Proof of a conjecture on a special class of matrices over commutative rings of characteristic 2

Baofeng Wu

Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
wubaofeng@iie.ac.cn

Abstract

In this note, we prove the conjecture posed by Keller and Rosemarin at Eurocrypt 2021 on the nullity of a matrix polynomial of a block matrix with Hadamard type blocks over commutative rings of characteristic 2. Therefore, it confirms the conjectural optimal bound on the dimension of invariant subspace of the Starkad cipher using the HADES design strategy. We also give characterizations of the algebraic structure formed by Hadamard matrices over commutative rings.

Keywords: Hadamard matrix, block matrix, Characteristic polynomial, Cayley–Hamilton theorem.

1. Introduction

At Eurocrypt 2021, Keller and Rosemarin posed the following conjecture in [3] (an initial version appeared on ePrint in Feb. 2020 [1]), in their study of the resistance of the HADES design against invariant subspace attacks.

Conjecture 1 (See [3, Conjecture 1])**.** *Let $k, s \in \mathbb{N}$. Let R be a commutative ring with characteristic 2, and let M be an s-by-s block matrix over R, each of whose blocks is a 2^k-by-2^k special matrix. Denote the blocks of M by $\{M_{i,j}\}_{i,j=1}^{s}$. Let $M'' \in R^{s\times s}$ be defined by $M''_{i,j} = \lambda(M_{i,j})$, where $\lambda(M_{i,j})$ is the unique eigenvalue of the special matrix $M_{i,j}$. Denote by $q(x) = f_{M''}(x)$ the characteristic polynomial of M''. Then $q(M)^2 = 0$.*

[1] See https://eprint.iacr.org/eprint-bin/versions.pl?entry=2020/179

In Conjecture 1, a $2^k \times 2^k$ special matrix over a commutative ring[2] R is defined recursively in the manner that

$$M = \begin{pmatrix} A & B \\ B & A \end{pmatrix},$$

where A and B are both $2^{k-1} \times 2^{k-1}$ special matrices over R (see [3, Definition 1]). Note that when $R = \mathbb{F}_{2^n}$ is a finite field, a special matrix is just the so-called Finite Field Hadamard (FFHadamard) matrix definied in [4]. Since when $\mathrm{Char}(R) = 2$ such special matrices share similar properties with the classical $\{\pm 1\}$-valued Hadamard matrices, so in the following we also call them Hadamard matrices over R.

Hadamard matrices over a commutative ring R have many nice properties. For example, the set of all $2^k \times 2^k$ Hadamard matrices, $\mathcal{H}_k(R)$, forms a commutative ring (see [3, Proposition 1]), and since it is naturally an R-module, it forms a commutative R-algebra. We further characterize structure of this algebra in Section 4 as a supplement to help understanding properties of Hadamard matrices.

It is easy to observe that any $H \in \mathcal{H}_k(R)$ is determined by its first row, say, $(a_0, a_1, \ldots, a_{2^k-1}) \in R^{2^k}$, from the recursive definition of a Hadamard matrix. By induction on k, we can prove that

$$H_{i,j} = a_{i \oplus j}, \ 0 \le i, j \le 2^k - 1. \tag{1}$$

Note that here we index the rows and columns of H starting from 0, and $\oplus$ is the exclusive-or operation of integers, in the sense of distinguishing them with binary vectors in $\mathbb{F}_2^k$ through 2-adic expansions. From this explicit representation of Hadamard matrices, one can derive all properties of them presented in [3] in the case $\mathrm{Char}(R) = 2$, in a slightly different but more direct manner. We summarize some of them in the following proposition.

Proposition 1.1. *Let R be a commutative ring of characteristic 2 and $H, H_1, H_2 \in \mathcal{H}_k(R)$ where $k \in \mathbb{N}$. Let $\det(\cdot)$ and $\lambda(\cdot)$ denote the determinant and an eigenvalue of any matrix over a commutative ring. Then we have*

(1) *H has a unique eigenvalue, namely, $\lambda(H) = \sum_{i=0}^{2^k-1} a_i$, where $(a_0, a_1, \ldots, a_{2^k-1})$ is the 1st row of H;*

[2] All rings considered in this paper are assumed to be unital ones.

(2) $H^2 = \lambda(H)^2 I_{2^k}$, *where* I_{2^k} *is the identity matrix;*
(3) $\det(H_1 + H_2) = \det(H_1) + \det(H_2)$;
(4) $\lambda(H_1 + H_2) = \lambda(H_1) + \lambda(H_2)$, $\lambda(H_1 H_2) = \lambda(H_1)\lambda(H_2)$.

From an algebraic point of view, Proposition 1.1 says that the two maps

$$\det : \mathcal{H}_k(R) \longrightarrow R \text{ and } \lambda : \mathcal{H}_k(R) \longrightarrow R$$

are both homomorphisms of rings.

Let R be a commutative ring with characteristic 2 and denote by $\mathscr{M}_{s\times s}(\mathcal{H}_k(R))$ and $\mathscr{M}_{s\times s}(R)$ the $\mathcal{H}_k(R)$- and R-algebra of $s \times s$ matrices over $\mathcal{H}_k(R)$ and R, respectively. The homomorphism $\lambda : \mathcal{H}_k(R) \longrightarrow R$ extends naturally to an R-algebraic homomorphism $\bar{\lambda} : \mathscr{M}_{s\times s}(\mathcal{H}_k(R)) \longrightarrow \mathscr{M}_{s\times s}(R)$, $(M_{i,j}) \longmapsto (\lambda(M_{i,j}))$. Similarly, the homomorphism det extends to $\overline{\det}$ over matrix algebras in this manner. For the purpose of clearity, let Det denote the classical determinalt map for $s \times s$ matrices over commutative rings, which is a homomorphism between multiplicative monoids of rings. Then Proposition 1.1 also implies that the diagrams for multiplicative monoids of algebras (rings)

$$\begin{array}{ccc} \mathscr{M}_{s\times s}(\mathcal{H}_k(R)) & \xrightarrow{\text{Det}} & \mathcal{H}_k(R) \\ \downarrow{\scriptstyle \bar{\lambda}} & & \downarrow{\scriptstyle \lambda} \\ \mathscr{M}_{s\times s}(R) & \xrightarrow[\text{Det}]{} & R \end{array}$$

and

$$\begin{array}{ccc} \mathscr{M}_{s\times s}(\mathcal{H}_k(R)) & \xrightarrow{\text{Det}} & \mathcal{H}_k(R) \\ \downarrow{\scriptstyle \overline{\det}} & & \downarrow{\scriptstyle \det} \\ \mathscr{M}_{s\times s}(R) & \xrightarrow[\text{Det}]{} & R \end{array}$$

are both commutative (see also [3, Proposition 8]).

2. Proof of Conjecture 1

In this part we explain how to prove Conjecture 1. It turns out that the main argument leads to the proof is incredibly simple, as long as we have found the key point.

For a generic $s \times s$ matrix $A = (a_{ij})$ over a commutative ring, it is well known from linear algebra that $\mathrm{Det}(A)$ is a multivariate polynomial in the entries a_{ij}. Assume $f_A(x) = \det(xI_s - A) = x^s + \sum_{i=1}^{s} f_i x^{s-i}$ is the characteristic polynomial of A. We are then clear that f_k is a multivariate polynomial in the entries $\{a_{ij}\}$ for any $1 \leq k \leq s$. In fact, it is well known $f_s = (-1)^s \mathrm{Det}(A)$. A not-so-well-known result is that for $1 \leq k \leq s$,

$$f_k = (-1)^k \mathrm{tr}\left(\bigwedge^k A\right),$$

where $\mathrm{tr}\left(\bigwedge^k A\right)$ is the trace of the k-th exterior power of the endmorphism induced by A, which can be computed as the sum of all principle minors of A of size k (of course a multivariate polynomial in the entries of A).

Let R be a commutative ring with characteristic 2, and let M and M'' be the matrices in Conjecture 1. Instead of a block matrix, we view M as a matrix over the commutative ring $\mathcal{H}_k(R)$. Assume the characteristic polynomial of M and M'' are $Q(x) = \sum_{i=0}^{s} Q_i x^i$ and $q(x) = \sum_{i=0}^{s} q_i x^i$, respectively. Note that $Q_i \in \mathcal{H}_k(R)$ while $q_i \in R$, $0 \leq i \leq s$. From the above discussion, Q_i and q_i can be computed by evaluating the same multivariate polynomial in the corresponding entries of M and M'', respectively. Since $\lambda : \mathcal{H}_k(R) \longrightarrow R$ is a homomorphism, we are clear that $\lambda(Q_i) = q_i$. From Proposition 1.1 (2), we also have $Q_i^2 = \lambda(Q_i)^2 \cdot id = q_i^2 \cdot id$, where id is the identity element of $\mathcal{H}_k(R)$, namely, I_{2^k}.

By Cayley–Hamilton theorem for matrices over commutative rings, we know that $Q(M) = 0$, and of course $Q(M)^2 = 0$. Since the ring $\mathcal{H}_k(R)$ also has characteristic 2, we have

$$0 = Q(M)^2 = \sum_{i=0}^{s} Q_i^2 M^{2i} = \sum_{i=0}^{s} (q_i^2 \cdot id) M^{2i} = \sum_{i=0}^{s} q_i^2 M^{2i} = q(M)^2.$$

This completes the proof.

3. Further discussions on Conjecture 1 and cryptographic applications

The proof of Conjecture 1 answers the second open problem in [3]. It is a great observation in [3] that the Cauchy-type MDS matrix used in the design of the Starkad cipher [1], which is an instantiations of the HADES design [2], can be viewed as an $s \times s$ block matrix with $2^k \times 2^k$ Hadamard-type blocks over $\mathbb{F}_{2^n}$. As a result, the authors mounted an attack on Starkad after finding that this matrix admitted an invariant subspace with dimension at least $t - (k+1)s$ for the PSPN part of the cipher, where $t = 2^k s$. This bound was obtained by proving that $q(M)^{k+1} = 0$, where $q(x)$ and M are the same as in Conjecture 1. In fact, dimension of the invariant subspace depends on the smallest power l such that M^l can be represented as R-linear combinations of lower powers of M. The nullity of $q(M)^{k+1}$ promises $l \leq (k+1)s$ since $\deg q(x)^{k+1} = (k+1)s$. Therefore, proof of Conjecture 1 improves this bound to $2s$.

Can this bound be further improved? We should note first that the bound $2s$ is a general one, not depending on the ring R and the shapes of these Hadamard blocks of M. Of course when these blocks are of certain special types, e.g., scalar matrices, the bound $2s$ can be improved to, e.g., s. However, this is not the case for the Cauchy matrix used in Starkad.

Another natural question is whether the characteristic polynomial $q(x)$ in Conjecture 1 can be replaced by minimal polynomial, which may has a degree less than s. More precisely, if the minimal polynomials of M'' is $\phi(x)$, shall we have $\phi(M)^2 = 0$? First, it should be noted that in this case the method for proving Conjecture 1 in Sect. 2 will not work, since coefficients of minimal polynomial of a matrix have no direct and explicit relations with its entries. Second, when R is a generic commutative ring, the minimal polynomial of a matrix over R may not be unique. Actually, minimal polynomial of a matrix A over R is defined as the least degree polynomials in the annihilating ideal of A in $R[x]$, which may not be a principle ideal. Even the minimal polynomial is unique, $\phi(M)^2 = 0$ does not always hold. Indeed, one can quickly observe that, for example, when $M'' = 0$, its minimal polynomial is $\phi(x) = x$, however, one cannot obtain $M^2 = 0$ for any M whose blocks all have eigenvalue 0.

But on the contrary, if we can find the minimal polynomial $\Phi(x) = \sum_{i=0}^{s} \Phi_i x^i \in \mathcal{H}_k(R)[x]$ of M, that is $\Phi(M) = 0$, then we can obtain $\phi(M)^2 = 0$ where $\phi(x) = \sum_{i=0}^{s} \phi_i x^i$ with $\phi_i = \lambda(\Phi_i)$. This will improve the bound for the aforementioned l to $2 \cdot \deg \Phi(x)$. However, for generic $s \times s$ matrices over commutative rings, the best general upper bound for the degrees of their minimal polynomials one can get is s. So in this sense, the bound $2s$ for a generic M is optimal. When M is considered in some special classes of matrices over $\mathcal{H}_k(R)$, e.g., circulant matrices, Vandermonde matrices, or Hadamard matrices we consider, this bound can possibly be improved.

As for Conjecture 1, it seems hard to directly prove it through evaluating $q(M)^2$. It has already been observed in [3] that $q(M)$ lies in the kernel of the homomorphism $\bar{\lambda}$, that is, all blocks of $q(M)$ have eigenvalue 0. However, as mentioned above, we cannot obtain $\tilde{M}^2 = 0$ for any $\tilde{M} \in \ker\bar{\lambda}$ in general. Besides, we can see that if $q(M)^2 = 0$, then for any $\tilde{M} \in \ker\bar{\lambda}$, we have

$$q(M + \tilde{M})^2 = 0.$$

But this does not mean if $g(M) = 0$ for certain $g(x) \in R[x]$, then we have $g(M + \tilde{M}) = 0$ for any $\tilde{M} \in \ker\bar{\lambda}$. Indeed, any $M \in \mathscr{M}_{s\times s}(\mathcal{H}_k(R))$ can be factorized into

$$M = M'' \otimes I_{2^k} + \tilde{M}$$

for a unique $\tilde{M} \in \ker\bar{\lambda}$. Obviously, for any $g(x) \in R[x]$ with $g(M'') = 0$ (e.g., $g(x) = q(x)$, the characteristic polynomial of M''), we have

$$g(M'' \otimes I_{2^k}) = g(M'') \otimes I_{2^k} = 0.$$

But this does not promise $g(M) = 0$ for any $\tilde{M} \in \ker\bar{\lambda}$.

Another interesting corollary of Conjecture 1 is, if $M \in \ker\bar{\lambda}$, then we have $M^{2s} = 0$ (not depending on k) since the characteristic polynomial of $M'' = 0$ is x^s. Recall that in [3] it was proved $M^{k+1} = 0$, an equality depending on k. The power $k+1$ comes from [3, Proposition 7], namely, any $k+1$ elements of $\mathcal{H}_k(R)$ all having eigenvalue 0 will multiply to 0. The result $M^{2s} = 0$ implies more complicated relations between elements of $\mathcal{H}_k(R)$ having eigenvalue 0, which seems not easy to directly reveal. In the next section we will further discuss the set of all such elements.

4. Structure of the algebra $\mathcal{H}_k(R)$

To further understand properties of Hadamard matrices over a commutative ring R, in this part, we give characterizations of the structure of the algebra formed by them, namely, the R-algebra $\mathcal{H}_k(R)$.

Let $G = (\mathbb{F}_2^k, \oplus)$, the additive group of the vector space $\mathbb{F}_2^k$. We denote the identity of G by e, i.e., $e = (0, 0, \ldots, 0)$. Let $R[G]$ be the group ring (algebra) generated by G over R. Elements of $R[G]$ are all of the form $a = \sum_{g\in G} a_g g$ where $a_g \in R$ for any $g \in G$, that is, formal linear combinations of elements of G over R. Multiplication of two elements a and b are defined in a convolutional manner, that is,

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g,h\in G} a_g b_h (g\oplus h) = \sum_{g\in G}\left(\sum_{h\in G} a_g b_{g\oplus h}\right) g.$$

We have the following theorem.

Theorem 4.1.

$$\mathcal{H}_k(R) \cong R[G].$$

Proof. For two Hadamard matrices A and B in $\mathcal{H}_k(R)$, assume their first rows are $(a_0, a_1, \ldots, a_{2^k-1}) \in R^{2^k}$ and $(b_0, b_1, \ldots, b_{2^k-1}) \in R^{2^k}$, respectively. Then we know from (1) that

$$A = (a_{i\oplus j})_{i,j=0}^{2^k-1}, \quad B = (b_{i\oplus j})_{i,j=0}^{2^k-1}.$$

Let $C = AB = (c_{ij})$. Then we have

$$c_{ij} = \sum_{k=0}^{2^k-1} a_{ik} b_{kj} = \sum_{k=0}^{2^k-1} a_{i\oplus k} b_{k\oplus j} = \sum_{k=0}^{2^k-1} a_k b_{k\oplus i\oplus j},$$

which means C is a Hadamard matrix with first row $(\sum_{k=0}^{2^k-1} a_k b_{k\oplus j} \mid 0 \le j \le 2^k-1)$. Therefore, the map

$$\mathcal{H}_k(R) \longrightarrow R[G], \quad (a_{i\oplus j}) \longmapsto \sum_{j=0}^{2^k-1} a_{\mathrm{bin}(j)} \mathrm{bin}(j)$$

implies the isomorphism between $\mathcal{H}_k(R)$ and $R[G]$, where

$$\mathrm{bin}: \mathbb{Z}_{2^k} \longrightarrow G, \quad j = \sum_{l=0}^{k-1} j_l 2^{k-1-l} \longmapsto (j_0, j_1, \ldots, j_{k-1}),$$

represents the 2-adic expansion of integers. □

$R[G]$ is an algebra over R with dimension 2^k, and a basis is $\{g \mid g \in G\}$. Note that all these basis elements are idempotent in $R[G]$. Elements of $R[G]$ can also be distinguished with functions from G to R. In this sense, $R[G]$ is isomorphic to the R-representation of G. Since $G = \mathbb{F}_2^{\oplus k}$, the k-fold direct sum of $\mathbb{F}_2$, we also have

$$\mathcal{H}_k(R) \cong R[G] \cong R[\mathbb{F}_2]^{\otimes k} \cong \mathcal{H}_1(R)^{\otimes k}. \tag{2}$$

(Here $\otimes k$ denotes k-fold tensor product of an R-algebra.) This tensor decomposition can also be made explicit. Let $\{e_i \mid 0 \le i \le k-1\}$ be the standard basis of G over $\mathbb{F}_2$. Then any $g \in G \backslash \{e\}$ can be represented as $g = e_{i_1} \oplus e_{i_2} \oplus \cdots \oplus e_{i_s}$ for certain $0 \le i_1 < i_2 < \cdots < i_s \le k-1$. It is easy to check that the Hadamard matrix corresponding to this g, which is actually a permutation matrix, can be decomposed into

$$I_2 \otimes \cdots \otimes I_2 \otimes \overset{i_1}{J_2} \otimes I_2 \otimes \cdots \otimes I_2 \otimes \overset{i_2}{J_2} \otimes \cdots \otimes \overset{i_s}{J_2} \otimes \cdots \otimes I_2 \text{ (k terms in total)},$$

where

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad J_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Besides, the Hadamard matrix corresponding to e is obviously $I_{2^k} = I_2^{\otimes k}$. Note that I_2 and J_2 form the basis of $\mathcal{H}_1(R)$ and $J_2^2 = I_2$. Therefore, under the conversion that $J_2^0 = I_2$, the isomorphism (2) implies that any $2^k \times 2^k$ Hadamard matrix over R can be decomposed into a polynomial-like form, that is,

$$A = \sum_{i=0}^{2^k-1} a_i J_2^i, \quad a_i \in R,$$

where

$$J_2^i := J_2^{i_0} \otimes J_2^{i_1} \otimes \cdots \otimes J_2^{i_{k-1}}, \quad i = \sum_{l=0}^{k-1} i_l 2^{k-1-l}.$$

From properties of Kronecker products of matrices, we have $J_2^i \cdot J_2^j = J_2^{i \oplus j}$. Hence this polynomial-like representation for Hadamard matrices indeed induces an isomorphism between $\mathcal{H}_k(R)$ and a polynomial algebra. In this sense, $\mathcal{H}_k(R)$ is also a Clifford algebra over R.

Theorem 4.2.

$$\mathcal{H}_k(R) \cong R[x_1, x_2, \ldots, x_k]/(x_1^2 - 1, \ldots, x_k^2 - 1).$$

Recall that for any group ring, we can define the augmentation map, that is,

$$\epsilon:\ R[G] \longrightarrow R,\quad \sum_{g\in G} a_g g \longmapsto \sum_{g\in G} a_g.$$

The kernel I of ϵ is called the augmentation ideal of $R[G]$. It is easy to prove that, as a sub-algebra of $R[G]$, I has dimension $2^k - 1$ with a basis $\{g - e \mid g \in G\backslash\{e\}\}$. In the following, we assume $\mathrm{Char}(R) = 2$. From Proposition 1.1 we know that, by distinguishing a Hadamard matrix over R with an element in $R[G]$, its image under ϵ is just the eigenvalue. Therefore, all elements in I are nilpotent. When the ring R has no nilpotent elements, the ideal I is just the nilradical of $R[G]$, i.e., intersection of all prime ideals of $R[G]$. Specifically, when R is a field, I is the unique maximal ideal of $R[G]$ and thus $R[G]$ is a local ring.

The nilpotency degree of an ideal is defined to be the smallest power that will make it vanish. For the ideal I we talk about, its nilpotency degree can be determined.

Theorem 4.3. *Assume* $\mathrm{Char}(R) = 2$ *and* I *is the augmentation ideal of the group ring* $R[G]$. *Then the nilpotency degree of* I *is* $k + 1$.

Proof. We prove $I^{k+1} = (0)$ while $I^k \neq (0)$. As I is an R-algebra, we need only to prove that any $k + 1$ basis elements multiply to 0 while there exist k basis elements that cannot.

Let $\{e_i \mid 0 \le i \le k-1\}$ be the standard basis of G over $\mathbb{F}_2$. Then $\{e_i + e \mid 0 \le i \le k-1\}$ are k basis elements of I. Note that

$$\prod_{i=0}^{k-1}(e_i + e) = \sum_{c_0,c_1,\dots,c_{k-1}\in\mathbb{F}_2} \bigoplus_{i=0}^{k-1} c_i e_i = \sum_{g\in G} g \neq 0$$

in $R[G]$.

On the other hand, let $\{g_i + e \mid g_i \in G,\ 0 \le i \le k\}$ be any $k+1$ basis elements of I. We can assume they are pairwise distinct, since otherwise they will multiply to 0 naturally. Then

$$\prod_{i=0}^{k}(g_i + e) = \sum_{c_0,c_1,\dots,c_k\in\mathbb{F}_2} \bigoplus_{i=0}^{k} c_i g_i.$$

Note that this sum iterates over all $\mathbb{F}_2$-linear combination of $\{g_i \mid 0 \le i \le k\}$. As $\{g_i \mid 0 \le i \le k\}$ must be linearly dependent over $\mathbb{F}_2$, each term turns out to appear 2^r times in the sum (in fact, $r = k - \text{rank}\{g_i\}$). Therefore, the sum vanishes since $\text{Char}(R[G]) = 2$. $\square$

Theorem 4.3 indicates that any $k + 1$ elements of I multiply to 0, which coincides with [3, Proposition 7].

References

[1] L. Grassi, D. Kales, D. Khovratovich, et al., Starkad and poseidon: new hash functions for zero knowledge proof systems, IACR Cryptol. ePrint Arch. 2019/458 (2019). https://eprint.iacr.org/2019/458

[2] L. Grassi, R. Lüftenegger, C. Rechberger, et al., On a generalization of substitution-permutation networks: the HADES design strategy, In: A. Canteaut, Y. Ishai (eds.) EUROCRYPT 2020., LNCS, vol. 12106, pp. 674—704, Springer, Cham, 2020. https://doi.org/10.1007/978-3-030-45724-223

[3] N. Keller, A. Rosemarin, Mind the Middle Layer: The HADES Design Strategy Revisited. In: A. Canteaut, FX. Standaert (eds) Advances in Cryptology — EUROCRYPT 2021, LNCS, vol. 12697, Springer, Cham, 2021. https://doi.org/10.1007/978-3-030-77886-6$_2$

[4] M. Sajadieh, M. Dakhilalian, H. Mala, et al., On construction of involutory MDS matrices from Vandermonde Matrices in $GF(2^q)$, Des. Codes Cryptogr. 64, 287—308 (2012). https://doi.org/10.1007/s10623-011-9578-x