ciencia e Ingeniería de los Materiales y Tecnología Electrónica
Universidad Rey Juan Carlos, 28933 Móstoles (Madrid), Spain
esther.garcia@urjc.es

Miguel Gómez Lozano
Departamento de Álgebra, Geometría y Topología
Universidad de Málaga, 29071 Málaga, Spain
miggl@uma.es

Received 7 September 2021
Accepted 6 December 2021
Published 31 January 2022

Communicated by J. Almeida

In order to find a suitable expression of an arbitrary square matrix over an arbitrary finite commutative ring, we prove that every such matrix is always representable as a sum of a potent matrix and a nilpotent matrix of order at most two when the Jacobson radical of the ring has zero-square. This somewhat extends results of ours in Linear Multilinear Algebra (2022) established for matrices considered on arbitrary fields. Our main theorem also improves on recent results due to Abyzov *et al.* in *Mat. Zametki* (2017), Šter in *Linear Algebra Appl.* (2018) and Shitov in *Indag. Math.* (2019).

Keywords: Finite commutative ring; nilpotent matrix; potent matrix; lifting potent elements.

Mathematics Subject Classification 2020: 15A24, 15B33, 16U99

1. Introduction and Fundamentals

We start the frontier of this paper by recalling that an element x of an arbitrary ring R is said to be *nilpotent* if there is an integer $i > 0$ such that $x^i = 0$ whereas

*Corresponding author.

an element y from R is said to be *potent*, or more exactly *m-potent*, if there is a natural number $m \geq 2$ with $y^m = y$. In particular, all the idempotents are always 2-potent elements.

Our work is devoted for further study, first somewhat initiated in [5], of decomposing square matrices as a sum of a potent and a nilpotent. Concretely, a brief retrospection of the most important results in this direction is as follows:

In [5] it was proven that each matrix from the ring $\mathbb{M}_n(\mathbb{F}_2)$ of $n \times n$ matrices over the field $\mathbb{F}_2$ of two elements is a sum of an idempotent matrix and a nilpotent matrix – even something more, if the matrix ring $\mathbb{M}_n(F)$ over an arbitrary field F possesses this property, then $F \cong \mathbb{F}_2$. This result was substantially strengthened by Šter in [15] who proved that every matrix in $\mathbb{M}_n(\mathbb{F}_2)$ is actually a sum of an idempotent matrix and a nilpotent matrix of index at most 4. Lately, this result was significantly improved by Shitov in [14] for certain matrix sizes n. Moreover, an important work was done by de Seguins Pazzis in [10], where a valuable discussion on the decomposition of a matrix as a sum of an idempotent and a square-zero matrix is provided.

In another vein, Abyzov and Mukhametgaliev showed in [1] that, for all naturals $n \geq 1$, any element of the ring $\mathbb{M}_n(F)$ is presented as a sum of a nilpotent and a q-potent element, provided that F is a field of cardinality q-specifically, in [1, Theorem 2] was shown that some square matrix over a finite field is expressible as a sum of a potent and a nilpotent but the order of the existing nilpotent is, in general, greater than 2. Also, a recent paper [4] by Breaz deals with the more exact presentation of matrices over fields of odd cardinality q as a sum of a q-potent matrix and a nilpotent matrix of order 3. Besides, it was constructed in [4, Example 6] an ingenious example of a 3×3 matrix over the field $\mathbb{F}_3$ of three elements that cannot be presented as the sum of a 3-potent and a nilpotent matrix of order 2 (in other terms, the latter matrix is also called *square-zero* or, equivalently, *zero-square*). Furthermore, improving the aforementioned results from [4], we establish in [9] that each square matrix over any infinite field as well as each matrix over some special finite fields can be expressed as a sum of a potent matrix and a square-zero matrix.

So, a question which logically arises is whether or not our results in [9] could be expanded for some kinds of (finite) commutative rings, that is, is every square matrix over a finite commutative ring of square-prime characteristic decomposed as a sum of a potent matrix and a square-zero matrix (for example, for rings of the sort $\mathbb{Z}_{p^2}$ for some fixed prime p)? To keep a record straight, we notice that a similar representation of such a matrix ring over $\mathbb{Z}_4$ already exists in terms of a nilpotent of order less than or equal to 8 and an idempotent (see, e.g., [15]). Even more generally, it was established in [1, Lemma 1] and [1, Theorem 4] that, for all $n, m \in \mathbb{N}$, the matrices in $\mathbb{M}_n(\mathbb{Z}_{p^m})$ are presentable as the sum of a nilpotent matrix and a p-potent matrix, whenever p is a prime. However, the exact bound (of course, if it eventually exists) of the existing nilpotent matrix is not explicitly calculated yet.

So, being seriously motivated by this idea, in what follows, we shall completely resolve [9, Problem 2] (for more account, see also [7]) even in a more general setting (see, e.g., Theorem 2.6 stated and proved below where we will show that the decomposition holds for matrices over a finite commutative ring with Jacobson radical $\mathrm{rad}(R)$ of zero-square) and, besides, we shall strengthen the previously mentioned achievements from [1, 15, 14], respectively. Part of our results are somewhat announced in [8].

Likewise, for completeness of the introductory section, we refer to the bibliography, and we also note that some related results can be found by the interested reader in [6, 13] along with the given references therewith, respectively.

2. Main Results and Conjecture

We begin here with the following simple but useful claim.

Lemma 2.1. *Let R be a finite unital commutative ring. Then, for every invertible matrix $A \in \mathbb{M}_n(R)$, there exists $m \in \mathbb{N}$ such that $A^{m-1} = \mathrm{Id}$ and $A^m = A$.*

Proof. Let A be an invertible matrix in $\mathbb{M}_n(R)$ and consider the set of matrices $\{A^0, A^1, \ldots, A^n, \ldots\}$. Since this set is finite, there exists $k < l$ such that $A^k = A^l$, and since A is invertible $\mathrm{Id} = A^{l-k}$. The claim now follows by taking $m - 1 = l - k$. □

The following result generalizes [9, Corollary 3.2], where it was shown that every matrix over a finite field is a sum of a potent matrix and a zero-square matrix by using a different approach. The result of this paper is entirely based on the primary rational canonical form of a matrix [12, VII.Corollary 4.7(ii)], which states that every matrix $A \in \mathbb{M}_n(\mathbb{F})$ where $\mathbb{F}$ is a field is similar to a direct sum of companion matrices of prime power polynomials $p_1^{m_{11}}, \ldots, p_s^{m_{sk_s}} \in \mathbb{F}[x]$ where each p_i is prime (irreducible) in $\mathbb{F}[x]$. The matrix A is uniquely determined except for the order of the companion matrices of the $p_i^{m_{ij}}$ along its main diagonal. The polynomials $p_1^{m_{11}}, \ldots, p_s^{m_{sk_s}}$ are called *the elementary divisors* of the matrix A.

Proposition 2.2. *Let $\mathbb{F}$ be a finite field. For any matrix $A \in \mathbb{M}_n(\mathbb{F})$ there exists $k \in \mathbb{N}$ such that $A = P + N$, where $N^2 = 0$, $P^k = P$, $E = P^{k-1}$ is an idempotent with $PE = EP = P$ and $EN = NE = N$.*

Proof. Let us consider the primary rational canonical form of the matrix A. Also, let us split our argument between elementary divisors $q_i(x)$ of A with $q_i(0) \neq 0$ and those with $q_i(0) = 0$:

(i) Any elementary divisor $q_i(x)$ with $q_i(0) \neq 0$ gives rise to an invertible companion matrix C_i. By Lemma 2.1, there exists $k_i \in \mathbb{N}$ such that $C_i^{k_i} = C_i$ and $C_i^{k_i - 1} = \mathrm{Id}$. Let us denote $P_i := C_i$ and define N_i as the zero matrix.

(ii) Let us suppose that $q_i(x)$ is an elementary divisor (power of an irreducible polynomial in $\mathbb{F}[x]$) such that $q_i(0) = 0$. This implies that $q_i(x) = x^{i_s}$ for certain $i_s \in \mathbb{N}$ and its associated companion matrix is of the form

$$C_i = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & & \vdots \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix} \in M_{i_s}(\mathbb{F}),$$

i.e., it is a nilpotent Jordan block.

(ii.1) If $i_s \geq 2$, write

$$P_i = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 1 & 0 & & \vdots \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix} \quad \text{and} \quad N_i := \begin{pmatrix} 0 & 0 & \cdots & -1 \\ 0 & 0 & & \vdots \\ & \ddots & \ddots & \\ 0 & & 0 & 0 \end{pmatrix}.$$

Note that P_i is an invertible matrix and by 2.1 there exists $k_i \in \mathbb{N}$ such that $P_i^{k_i} = P_i$ and $P_i^{k-1} = \mathrm{Id}$ with $C_i = P_i + N_i$.

(ii.2) If $i_s = 1$, then

$$C_i = (0).$$

Let Q be the invertible matrix in $\mathbb{M}_n(\mathbb{F})$ such that $Q^{-1}AQ$ is decomposed into its primary rational canonical form (suppose without loss of generality that the blocks corresponding to (ii.2) are written together as the last zero block):

$$Q^{-1}AQ = \left(\begin{array}{c|c|c|c|c} C_1 & 0 & \cdots & 0 & 0 \\ \hline 0 & C_2 & \cdots & 0 & 0 \\ \hline \vdots & \vdots & \ddots & \vdots & \\ \hline 0 & 0 & \cdots & C_r & 0 \\ \hline 0 & 0 & & & 0 \end{array}\right) = \underbrace{\left(\begin{array}{c|c|c|c|c} P_1 & 0 & \cdots & 0 & 0 \\ \hline 0 & P_2 & \cdots & 0 & 0 \\ \hline \vdots & \vdots & \ddots & \vdots & \\ \hline 0 & 0 & \cdots & P_r & 0 \\ \hline 0 & 0 & & & 0 \end{array}\right)}_{P'}$$

$$+ \underbrace{\left(\begin{array}{c|c|c|c|c} N_1 & 0 & \cdots & 0 & 0 \\ \hline 0 & N_2 & \cdots & 0 & 0 \\ \hline \vdots & \vdots & \ddots & \vdots & \\ \hline 0 & 0 & \cdots & N_r & 0 \\ \hline 0 & 0 & & & 0 \end{array}\right)}_{N'}.$$

Since each P_i satisfies $P_i^{k_i-1} = \mathrm{Id}$, we have that $(P')^k = P'$ for $k = 1+\prod_{i=1}^{r}(k_i-1)$ and, therefore, $E' := P'^{k-1}$ is an idempotent of $\mathbb{M}_n(\mathbb{F})$ (as $E'^2 = (P'^{k-1})^2 = P'^k P'^{k-2} = P'^{k-1} = E'$). By construction, $N'^2 = 0$ and, since $P_i^{k-1} = \mathrm{Id}$, in each block it must be that $E'N' = N'E' = N'$, as asked for.

Finally, for $P := QP'Q^{-1}$, $N := QN'Q^{-1}$ and $E := QE'Q^{-1}$ we have that E is an idempotent of $M_n(\mathbb{F})$ satisfying the properties $E = P^{k-1}$, $A = P + N$, $P^k = P$, $N^2 = 0$, $EN = NE = N$ and $EP = PE = P$. In particular, $P = EPE$ is invertible in the subring $E\mathbb{M}_n(\mathbb{F})E$ (note that $E\mathbb{M}_n(\mathbb{F})E$ is a unital ring with unit E). This, in turn, implies that P is strongly regular, as required. □

The next property of lifting idempotents is well known, but we list the statement here only for the sake of completeness and for the convenience of the readers.

Lemma 2.3 ([2, 27.1]). *Let R be a ring and let I be a nilpotent ideal of R. Then any idempotent of R/I lifts to an idempotent of R.*

The following two technicalities on lifting special elements are the key for the establishment of our further results.

Lemma 2.4. *Let R be a ring and let I be a nilpotent ideal of R. Let us suppose that $\overline{a} \in R/I$ has zero-square and that $\bar{a}$ is a von Neumann regular element in R/I. Then the element $\overline{a}$ lifts to an element of R with zero-square.*

Proof. Since $\overline{a}$ is a von Neumann regular element of zero square, there exists $\overline{b} \in R/I$ such that $\bar{a}\bar{b}\bar{a} = \bar{a}$, $\bar{b}\bar{a}\bar{b} = \bar{b}$ and $\bar{b}^2 = 0$ (see [11, Lemma 2.4]). Let us consider the idempotent $\bar{e} = \bar{a}\bar{b} \in R/I$. Notice that $\bar{e}\bar{a}(1-\bar{e}) = \bar{a}$, because $\bar{a}\bar{e} = \bar{0}$. By [2, 27.1], the element $\bar{e}$ lifts to an idempotent $e \in R$. If now we take any representant a of $\bar{a}$ in R, we will have that $ea(1-e) \in R$ has zero-square and $\overline{ea(1-e)} = \bar{e}\bar{a}(1-\bar{e}) = \bar{a}$, as claimed. □

For completeness of the exposition, let us recall now that a unital commutative ring is said to be *a local ring* if it contains a unique maximal ideal, say M. In that case, the factor ring R/M is a field, called *the residue field* of R – cf. [3, Definition 1.2.9]. Moreover, any finite commutative ring with identity R can be expressed as a direct sum of local rings and the decomposition is unique up to a permutation of the direct summands (see, e.g., [3, Theorem 3.1.4]).

Lemma 2.5. *Let R be a unital finite commutative local ring such that its unique maximal ideal M possesses the property that $M^2 = 0$. Let $S = \mathbb{M}_n(R)$. Take $P, E \in S$ such that E is an idempotent of S and $P = EPE$ and suppose that there exists $k \in \mathbb{N}$ such that $\overline{P}^{k-1} = \overline{E} \in S/\mathrm{rad}(S)$. Then there exists a prime $p > 1$ such that $P^{(k-1)p} = E$. In particular, $P^{(k-1)p+1} = P$ and P is invertible in ESE.*

Proof. Since $\overline{P}^{k-1} = \overline{E}$, there exists $U \in \mathrm{rad}(S) = \mathbb{M}_n(M)$ such that $E = P^{k-1} + U$. Multiplying on the left and on the right by E, we replace U by EUE. We know that R/M is a finite field of certain prime characteristic p. Thus $p \cdot 1 \in M$, so we have that $pM \subset M^2 = 0$. We, consequently, calculate that

$$P^{(k-1)p} = (E-U)^p = E + \sum_{i=1}^{p}(-1)^i \binom{p}{i} U^i = E,$$

as expected. □

So, we arrive at our central result on decomposing any matrix over special finite commutative rings into a potent matrix and a zero-square matrix.

Theorem 2.6. *Let R be a finite commutative ring such that its Jacobson radical has zero-square. Then every matrix A in $\mathbb{M}_n(R)$ can be expressed as $P+N$, where P is a potent matrix and N is a nilpotent matrix with $N^2 = 0$.*

Proof. We know with the aid of the comments alluded to above that R is a direct sum $R = \bigoplus R_i$, where each R_i is a local ring. Then one finds that the decomposition $\mathbb{M}_n(R) = \bigoplus_i \mathbb{M}_n(R_i)$ holds, so that we can express A as a direct sum of matrices over local rings.

Suppose without loss of generality that R is a local ring. Let us denote $S := \mathbb{M}_n(R)$ and let us decompose $A \in \mathbb{M}_n(R)$ into the sum of a potent and a zero-square matrix. Let I be the unique maximal ideal of R. By hypothesis, one calculates that $I^2 = 0$ because I coincides with the Jacobson radical $\mathrm{rad}(R)$ of R. Clearly, $J := \mathrm{rad}(\mathbb{M}_n(R)) = \mathbb{M}_n(\mathrm{rad}(R)) = \mathbb{M}_n(I)$ and hence $J^2 = 0$.

Let us consider the residue class of A modulo J: In fact, $\bar{A} \in S/J \cong \mathbb{M}_n(R/I)$. Since R/I is a finite field, by virtue of Proposition 2.2 there exists $k \in \mathbb{N}$ such that $\bar{A} = \hat{P} + \hat{N}$ with $\hat{P}^k = \hat{P}$, $\hat{N}^2 = 0$, and $\hat{E} := \hat{P}^{k-1}$ is an idempotent with $\hat{E}\,\hat{N} = \hat{N}\,\hat{E} = \hat{N}$ and $\hat{E}\,\hat{P} = \hat{P}\,\hat{E} = \hat{P}$.

Now, with Lemma 2.3 at hand, there exists an idempotent E of S such that $\overline{E} = \hat{E}$. Let us consider $P \in S$ such that $\overline{P} = \hat{P}$. Since $\hat{E}\hat{P} = \hat{P}\hat{E} = \hat{P}$, we have that $\overline{EP} = \overline{PE} = \overline{P}$ and we can suppose (by replacing P by EPE) that $EP = PE = P$. Applying Lemma 2.4 to the zero-square von Nemann-regular matrix $\hat{N} \in S/J$, there exists $N \in S$ such that $N^2 = 0$ with $\overline{N} = \hat{N}$.

Let us take $V \in J$ such that $A = P + N + V$, and write

$$A = \underbrace{P + EVE + (1-E)VE + EV(1-E)} + \underbrace{N + (1-E)V(1-E)}. \qquad (*)$$

(1) Let us show that $P + EVE + (1-E)VE + EV(1-E)$ is a potent element of S: In fact, notice that for any $n \in \mathbb{N}$

$$\begin{aligned}((P + EVE) &+ (1-E)VE + EV(1-E))^n \\ &= (P+EVE)^n + (1-E)VE(P+EVE)^{n-1} \\ &\quad + (P+EVE)^{n-1}EV(1-E),\end{aligned}$$

because EVE, $(1-E)VE$, $EV(1-E)$ and $(1-E)V(1-E)$ belong to an ideal of zero-square. Moreover, since P is invertible in ESE, the matrix $P + EVE$

is invertible and, therefore, it is potent (alternatively, since EVE lies in $J = \mathbb{M}_n(I)$, we have $\overline{P} = \overline{P + EVE}$). Furthermore, $P + EVE$ satisfies the conditions of Lemma 2.5, so we detect that $(P + EVE)^{(k-1)p} = E$ for some prime number p, so $(P + EVE)^{(k-1)p+1} = P + EVE$. Then

$$\begin{aligned}((P + EVE) + (1-E)VE + EV(1-E))^{(k-1)p+1} \\ &= (P + EVE)^{(k-1)p+1} + (1-E)VE(P + EVE)^{(k-1)p} \\ &\quad + (P + EVE)^{(k-1)p}EV(1-E) \\ &= P + EVE + (1-E)VE + EV(1-E).\end{aligned}$$

(2) Let us show that $N + (1-E)V(1-E)$ has zero-square: Indeed, since $N(1-E)$ and $(1-E)N$ belong to J and $J^2 = 0$, we have that

$$\begin{aligned}(N + (1-E)V(1-E))^2 &= N^2 + N(1-E)V(1-E) + (1-E)V(1-E)N \\ &\quad + ((1-E)V(1-E))^2 = 0.\end{aligned}$$

Therefore, equality $(*)$ provides the desired decomposition of A into a potent matrix and a zero-square matrix, as wanted. □

Since $\mathbb{Z}_{p^2}$ is a unital commutative local ring whose Jacobson radical has zero-square, we immediately obtain the following consequence, which completely resolves [9, Problem 2] when $p = 2$, i.e., for the ring $\mathbb{Z}_4$.

Corollary 2.7. *For all natural numbers n and primes p, every matrix in $\mathbb{M}_n(\mathbb{Z}_{p^2})$ can be expressed as $P + N$, where P is a potent matrix and N is a matrix with $N^2 = 0$.*

The next construction sheds a further light on the more concrete decomposition of such a type.

Example 2.8. Let us check in an example how this decomposition successfully works. Suppose $S = \mathbb{M}_8(\mathbb{Z}_4)$ and consider the following matrix:

$$A = \underbrace{\left(\begin{array}{ccc|ccc|c|c} 0 & & 1 & & & & & \\ 1 & 0 & 0 & & 0 & & 0 & 0 \\ 0 & 1 & 1 & & & & & \\ \hline & & & 0 & & 0 & & \\ & 0 & & 1 & 0 & 0 & 0 & 0 \\ & & & 0 & 1 & 0 & & \\ \hline & 0 & & & 0 & & 0 & 0 \\ \hline & 0 & & & 0 & & 0 & 0 \end{array}\right)}_{\bar{A}} + 2B,$$

where B is any matrix in S,

$$B=\left(\begin{array}{c|c|c|c} a & b & c & d \\ \hline e & f & g & h \\ \hline i & j & k & l \\ \hline m & n & p & q \end{array}\right),$$

where $a, b, \dots, q$ denote matrices of the appropriate sizes.

If we regard A as a matrix over $\mathbb{Z}_2$, we will obtain $\bar{A}$, whose elementary divisors are x^3+x^2+1, x^3, x, x. As in the proof of Proposition 2.2 and Theorem 2.6, we add and subtract the element 1 in the adequate position of the second diagonal box in order to transform the companion matrix of x^3 into an invertible matrix plus a zero-square matrix:

$$A=\underbrace{\left(\begin{array}{c|c|c|c} \begin{matrix}0&&1\\1&0&0\\0&1&1\end{matrix} & 0 & 0 & 0 \\ \hline 0 & \begin{matrix}0&&\boxed{1}\\1&0&0\\0&1&0\end{matrix} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right)}_{\hat{P}=\bar{A}+e_{4,7}}+\underbrace{\left(\begin{array}{c|c|c|c} 0 & 0 & 0 & 0 \\ \hline 0 & \begin{matrix}&&\boxed{3}\\&0&\\&&\end{matrix} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right)}_{\hat{N}=3e_{4,7}}+2B.$$

The matrix $\hat{P}=\bar{A}+e_{4,7}$ satisfies

$$\hat{P}^{42}=\left(\begin{array}{c|c|c|c} \begin{matrix}1&&\\&1&\\&&1\end{matrix} & 0 & & \\ \hline & \begin{matrix}1&&\\&1&\\&&1\end{matrix} & & \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right),$$

(it is worthwhile noticing that the first diagonal box to the 7th-power is the identity when regarded as a matrix over $\mathbb{Z}_2$, the second diagonal box to the 3rd-power is the identity when regarded as a matrix over $\mathbb{Z}_2$, so globally we need $7 \times 3 \times 2$ to get a common identity over $\mathbb{Z}_4$).

Following the proof of the theorem, let us denote $E = \hat{P}^{42}$, which is clearly an idempotent of S.

Now,

$$A = \underbrace{\hat{P} + E(2B)E + (1-E)(2B)E + E(2B)(1-E)}_{P} + \underbrace{\hat{N} + (1-E)(2B)(1-E)}_{N},$$

where we have

- $$\begin{aligned} P &= \hat{P} + E(2B)E + (1-E)(2B)E + E(2B)(1-E) \\ &= \left(\begin{array}{c|c|c|c} \begin{matrix}0 & & 1\\ 1 & & 0\\ 0 & 1 & 1\end{matrix} & 0 & 0 & 0 \\ \hline 0 & \begin{matrix}0 & & \boxed{1}\\ 1 & & 0\\ 0 & 1 & 0\end{matrix} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right) + 2\left(\begin{array}{c|c|c|c} a & b & c & d \\ \hline e & f & g & h \\ \hline i & j & 0 & 0 \\ \hline m & n & 0 & 0 \end{array}\right). \end{aligned}$$

- $$\begin{aligned} N &= \hat{N} + (1-E)(2B)(1-E) \\ &= \left(\begin{array}{c|c|c|c} 0 & 0 & 0 & 0 \\ \hline 0 & \begin{matrix} & \boxed{3}\\ 0 & \end{matrix} & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \end{array}\right) + 2\left(\begin{array}{c|c|c|c} 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & k & l \\ \hline 0 & 0 & p & q \end{array}\right), \end{aligned}$$

and $P^{43} = P$ along with $N^2 = 0$.

The following construction unambiguously illustrates that the square-prime characteristic of the ring is an essential condition and cannot be dropped off.

Remark 2.9. There are matrices over $\mathbb{Z}_{2^3}$ that do not admit a decomposition into potent + zero-square. For example, the matrix

$$A = 2\,\mathrm{Id} \in \mathbb{M}_n(\mathbb{Z}_{2^3}),$$

does not admit such a decomposition. Otherwise, since $A^2 \neq 0$ there would exist a non-zero potent matrix P and a zero-square matrix N such that $A = P + N$. Then $P^4 = ((A-N)^2)^2 = (4\,\mathrm{Id} - 4N)^2 = 0$, which is not possible if P is potent and non-zero, thus establishing our claim.

On the other side, Theorem 2.6 remains no longer true for finite commutative rings of characteristic p^2 for some arbitrary but fixed prime p. In fact, it suffices to find a finite commutative ring R of characteristic p^2 having an element a with $a^3 = 0$ and $a^2 \neq 0$. For example, consider the ring $R = \mathbb{Z}_4[x]/I$ where I is the ideal generated by the polynomial $(x^2+x+1)^3$. The characteristic of R is then exactly 4. Choose $a = (x^2+x+1) + I \in R$, and let us consider similarly to above the matrix $A = a\,\mathrm{Id} \in \mathbb{M}_n(R)$ for some $n \in \mathbb{N}$. This matrix A has the properties $A^2 \neq 0$ and $A^3 = 0$, whence with the help of the same argument as above it surely cannot be decomposed into the sum of a potent and a zero-square nilpotent. This concludes our arguments.

In order to generalize Theorem 2.6 to commutative rings of the form $\mathbb{Z}_{p^r}$ for some natural number $r \geq 2$, we first show that potent elements lift modulo a nilpotent ideal. Our proof follows the ideas of the classical lifting of idempotents (see, for instance, [2, Proposition 27.1]).

Proposition 2.10. *Let R be a finite ring and let I be a nilpotent ideal of R of index n. Let us suppose $A \in R$ is such that $\overline{A} \in R/I$ is a potent element of R/I. Then there exists $B \in R$ such that $\overline{A} = \overline{B}$ and B is potent in R.*

Proof. Suppose that $\overline{A}^t = \overline{A} \in R/I$. Then $A^t - A \in I$ and, therefore, one can calculate that

$$\begin{aligned} 0 = (A^t - A)^n &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} A^{kt} A^{(n-k)} \\ &= (-1)^n A^n - \sum_{k=1}^{n} (-1)^{n-k+1} \binom{n}{k} A^{n+(t-1)k} \\ &= (-1)^n A^n - A^{n+(t-1)} \left(\sum_{k=1}^{n} (-1)^{n-k+1} \binom{n}{k} A^{(k-1)(t-1)} \right). \end{aligned}$$

Let $T := \sum_{k=1}^{n} (-1)^{2n-k+1} \binom{n}{k} A^{(k-1)(t-1)}$. Therefore, $A^n = A^{n+(t-1)}T$. Define $E := A^{n(t-1)}T^n$. Note that $EA = AE$. Let us show that E is an idempotent of R. In fact, one sees that

$$E = A^{n(t-1)}T^n = A^{n(t-1)+(t-1)}T^{n+1} = A^{n(t-1)+2(t-1)}T^{n+2} = \cdots$$
$$= A^{n(t-1)+n(t-1)}T^{n+n} = E^2.$$

From the above calculations, we may write that

$$E = (EA)(EA^{n(t-1)-1}T^n),$$

and so we get that EA is an invertible element in ERE (note that ERE is a unital ring with identity element E). Decompose $A = EA + (1-E)A$. Since $A^n = A^{n+(t-1)}T = \cdots = A^{n+n(t-1)}T^n = A^nA^{n(t-1)}T^n = A^nE = EA^n$, it must be that $((1-E)A)^n = 0$. On the other hand, if we choose k such that $t^k \geq n$ and taking into account that $\bar{A}$ is t-potent, it follows that

$$\bar{A} = \bar{A}^t = \ldots = \bar{A}^{t^k} = (\overline{EA} + \overline{(1-E)A})^{t^k} = \overline{EA}^{t^k} + \overline{(1-E)A}^{t^k}$$
$$] = \overline{EA}^{t^k} \in \overline{ER},$$

so $\bar{A} = \overline{EA} + \overline{(1-E)A} \in \overline{ER}$, and hence $\bar{A} = \overline{EA}$.

To conclude that EA is potent, it suffices to consider the finite set

$$\{EA, (EA)^2, \ldots, (EA)^r, \ldots\},$$

to get that $(EA)^l = (EA)^m$ for some $l < m \in \mathbb{N}$, and from the invertibility of EA we get that $(EA)^{m-l} = E$, so $(EA)^{m-l+1} = EA$, as asserted. □

So, we are ready to proceed by proving the promised generalization of the chief Theorem 2.6.

Corollary 2.11. *Let n, r be two natural numbers. Then every matrix A in $\mathbb{M}_n(\mathbb{Z}_{p^r})$ can be expressed as $P+N$, where P is a potent matrix and N is a matrix such that $N^2 \in \mathbb{M}_n(p^2\mathbb{Z}_{p^r})$.*

Proof. Let $R = \mathbb{M}_n(\mathbb{Z}_{p^r})$ and let us consider the nilpotent ideal I of R generated by $p^2\,\mathrm{Id}$, i.e., $I = \mathbb{M}_n(p^2\mathbb{Z}_{p^r})$. Then $R/I \cong \mathbb{M}_n(\mathbb{Z}_{p^2})$ and thus R/I satisfies the hypothesis of Theorem 2.6. Consequently, there exist $\overline{P}, \overline{N} \in R/I$ such that $\bar{A} = \bar{P} + \bar{N}$, where $\overline{P}$ is potent and $\overline{N}^2 = \overline{0}$. By making use of Proposition 2.10, we can lift $\bar{P}$ to a potent matrix P of R. Take any matrix $N \in R$ such that N modulo I equals $\bar{N}$ (in particular we have that $N^2 \in I$). Finally, there exists $V \in I$ such that $A = P + N + V$, where

- P is potent
- $(N+V)^2 = N^2 + NV + VN + V^2 \in I = \mathbb{M}_n(p^2\mathbb{Z}_{p^r})$. □

It is worth noticing that this result extends Corollary 2.7 (note that when $r = 2$, the ideal $\mathbb{M}_n(p^2\mathbb{Z}_{p^2})$ of the former ring $\mathbb{M}_n(\mathbb{Z}_{p^2})$ is zero and so it is immediate that N has zero-square).

We finish off our work with the following conjecture which addresses Remark 2.9 quoted above.

Conjecture. Suppose $m \geq 2,\ n \geq 2$ are natural numbers and p is a prime. Then every matrix in $\mathbb{M}_n(\mathbb{Z}_{p^m})$ is a sum of a potent and of a nilpotent of order at most m.

Note that our results stated above (especially Corollary 2.7) completely settled the problem for $m = 2$. In this aspect, can we refine our machinery and results for finite commutative rings of characteristic p^m?

Acknowledgments

The authors would like to thank the anonymous referee for his/her careful reading of the manuscript and his/her competent comments and suggestions. The authors are also very grateful to the handling editor, Professor Jorge Almeida, for his professional editorial management.

The first-named author (Peter V. Danchev) was supported in part by the Bulgarian National Science Fund under Grant KP-06 No. 32/1 of December 07, 2019. The second two authors were partially supported by MTM2017-84194-P (AEI/FEDER, UE), by the Junta de Andalucía FQM264 and by B4: Ayudas para Proyectos Puente UMA "Sistemas de Jordan, álgebras de Lie y estructuras relacionadas".

References

[1] A. N. Abyzov and I. I. Mukhametgaliev, On some matrix analogues of the little Fermat theorem, *Mat. Zametki* **101**(2) (2017) 163–168.

[2] F. W. Anderson and K. R. Fuller, *Rings and Categories of Modules*, Vol. 13 of Graduate Texts in Mathematics, 2nd edn. (Springer-Verlag, New York, 1992).

[3] G. Bini and F. Flamini, *Finite Commutative Rings and Their Applications*, Vol. 680 of The Kluwer International Series in Engineering and Computer Science (Kluwer Academic Publishers, Boston, MA, 2002), (With a foreword by Dieter Jungnickel.)

[4] S. Breaz, Matrices over finite fields as sums of periodic and nilpotent elements, *Linear Algebra Appl.* **555** (2018) 92–97.

[5] S. Breaz, G. Călugăreanu, P. Danchev and T. Micu, Nil-clean matrix rings, *Linear Algebra Appl.* **439** (2013) 3115–3119.

[6] S. Breaz and S. Megiesan, Nonderogatory matrices as sums of idempotent and nilpotent matrices, *Linear Algebra Appl.* **605** (2020) 239–248.

[7] P. Danchev, On some decompositions of matrices over algebraically closed and finite fields, *J. Siberian Federal Univ. – Math. Phys.* **14** (2021) 547–553.

[8] P. Danchev, E. García and M. G. Lozano, On some special matrix decompositions over fields and finite commutative rings, *Proc. 50th Spring Conf. Union of Bulgarian Mathematicians* **50** (Union of Bulgarian Mathematicians, 2021), pp. 95–101.

[9] P. Danchev, E. García and M. G. Lozano, Decompositions of matrices into diagonalizable and square-zero matrices, *Linear Multilinear Algebra* **70** (2022).

[10] C. de Seguins Pazzis, Sums of two triangularizable quadratic matrices over an arbitrary field, *Linear Algebra Appl.* **436** (2012) 3293–3302.

[11] E. García, M. G. Lozano, R. M. Alcázar and G. Vera de Salas, A Jordan canonical form for nilpotent elements in an arbitrary ring, *Linear Algebra Appl.* **581** (2019) 324–335.

[12] T. W. Hungerford, *Algebra*, Vol. **73** of Graduate Texts in Mathematics (Springer-Verlag, New York-Berlin, 1980), (Reprint of the 1974 original.)

[13] D. A. Jaume and R. Sota, On the core-nilpotent decomposition of trees, *Linear Algebra Appl.* **563** (2019) 207–214.

[14] Y. Shitov, The ring $\mathbb{M}_{8k+4}(\mathbb{Z}_2)$ is nil-clean of index four, *Indag. Math. (N.S.)* **30** (2019) 1077–1078.

[15] J. Šter, On expressing matrices over $\mathbb{Z}_2$ as the sum of an idempotent and a nilpotent, *Linear Algebra Appl.* **544** (2018) 339–349.