Finite Fields and Their Applications 103 (2025) 102580

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

The distance function on Coxeter-like graphs and self-dual codes

Marko Orel [a,b,c,*], Draženka Višnjić [b]

[a] University of Primorska, FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia
[b] University of Primorska, IAM, Muzejski trg 2, 6000 Koper, Slovenia
[c] IMFM, Jadranska 19, 1000 Ljubljana, Slovenia

A R T I C L E I N F O

Article history:
Received 1 April 2024
Received in revised form 23 October 2024
Accepted 8 January 2025
Available online xxxx
Communicated by Gary L. Mullen

MSC:
15B33
05C12
94B05
15A03
05C50
15B57

Keywords:
Coxeter graph
Invertible symmetric matrices
Binary field
Rank
Distance in graphs
Alternate matrices
Self-dual codes

A B S T R A C T

Let $SGL_n(\mathbb{F}_2)$ be the set of all invertible $n \times n$ symmetric matrices over the binary field $\mathbb{F}_2$. Let Γ_n be the graph with the vertex set $SGL_n(\mathbb{F}_2)$ where a pair of matrices $\{A, B\}$ form an edge if and only if $\mathrm{rank}(A - B) = 1$. In particular, Γ_3 is the well-known Coxeter graph. The distance function $d(A, B)$ in Γ_n is described for all matrices $A, B \in SGL_n(\mathbb{F}_2)$. The diameter of Γ_n is computed. For odd $n \geqslant 3$, it is shown that each matrix $A \in SGL_n(\mathbb{F}_2)$ such that $d(A, I) = \frac{n+5}{2}$ and $\mathrm{rank}(A - I) = \frac{n+1}{2}$ where I is the identity matrix induces a self-dual code in $\mathbb{F}_2^{n+1}$. Conversely, each self-dual code C induces a family $\mathcal{F}_C$ of such matrices A. The families given by distinct self-dual codes are disjoint. The identification $C \leftrightarrow \mathcal{F}_C$ provides a graph theoretical description of self-dual codes. A result of Janusz (2007) is reproved and strengthened by showing that the orthogonal group $\mathcal{O}_n(\mathbb{F}_2)$ acts transitively on the set of all self-dual codes in $\mathbb{F}_2^{n+1}$.

* Corresponding author at: University of Primorska, FAMNIT, Glagoljaška 8, 6000 Koper, Slovenia.
E-mail addresses: marko.orel@upr.si (M. Orel), drazenka.visnjic@iam.upr.si (D. Višnjić).

https://doi.org/10.1016/j.ffa.2025.102580

1. Introduction

Vector spaces formed by matrices/bilinear forms over a (finite) field, equipped with the metric $(A, B) \mapsto \text{rank}(A - B)$, are studied in multiple research areas. In algebraic combinatorics, they are investigated within association schemes and distance-regular graphs [2,4,22,37]. In coding theory, they appear in the context of rank-metric codes [9, 11,13,36,38,41,42]. In matrix theory, they are explored in preserver problems [10,17, 20,40,44]. This research field mixes also with the study of graph homomorphisms and cores [28,31,33]. Often, the full set of matrices is replaced by a subset of hermitian, alternate, or symmetric matrices [7,14,16,18,19,28,31]. If we consider the graph Γ with the vertex set formed by all rectangular $n \times m$ matrices with coefficients from a finite field $\mathbb{F}_q$ where a pair $\{A, B\}$ of matrices form an edge if and only if $\text{rank}(A-B) = 1$, then it is well known and easy to see that the distance in this graph equals $d_\Gamma(A, B) = \text{rank}(A - B)$ for all matrices A, B (cf. [44, Proposition 3.5]). Similar claims are true for analogous graphs formed by hermitian, alternate, or symmetric matrices (cf. [44]). In all these cases, the simplicity of providing a distance formula for $d_\Gamma(A, B)$ lies in the fact that the vertex sets are vector spaces. The distance function as well as many other properties of the corresponding subgraphs, which are induced by invertible matrices, are much more difficult to investigate because the vertex sets are not closed under the addition. The only properties/results about these subgraphs we are aware of are contained in the papers [29,30,32] and in the survey [33, Examples 3.11-3.18].

In this paper, we focus on graph Γ_n where the vertex set is $SGL_n(\mathbb{F}_2)$, i.e. the set of all $n \times n$ invertible binary symmetric matrices, and where $\{A, B\}$ is an edge if and only if $\text{rank}(A - B) = 1$. There are multiple reasons to focus on graph Γ_n. As observed by the first author in [32], it generalizes the well-known Coxeter graph [8], which is obtained if $n = 3$ (see Fig. 1). Similarly, the graph obtained by the set $HGL_n(\mathbb{F}_4)$ of all $n \times n$ invertible hermitian matrices over $\mathbb{F}_4$ generalizes the well-known Petersen graph. These two graphs are very important as they are among the five (currently) known vertex-transitive graphs that do not have a Hamiltonian cycle. Hamiltonicity of vertex-transitive graphs is an active research area with a long tradition (see for example [1, 3,12,24,26,27] and the references therein). In [32], it was posed as an open problem if the graph Γ_n (and the corresponding graph formed by $HGL_n(\mathbb{F}_4)$) has a Hamiltonian cycle. Here, we do not solve this problem. However, all of the above indicate that the infinite family of graphs Γ_n ($n \in \mathbb{N}$) should be studied extensively. Some properties of graphs Γ_n were obtained already in [32]. In particular, it was shown that these graphs are cores for $n \geqslant 3$, that is, all their endomorphisms are automorphisms. In this paper, we describe the distance function $d(A, B) := d_{\Gamma_n}(A, B)$ in Γ_n and hope to report about a similar result on $HGL_n(\mathbb{F}_4)$ in the future. We also need to mention that it is expected that the computation of the diameter of Γ_n (Corollary 7.3) will help us to describe all automorphisms of Γ_n as well as some related homomorphisms [34].

To understand better the difficulty of the computation of the distance function in the context of invertible matrices, and to provide an additional reason why to focus on the

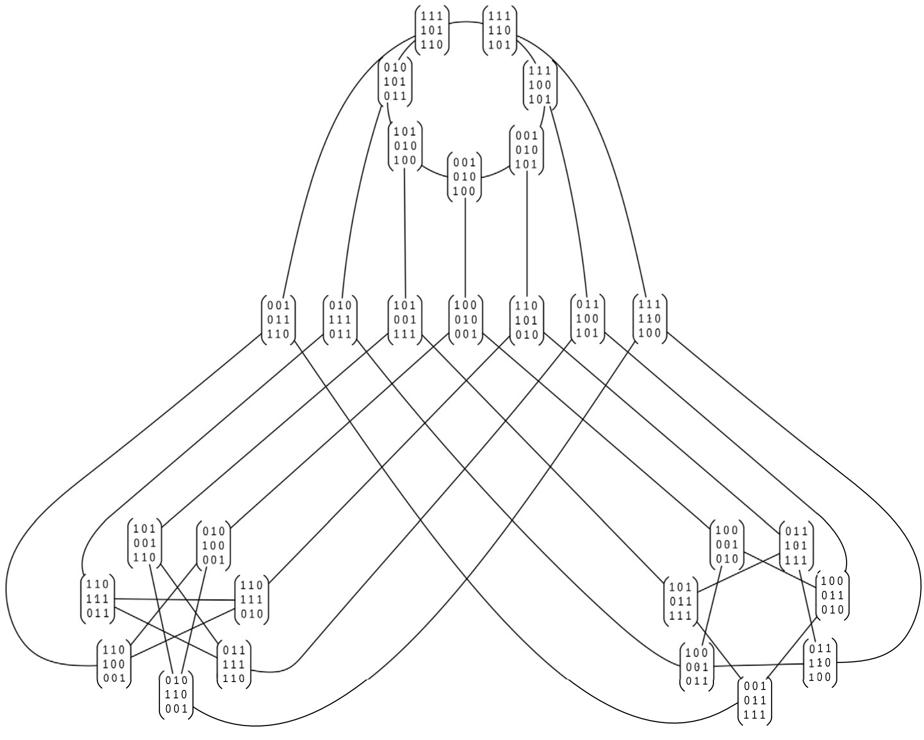

Fig. 1. Graph Γ_3 is the Coxeter graph.

binary field $\mathbb{F}_2$, consider the graph $\widehat{\Gamma}_n$ with the vertex set formed by the set $S_n(\mathbb{F}_2)$ of all $n \times n$ binary symmetric matrices where edges are defined in the same way as for the graph Γ_n. It is well known that the distance in $\widehat{\Gamma}_n$ is given by $d_{\widehat{\Gamma}_n}(A, B) = \mathrm{rank}(A - B)$ if $A - B$ is nonalternate or zero, and $d_{\widehat{\Gamma}_n}(A, B) = \mathrm{rank}(A - B) + 1$ if $A - B$ is a nonzero alternate matrix (see [44, Proposition 5.5]). In fact, if $A - B$ is nonalternate of rank r, then $B = A + \sum_{i=1}^{r} \mathbf{x}_i \mathbf{x}_i^\top$ for some linearly independent column vectors $\mathbf{x}_1, \dots, \mathbf{x}_r$. Consequently, if $C_j = A + \sum_{i=1}^{j} \mathbf{x}_i \mathbf{x}_i^\top$ for $j \in \{0, 1, \dots, r\}$, then $A = C_0, C_1, \dots, C_r = B$ is a path of length r between A and B. Similarly we can find a path of length $r + 1$ if $A - B$ is alternate of rank $r > 0$ (see Lemma 2.1). It is easy to see that there are no shorter paths of this kind. Now, if we consider the case $A, B \in SGL_n(\mathbb{F}_2)$, then it is certainly possible that some of the matrices C_j are not invertible. Hence, some distances in graph Γ_n, which is induced by the set $SGL_n(\mathbb{F}_2)$, could be larger than $d_{\widehat{\Gamma}_n}(A, B)$. This seems quite likely (and turns out to be true) because the proportion of the invertible symmetric matrices $\frac{|SGL_n(\mathbb{F}_2)|}{|S_n(\mathbb{F}_2)|}$ is quite low (see Table 1; value $|SGL_n(\mathbb{F}_2)|$ can be found in [4, Lemma 9.5.9] or [32]). This fact provides us another reason to focus on the binary field $\mathbb{F}_2$ because the corresponding proportions over larger finite fields $\mathbb{F}_q$ are much higher and converge to 1 as $q \to \infty$.

Lastly, we mention that the investigation of Γ_n represents a novel graph theoretical technique to study linear codes, self-dual codes in particular. In fact, we show that for

Table 1
$\lim_{n\to\infty} \frac{|SGL_n(\mathbb{F}_2)|}{|S_n(\mathbb{F}_2)|} = \prod_{i=1}^{\infty}\left(1-\frac{1}{2^{2i-1}}\right) = 0.4194224417951075\ldots$.

n	2	3	4	5	6	7
$\frac{\lvert SGL_n(\mathbb{F}_2)\rvert}{\lvert S_n(\mathbb{F}_2)\rvert} \doteq$	0.5	0.4375	0.4238	0.4205	0.4197	0.4195

odd n a certain subset of matrices in $SGL_n(\mathbb{F}_2)$, which is defined by the distance and the rank function in Γ_n, corresponds to self-dual codes in $\mathbb{F}_2^{n+1}$ and vice versa. Moreover, the linear codes that are self-dual are completely determined by two graph parameters, namely $d(A, I)$ and $d_{\hat{\Gamma}_n}(A, I)$ where I is the identity matrix and $A \in SGL_n(\mathbb{F}_2)$ is a matrix associated to the code. A well-known and intractable open problem in coding theory is to determine the number of permutation inequivalent self-dual codes in $\mathbb{F}_2^{n+1}$. Its value for small n and its asymptotical behavior are determined in [5, Table V][1] and [15], respectively. In [23, Theorem 10], Janusz proved that all self-dual codes are 'orthogonally equivalent'. As a corollary, he was able to show that the enumeration of permutation inequivalent self-dual codes in $\mathbb{F}_2^{n+1}$ is equivalent to the enumeration of certain double cosets in the orthogonal group $\mathcal{O}_{n+1}(\mathbb{F}_2)$. Our technique enables us to improve [23, Theorem 10] by showing that already the group $\mathcal{O}_n(\mathbb{F}_2)$ acts transitively on the set of all self-dual codes in $\mathbb{F}_2^{n+1}$.

The rest of the paper is organized as follows. In Section 2, we describe the necessary notation and collect a couple of lemmas with two roles. On one hand, they are applied in the proofs, on the other hand, they provide a better understanding of the main results to the reader. These are Theorems 3.1 and 3.3, which describe the distance function $d(A, B)$ in the graph Γ_n, and are stated in Section 3. Section 4 contains more auxiliary lemmas that are needed in the proofs. We remark that some of the results in Sections 2 and 4 could be interesting on their own from a perspective of linear algebra. Sections 5 and 6 contain the proofs of Theorems 3.1 and 3.3, respectively. In Section 7, we compute the diameter of graph Γ_n (Corollary 7.3). The connection of graph Γ_n with self-dual codes is described in Section 8 (Theorems 8.3, 8.5, 8.6, 8.10). Finally, Section 9 summarizes the meaning of the results in this paper.

2. Notation and preliminaries

Throughout the paper, $\mathbb{F}$ is a field and $\mathbb{F}_2 = \{0, 1\}$ is the binary field. Given positive integers n and m, $M_{n\times m}(\mathbb{F})$ denotes the set of all $n \times m$ matrices with coefficients from the field $\mathbb{F}$. Similarly, $GL_n(\mathbb{F})$ denotes the subset in $M_{n\times n}(\mathbb{F})$, which is formed by all invertible matrices. We use $I = I_n$ to denote the identity matrix in $GL_n(\mathbb{F})$, while $J = J_{n\times m}$ and $O = O_{n\times m}$ are the matrices in $M_{n\times m}(\mathbb{F})$ with all coefficients equal to 1 and 0, respectively. The determinant, the rank, the transpose, and the trace of a matrix A are denoted by $\det A$, $\operatorname{rank} A$, $A^\top$, and $\operatorname{Tr} A$, respectively. The elements of $\mathbb{F}^n := M_{n\times 1}(\mathbb{F})$,

[1] The value for $n + 1 = 30$ is corrected in [6].

i.e. the column vectors, are written in bold style, like $\mathbf{x}$. In particular, $\mathbf{j}_n = J_{n\times 1}$, while $\mathbf{e}_i = (0,\dots,0,1,0,\dots,0)^\top \in \mathbb{F}^n$ where 1 appears as the i-th entry. The linear span of column vectors $\mathbf{x}_1,\dots,\mathbf{x}_r \in \mathbb{F}^n$ is denoted by $\langle \mathbf{x}_1,\dots,\mathbf{x}_r\rangle$. The subset $\{A \in M_{n\times n}(\mathbb{F}) : A^\top = A\}$ of all symmetric matrices is denoted by $S_n(\mathbb{F})$, while $SGL_n(\mathbb{F}) := S_n(\mathbb{F}) \cap GL_n(\mathbb{F})$ and $\mathcal{R}_1^{\mathrm{Tr}_0} := \{A \in S_n(\mathbb{F}) : \operatorname{rank} A = 1, \operatorname{Tr} A = 0\}$. In this paper, we apply the equality $\mathbf{x}^\top A\mathbf{y} = \mathbf{y}^\top A\mathbf{x}$, which holds for all $A \in S_n(\mathbb{F})$ and $\mathbf{x},\mathbf{y} \in \mathbb{F}^n$, repeatedly. Given a column vector $\mathbf{x} \in \mathbb{F}^n$, let $\mathbf{x}^2 := \mathbf{x}\mathbf{x}^\top \in S_n(\mathbb{F})$ denote the corresponding rank-one matrix. Similarly, for $\mathbf{x},\mathbf{y} \in \mathbb{F}^n$, let $\mathbf{x}\circ\mathbf{y} := \mathbf{x}\mathbf{y}^\top - \mathbf{y}\mathbf{x}^\top$. Observe that $\mathbf{x}\circ\mathbf{y} = -\mathbf{y}\circ\mathbf{x}$ and $\mathbf{x}\circ(\mathbf{y}+\mathbf{z}) = \mathbf{x}\circ\mathbf{y} + \mathbf{x}\circ\mathbf{z}$ for all $\mathbf{x},\mathbf{y},\mathbf{z} \in \mathbb{F}^n$. Recall that a matrix $A = [a_{ij}]_{i,j\in\{1,\dots,n\}} \in M_{n\times n}(\mathbb{F})$ is *alternate* if both $A^\top = -A$ and $a_{ii} = 0$ for all i, or equivalently $\mathbf{x}^\top A\mathbf{x} = 0$ for all $\mathbf{x} \in \mathbb{F}^n$. It is well known that the rank r of an alternate matrix $A \in S_n(\mathbb{F})$ is even, and $A = \mathbf{y}_1\circ\mathbf{y}_2 + \dots + \mathbf{y}_{r-1}\circ\mathbf{y}_r$ for some linearly independent vectors $\mathbf{y}_1,\dots,\mathbf{y}_r \in \mathbb{F}^n$ whenever $r > 0$ (cf. [44, Proposition 1.34]). Clearly, if characteristic of $\mathbb{F}$, $\operatorname{char}\mathbb{F}$, is two, then any alternate matrix is symmetric, $\mathbf{x}\circ\mathbf{y} = \mathbf{x}\mathbf{y}^\top + \mathbf{y}\mathbf{x}^\top = \mathbf{y}\circ\mathbf{x} \in S_n(\mathbb{F})$,

$$(\mathbf{x}+\mathbf{y})^2 = \mathbf{x}^2 + \mathbf{y}^2 + \mathbf{x}\circ\mathbf{y} \quad \text{and} \quad (\mathbf{x}+\mathbf{y})^\top A(\mathbf{x}+\mathbf{y}) = \mathbf{x}^\top A\mathbf{x} + \mathbf{y}^\top A\mathbf{y}$$

for all $A \in S_n(\mathbb{F})$. On the other hand, each nonalternate matrix $A \in S_n(\mathbb{F})$ of rank r where $\mathbb{F}$ is a finite (or perfect) field of characteristic two can be written as $A = \sum_{i=1}^r \mathbf{x}_i^2$ for some linearly independent $\mathbf{x}_1,\dots,\mathbf{x}_r \in \mathbb{F}^n$ (cf. [44, Corollary 1.36]). Hence, for such a field $\mathbb{F}$, each nonalternate $A \in SGL_n(\mathbb{F})$ can be written as $A = PP^\top$ where matrix $P \in GL_n(\mathbb{F})$ has $\mathbf{x}_i$ as the i-th column.

In this paper, our main concern are binary symmetric matrices. To summarize, if $A \in S_n(\mathbb{F}_2)$ is of rank $r > 0$, then there are linearly independent vectors $\mathbf{y}_1,\dots,\mathbf{y}_r$ or $\mathbf{x}_1,\dots,\mathbf{x}_r$ in $\mathbb{F}_2^n$ such that either $A = \sum_{i=1}^{\frac{r}{2}} \mathbf{y}_{2i-1}\circ\mathbf{y}_{2i}$ or $A = \sum_{i=1}^r \mathbf{x}_i^2$ if A is alternate or nonalternate, respectively. Lemma 2.1 provides an additional canonical form for alternate matrices in characteristic two.

Lemma 2.1. *If $A \in S_n(\mathbb{F})$ is an alternate matrix of rank $r > 0$ and $\operatorname{char}\mathbb{F} = 2$, then there exist linearly independent column vectors $\mathbf{x}_1,\dots,\mathbf{x}_r \in \mathbb{F}^n$ such that*

$$A = \mathbf{x}_1^2 + \dots + \mathbf{x}_r^2 + (\mathbf{x}_1 + \dots + \mathbf{x}_r)^2.$$

Moreover, if $A = \mathbf{y}_1\circ\mathbf{y}_2 + \dots + \mathbf{y}_{r-1}\circ\mathbf{y}_r$ for some linearly independent vectors $\mathbf{y}_1,\dots,\mathbf{y}_r$ where r is even, then the vectors

$$\begin{aligned}
\mathbf{x}_1 &:= \mathbf{y}_1, \\
\mathbf{x}_2 &:= \mathbf{y}_2, \\
\mathbf{x}_{2k-1} &:= \mathbf{y}_1 + \dots + \mathbf{y}_{2k-2} + \mathbf{y}_{2k-1}, && (2 \leqslant k \leqslant r/2), \\
\mathbf{x}_{2k} &:= \mathbf{y}_1 + \dots + \mathbf{y}_{2k-2} + \mathbf{y}_{2k}, && (2 \leqslant k \leqslant r/2).
\end{aligned}$$

have the desired property.

Proof. Observe that $\mathbf{x}_{2k-1} + \mathbf{x}_{2k} = \mathbf{y}_{2k-1} + \mathbf{y}_{2k}$ for each k, and consequently

$$\begin{aligned} \mathbf{y}_{2k-1} &= \mathbf{x}_1 + \cdots + \mathbf{x}_{2k-2} + \mathbf{x}_{2k-1}, && (2 \leqslant k \leqslant r/2), \\ \mathbf{y}_{2k} &= \mathbf{x}_1 + \cdots + \mathbf{x}_{2k-2} + \mathbf{x}_{2k}, && (2 \leqslant k \leqslant r/2). \end{aligned}$$

We prove the equality

$$\mathbf{y}_1 \circ \mathbf{y}_2 + \cdots + \mathbf{y}_{r-1} \circ \mathbf{y}_r = \mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_r)^2$$

by induction on r. If $r = 2$, the claim is obvious. Let $r \geqslant 4$ and assume that

$$\mathbf{y}_1 \circ \mathbf{y}_2 + \cdots + \mathbf{y}_{r-3} \circ \mathbf{y}_{r-2} = \mathbf{x}_1^2 + \cdots + \mathbf{x}_{r-2}^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_{r-2})^2.$$

Then,

$$\begin{aligned} A &= \mathbf{x}_1^2 + \cdots + \mathbf{x}_{r-2}^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_{r-2})^2 + \mathbf{y}_{r-1} \circ \mathbf{y}_r \\ &= \mathbf{x}_1^2 + \cdots + \mathbf{x}_{r-2}^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_{r-2})^2 \\ &+ \big((\mathbf{x}_1 + \cdots + \mathbf{x}_{r-2}) + \mathbf{x}_{r-1}\big) \circ \big((\mathbf{x}_1 + \cdots + \mathbf{x}_{r-2}) + \mathbf{x}_r\big) \\ &= \mathbf{x}_1^2 + \cdots + \mathbf{x}_{r-2}^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_{r-2})^2 \\ &+ 0 + \mathbf{x}_{r-1} \circ \mathbf{x}_r + (\mathbf{x}_1 + \cdots + \mathbf{x}_{r-2}) \circ (\mathbf{x}_{r-1} + \mathbf{x}_r) \\ &= \mathbf{x}_1^2 + \cdots + \mathbf{x}_{r-2}^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_r)^2 + (\mathbf{x}_{r-1} + \mathbf{x}_r)^2 + \mathbf{x}_{r-1} \circ \mathbf{x}_r \\ &= \mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_r)^2. \quad \square \end{aligned}$$

Lemma 2.2 describes trace-zero rank-one symmetric matrices over $\mathbb{F}_2$.

Lemma 2.2. *Let $A \in S_n(\mathbb{F}_2)$. Then $A \in \mathcal{R}_1^{\mathrm{Tr}_0}$ if and only if there exist a permutation matrix $Q \in GL_n(\mathbb{F}_2)$ and even $k \in \{2, \ldots, n\}$ such that*

$$A = Q \begin{pmatrix} J_{k \times k} & O \\ O & O \end{pmatrix} Q^\top. \tag{1}$$

In this case, $A^2 = O$, $I + A \in SGL_n(\mathbb{F}_2)$, and $(I + A)^{-1} = I + A$.

Proof. Since $Q^\top = Q^{-1}$ and Tr is invariant under the similarity operation, it is obvious that matrix (1) is in $\mathcal{R}_1^{\mathrm{Tr}_0}$. Moreover, since k is even, we deduce that

$$I + A^2 = (I + A)^2 = Q \begin{pmatrix} (J_{k \times k} + I_k)^2 & O \\ O & I_{n-k}^2 \end{pmatrix} Q^\top = I.$$

Hence, $A^2 = O$ and $I + A$ is invertible with $(I + A)^{-1} = I + A$.

Suppose now that $A = [a_{ij}]_{i,j=1}^n \in \mathcal{R}_1^{\mathrm{Tr}0}$ is arbitrary. Define the set $S_1 = \{i \in \{1,\dots,n\} : a_{ii} = 1\}$ and let $k = |S_1|$ be its cardinality. Since A has zero trace, it follows that k is even. Being of rank one, the matrix A is nonalternate and therefore $k > 0$. Pick a permutation matrix Q such that matrix $[b_{ij}]_{i,j=1}^n = Q^\top AQ$ satisfies $\{i \in \{1,\dots,n\} : b_{ii} = 1\} = \{1,\dots,k\}$. Since matrix $[b_{ij}]_{i,j=1}^n$ is symmetric and of rank one, it follows that $b_{ij} = b_{ij}^2 = b_{ij}b_{ji} = b_{ii}b_{jj}$, i.e.

$$[b_{ij}]_{i,j=1}^n = \begin{pmatrix} J_{k\times k} & O \\ O & O \end{pmatrix}. \quad \square$$

Lemmas 2.3 and 2.4 contain well-known equalities about the determinant. Lemma 2.3 can be found in [43]. Lemma 2.4 appears in [33, Corollary 2.9] or [45] where it is stated in a slightly different form (see also [43]).

Lemma 2.3. *Let $\mathbb{F}$ be any field. If $A \in M_{n\times n}(\mathbb{F})$ is partitioned in blocks as*

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

where A_{22} is invertible, then $\det A = \det A_{22} \cdot \det(A_{11} - A_{12}(A_{22})^{-1}A_{21})$.

Lemma 2.4. *Let $\mathbb{F}$ be any field, $A \in GL_n(\mathbb{F})$, and $X, Y \in M_{n\times r}(\mathbb{F})$. Then,*

$$\det(A + XY^\top) = \det(A) \cdot \det(I_r + Y^\top A^{-1}X).$$

If $A + XY^\top \in GL_n(\mathbb{F})$, then

$$(A + XY^\top)^{-1} = A^{-1} - A^{-1}X(I_r + Y^\top A^{-1}X)^{-1}Y^\top A^{-1}.$$

Corollary 2.5. *Assume that $A, B := A + \sum_{i=1}^r \mathbf{x}_i^2 \in SGL_n(\mathbb{F})$ where $\mathbf{x}_1,\dots,\mathbf{x}_r \in \mathbb{F}^n$ and* $\operatorname{char}\mathbb{F} = 2$. *Then, $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1$ for all i if and only if $\mathbf{x}_i^\top B^{-1}\mathbf{x}_i = 1$ for all i.*

Proof. Let X be the $n \times r$ matrix with $\mathbf{x}_i$ as its i-th column. Since $B = A + XX^\top$,

$$B^{-1} = A^{-1} - A^{-1}X(I_r + X^\top A^{-1}X)^{-1}X^\top A^{-1}$$

by Lemma 2.4. If $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1$ for all i, then $I_r + X^\top A^{-1}X$ is an alternate matrix. Hence, $C := A^{-1}X(I_r + X^\top A^{-1}X)^{-1}X^\top A^{-1}$ is also alternate and $\mathbf{x}_i^\top B^{-1}\mathbf{x}_i = \mathbf{x}_i^\top A^{-1}\mathbf{x}_i - \mathbf{x}_i^\top C\mathbf{x}_i = 1 + 0 = 1$. The converse is symmetric. $\square$

Corollary 2.6. *Let r be an odd integer such that $1 \leqslant r \leqslant n$. If $\mathbf{x}_1,\dots,\mathbf{x}_r \in \mathbb{F}_2^n$ and $A, A + \sum_{i=1}^r \mathbf{x}_i^2 \in SGL_n(\mathbb{F}_2)$, then there exists i such that $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 0$.*

Proof. Let $\mathbf{x}_i$ be the i-th column of $X \in M_{n\times r}(\mathbb{F}_2)$. By Lemma 2.4,

$$1 = \det\left(A + \sum_{i=1}^{r} \mathbf{x}_i^2\right) = \det(A + XX^\top) = \det(I_r + X^\top A^{-1}X).$$

Since r is odd, and alternate matrices have even rank, the symmetric matrix $I_r + X^\top A^{-1}X$ is not alternate, i.e. some of its diagonal entries equal one. □

Finally, recall that a vector subspace $C \subseteq \mathbb{F}_2^n$ is a (binary) *linear code* of *length* n and *dimension* $\dim C$. It is *self-orthogonal* if $C \subseteq C^\perp := \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x}^\top \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C\}$ (cf. [21]). In this case, $\dim C \leqslant \lfloor \frac{n}{2} \rfloor$. If $C = C^\perp$, then the code is *self-dual*, n is even, and $\dim C = \frac{n}{2}$. Given $\mathbf{x} \in \mathbb{F}_2^n$, let $\overline{\mathbf{x}} \in \mathbb{F}_2^{n+1}$ be defined by

$$\overline{\mathbf{x}} = \begin{pmatrix} \mathbf{x} \\ \mathbf{x}^\top \mathbf{x} \end{pmatrix}.$$

Lemma 2.7. *Let* $\operatorname{rank}\left([\mathbf{x}_i^\top \mathbf{x}_j]_{i,j=1}^r\right) \leqslant 1$ *for some* $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \mathbb{F}_2^n$*. Then,* $\langle \overline{\mathbf{x}}_1, \ldots, \overline{\mathbf{x}}_r \rangle$ *is a self-orthogonal code in* $\mathbb{F}_2^{n+1}$*. If* $\mathbf{x}_1, \ldots, \mathbf{x}_r$ *are linearly independent, then* $r \leqslant \left\lfloor \frac{n+1}{2} \right\rfloor$*.*

Proof. Since $[\mathbf{x}_i^\top \mathbf{x}_j]_{i,j=1}^r$ is of rank $\leqslant 1$, all its 2×2 minors vanish. Hence,

$$\overline{\mathbf{x}}_i^\top \overline{\mathbf{x}}_j = \mathbf{x}_i^\top \mathbf{x}_j + \mathbf{x}_i^\top \mathbf{x}_i \cdot \mathbf{x}_j^\top \mathbf{x}_j = \mathbf{x}_i^\top \mathbf{x}_i \cdot \mathbf{x}_j^\top \mathbf{x}_j - (\mathbf{x}_i^\top \mathbf{x}_j)^2 = 0$$

for all i, j and the code $\langle \overline{\mathbf{x}}_1, \ldots, \overline{\mathbf{x}}_r \rangle$ is self-orthogonal. If $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \mathbb{F}_2^n$ are linearly independent, then $\dim\langle \overline{\mathbf{x}}_1, \ldots, \overline{\mathbf{x}}_r \rangle = r$ and therefore $r \leqslant \left\lfloor \frac{n+1}{2} \right\rfloor$. □

3. Statement of the main results

Theorems 3.1 and 3.3, which describe the distance $d(A, B)$ between arbitrary vertices $A, B \in SGL_n(\mathbb{F}_2)$ in graph Γ_n, are the main results of this paper. We write $A \sim B$ if $d(A, B) = 1$. Since Γ_n is an induced subgraph in $\widehat{\Gamma}_n$, it follows that $d(A, B) \geqslant d_{\widehat{\Gamma}_n}(A, B)$ for all $A, B \in SGL_n(\mathbb{F}_2)$, that is,

$$d(A, B) \geqslant \begin{cases} \operatorname{rank}(A - B), & \text{if } A - B \text{ is nonalternate or zero;} \\ \operatorname{rank}(A - B) + 1, & \text{if } A - B \text{ is alternate and nonzero.} \end{cases} \tag{2}$$

Theorem 3.1 describes $d(A, B)$ for all $A, B \in SGL_n(\mathbb{F}_2)$ where $A - B$ is an arbitrary nonalternate matrix of rank r.

Theorem 3.1. *Let* $A, B \in SGL_n(\mathbb{F}_2)$ *be such that* $B - A = \sum_{i=1}^r \mathbf{x}_i^2$ *for some linearly independent column vectors* $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \mathbb{F}_2^n$*.*

(i) *If* $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1$ *for all* i, *then*

$$d(A,B) = \begin{cases} r+2, & \text{if } \mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 1 \text{ for all } i,j; \\ r+1, & \text{otherwise.} \end{cases}$$

(ii) *If* $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r \in \mathcal{R}_1^{\mathrm{Tr}_0}$, *then* $d(A,B) = r+2$.
(iii) *Otherwise,* $d(A,B) = r$.

Remark 3.2. Observe that cases (i), (ii), (iii) are all distinct, except if r is even and $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 1$ for all i,j. In this case A,B fit the assumptions in (i) and (ii).

By Lemma 2.1, Theorem 3.3 describes $d(A,B)$ for all $A,B \in SGL_n(\mathbb{F}_2)$ where $A-B$ is an arbitrary alternate matrix of rank $r>0$.

Theorem 3.3. *Let* $A,B \in SGL_n(\mathbb{F}_2)$ *be such that* $B-A = \sum_{i=1}^{r+1}\mathbf{x}_i^2$ *for some linearly independent* $\mathbf{x}_1,\ldots,\mathbf{x}_r \in \mathbb{F}_2^n$ *where* $r>0$ *is even and* $\mathbf{x}_{r+1} = \sum_{i=1}^r \mathbf{x}_i$.

(i) *If* $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1}$ *is not of rank one, then* $d(A,B) = r+1$.
(ii) *If* $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1}$ *is of rank one, then* $d(A,B) = r+2$.

Remark 3.4. Observe that $\mathbf{x}_{r+1} = \sum_{i=1}^r \mathbf{x}_i$ implies that $\mathrm{Tr}([\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1}) = 0$ and $\mathrm{rank}([\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1}) = \mathrm{rank}([\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r})$.

Remark 3.5. In Theorems 3.1 and 3.3, $B = A + XX^\top$ where X is the $n \times r$ matrix or the $n \times (r+1)$ matrix with $\mathbf{x}_i$ as the i-th column. By Lemma 2.4,

$$X^\top B^{-1}X = X^\top A^{-1}X - X^\top A^{-1}X(I + X^\top A^{-1}X)^{-1}X^\top A^{-1}X. \tag{3}$$

Therefore, if $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j} = X^\top A^{-1}X \in \mathcal{R}_1^{\mathrm{Tr}_0}$, then Lemma 2.2 implies that $(X^\top A^{-1}X)^2 = O$ and $(I + X^\top A^{-1}X)^{-1} = I + X^\top A^{-1}X$. Consequently, $X^\top B^{-1}X = X^\top A^{-1}X$ by (3). In particular, $[\mathbf{x}_i^\top B^{-1}\mathbf{x}_j]_{i,j} \in \mathcal{R}_1^{\mathrm{Tr}_0}$. Likewise, if in Theorem 3.1, $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1$ for all i, then $\mathbf{x}_i^\top B^{-1}\mathbf{x}_i = 1$ for all i by Corollary 2.5. Hence, matrices A and B really occur symmetrically in Theorems 3.1 and 3.3 (observe that, by Corollary 2.6 and Lemma 2.2, the case $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 1$ for all i,j in Theorem 3.1 (i) is equivalent to $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j} \in \mathcal{R}_1^{\mathrm{Tr}_0}$ and $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1$ for all i).

4. Auxiliary results

Results in this section are essential for the proofs in Sections 5 and 6. Lemma 4.1 is of technical nature and is applied in the proof of Theorem 3.1.

Lemma 4.1. *Let $a \in \mathbb{F}_2$ be 1 if and only if the positive integer m is odd. Then,*

$$\begin{pmatrix} a & 1+a & \mathbf{j}_m^\top \\ 1+a & 1+a & \mathbf{j}_m^\top \\ \mathbf{j}_m & \mathbf{j}_m & I_m \end{pmatrix} \in SGL_{m+2}(\mathbb{F}_2). \tag{4}$$

Proof. Let A be the 2×2 top-left corner of the matrix in (4). By Lemma 2.3,

$$\det \begin{pmatrix} A & J_{2\times m} \\ J_{2\times m}^\top & I_m \end{pmatrix} = \det(A - J_{2\times m} J_{2\times m}^\top)$$
$$= \det(A - aJ_{2\times 2}) = \det \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = 1. \quad \square$$

It is a bit unexpected that the statement of Lemma 4.2 holds for arbitrary $A \in SGL_n(\mathbb{F})$. We apply this lemma in the proof of Lemma 4.3.

Lemma 4.2. *Let $A \in SGL_n(\mathbb{F})$ where $\operatorname{char}\mathbb{F} = 2$, let vectors $\mathbf{x}_1, \dots, \mathbf{x}_r \in \mathbb{F}^n$ be linearly independent, and assume that $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1$ for all i. If $\operatorname{rank}(\mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2 + \mathbf{y}^2) < r$ for some $\mathbf{y} \in \mathbb{F}^n$, then $\mathbf{y}^\top A^{-1}\mathbf{y} = 1$.*

Proof. Pick any $P \in GL_n(\mathbb{F})$ that has $\mathbf{x}_i$ as the i-th column for $i = 1, \dots, r$. Let $\mathbf{z} = P^{-1}\mathbf{y}$. Then $\mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2 + \mathbf{y}^2 = P(\mathbf{e}_1^2 + \cdots + \mathbf{e}_r^2 + \mathbf{z}^2)P^\top$, so

$$\operatorname{rank}(\mathbf{e}_1^2 + \cdots + \mathbf{e}_r^2 + \mathbf{z}^2) < r. \tag{5}$$

By [25, Lemma 3.1], $\mathbf{z} = \sum_{i=1}^r z_i \mathbf{e}_i$ for some $z_i \in \mathbb{F}$. By (5) and Lemma 2.4,

$$0 = \det(I_r + (z_1, \dots, z_r)^\top (z_1, \dots, z_r)) = 1 + (z_1, \dots, z_r)(z_1, \dots, z_r)^\top = 1 + \sum_{i=1}^r z_i^2.$$

Consequently, in characteristic two we deduce that

$$\mathbf{y}^\top A^{-1}\mathbf{y} = \left(\sum_{i=1}^r z_i \mathbf{e}_i\right)^\top P^\top A^{-1} P \left(\sum_{i=1}^r z_i \mathbf{e}_i\right) = \sum_{i=1}^r z_i^2 \cdot \mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1. \quad \square$$

Lemmas 4.3, 4.4 give the lower bounds for the cases (i), (ii) in Theorem 3.1.

Lemma 4.3. *Let $A, A + \sum_{i=1}^r \mathbf{x}_i^2 \in SGL_n(\mathbb{F}_2)$ where $\mathbf{x}_1, \dots, \mathbf{x}_r \in \mathbb{F}_2^n$ are linearly independent and $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1$ for all i. Then, $d(A, A + \sum_{i=1}^r \mathbf{x}_i^2) \geqslant r + 1$.*

Proof. By (2), $d(A, A + \sum_{i=1}^r \mathbf{x}_i^2) \geqslant r$. Suppose that $d(A, A + \sum_{i=1}^r \mathbf{x}_i^2) = r$. Then there exist nonzero vectors $\mathbf{y}_1, \dots, \mathbf{y}_r$ such that $A + \sum_{i=1}^s \mathbf{y}_i^2 \in SGL_n(\mathbb{F}_2)$ for all $s \in \{1, \dots, r\}$

and $\sum_{i=1}^r \mathbf{y}_i^2 = \sum_{i=1}^r \mathbf{x}_i^2$. In particular, $\operatorname{rank}(\sum_{i=1}^r \mathbf{x}_i^2 + \mathbf{y}_1^2) = \operatorname{rank}(\sum_{i=2}^r \mathbf{y}_i^2) \leqslant r-1$. By Lemma 4.2, $\mathbf{y}_1^\top A^{-1}\mathbf{y}_1 = 1$. On the other hand, Lemma 2.4 implies $1 = \det(A + \mathbf{y}_1^2) = 1 + \mathbf{y}_1^\top A^{-1}\mathbf{y}_1 = 0$, a contradiction. □

Lemma 4.4. *Let $A, A + \sum_{i=1}^r \mathbf{x}_i^2 \in SGL_n(\mathbb{F}_2)$ where $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \mathbb{F}_2^n$ are linearly independent, $2 \leqslant r \leqslant n$, and $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r \in \mathcal{R}_1^{\mathrm{Tr}_0}$. Then, $d(A, A + \sum_{i=1}^r \mathbf{x}_i^2) \geqslant r+2$.*

Proof. By Lemma 2.2, we can permute vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ to achieve that

$$[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r = \begin{pmatrix} J_{k\times k} & O \\ O & O \end{pmatrix} \tag{6}$$

for some even $k \in \{2, \ldots, r\}$.

Suppose that $d = d(A, A + \sum_{i=1}^r \mathbf{x}_i^2)$ where $d \leqslant r+1$. Then there exist nonzero $\mathbf{y}_1, \ldots, \mathbf{y}_d \in \mathbb{F}_2^n$ such that $A + \sum_{i=1}^s \mathbf{y}_i^2 \in SGL_n(\mathbb{F}_2)$ for all $s \in \{1, \ldots, d\}$ and $\sum_{i=1}^d \mathbf{y}_i^2 = \sum_{i=1}^r \mathbf{x}_i^2$. If there exists i_0 such that $\mathbf{y}_{i_0} \notin \langle \mathbf{x}_1, \ldots, \mathbf{x}_r\rangle$, then

$$r+1 = \operatorname{rank}(\mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2 + \mathbf{y}_{i_0}^2) = \operatorname{rank}\left(\sum_{i\neq i_0} \mathbf{y}_i^2\right) \leqslant d-1 \leqslant r,$$

a contradiction. Hence, $\langle \mathbf{y}_1, \ldots, \mathbf{y}_d\rangle \subseteq \langle \mathbf{x}_1, \ldots, \mathbf{x}_r\rangle$. On the other hand,

$$\dim\langle \mathbf{y}_1, \ldots, \mathbf{y}_d\rangle \geqslant \operatorname{rank}(\mathbf{y}_1^2 + \cdots + \mathbf{y}_d^2) = \operatorname{rank}(\mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2) = r.$$

Consequently, $d \in \{r, r+1\}$ and $\langle \mathbf{y}_1, \ldots, \mathbf{y}_d\rangle = \langle \mathbf{x}_1, \ldots, \mathbf{x}_r\rangle$. In particular,

$$\mathbf{y}_i = \sum_{j=1}^r \alpha_j^{(i)} \mathbf{x}_j \qquad (i = 1, \ldots, d)$$

for some $\alpha_j^{(i)} \in \mathbb{F}_2$.

We next claim that whenever $\mathbf{y}_s^\top A^{-1}\mathbf{y}_s = 0$ for some s, we have also $\mathbf{y}_s^\top A^{-1}\mathbf{y}_t = 0$ for all t. In fact,

$$\begin{aligned} 0 = \mathbf{y}_s^\top A^{-1}\mathbf{y}_s &= \left(\sum_{j=1}^r \alpha_j^{(s)}\mathbf{x}_j\right)^\top A^{-1}\left(\sum_{j=1}^r \alpha_j^{(s)}\mathbf{x}_j\right) \\ &= \sum_{j=1}^r (\alpha_j^{(s)})^2 \mathbf{x}_j^\top A^{-1}\mathbf{x}_j = \sum_{j=1}^k \alpha_j^{(s)} \end{aligned}$$

and consequently

$$\begin{aligned}\mathbf{y}_s^\top A^{-1}\mathbf{y}_t &= \left(\sum_{j=1}^{r}\alpha_j^{(s)}\mathbf{x}_j\right)^\top A^{-1}\left(\sum_{i=1}^{r}\alpha_i^{(t)}\mathbf{x}_i\right)\\ &= \sum_{j=1}^{r}\sum_{i=1}^{r}\alpha_j^{(s)}\alpha_i^{(t)}\mathbf{x}_j^\top A^{-1}\mathbf{x}_i\\ &= \left(\sum_{j=1}^{k}\alpha_j^{(s)}\right)\cdot\left(\sum_{i=1}^{k}\alpha_i^{(t)}\right) = 0.\end{aligned}$$

Next, we use the induction to prove that $\mathbf{y}_s^\top A^{-1}\mathbf{y}_s = 0$ for all s, and therefore

$$\mathbf{y}_s^\top A^{-1}\mathbf{y}_t = 0 \text{ for all } s,t. \tag{7}$$

Since $1 = \det(A + \mathbf{y}_1^2) = 1 + \mathbf{y}_1^\top A^{-1}\mathbf{y}_1$, we deduce that $\mathbf{y}_1^\top A^{-1}\mathbf{y}_1 = 0$. To prove the inductive step assume that $0 = \mathbf{y}_1^\top A^{-1}\mathbf{y}_1 = \cdots = \mathbf{y}_{s-1}^\top A^{-1}\mathbf{y}_{s-1}$. Then,

$$\begin{aligned}1 &= \det\left(A + \sum_{i=1}^{s}\mathbf{y}_i^2\right)\\ &= \det\left(I_s + [\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^{s}\right)\\ &= \det\begin{pmatrix} I_{s-1} & O_{(s-1)\times 1}\\ O_{1\times(s-1)} & 1 + \mathbf{y}_s^\top A^{-1}\mathbf{y}_s\end{pmatrix} = 1 + \mathbf{y}_s^\top A^{-1}\mathbf{y}_s\end{aligned}$$

by Lemma 2.4. Hence, $\mathbf{y}_s^\top A^{-1}\mathbf{y}_s = 0$. This completes the proof of (7). Since $\langle \mathbf{y}_1, \ldots, \mathbf{y}_d\rangle = \langle \mathbf{x}_1, \ldots, \mathbf{x}_r\rangle$, both vectors $\mathbf{x}_1, \mathbf{x}_2$ are linear combinations of $\mathbf{y}_1, \ldots, \mathbf{y}_d$. Therefore, (7) implies that $\mathbf{x}_1^\top A^{-1}\mathbf{x}_2 = 0$, which contradicts (6). Consequently, $d(A, A + \sum_{i=1}^{r}\mathbf{x}_i^2) \geqslant r + 2$. □

In the case vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ are linearly independent and r is even, then Lemmas 4.5, 4.6, and 4.7 all provide some information on a rank-one perturbation of an alternate matrix of rank r, for fields of characteristic two.

Lemma 4.5. *Let $1 \leqslant s < r \leqslant n$ where s is an odd integer, and let $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \mathbb{F}^n$ where* $\operatorname{char}\mathbb{F} = 2$. *Suppose $\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, r\}$ is a subset with s elements and complement $\{i_{s+1}, \ldots, i_r\} = \{1, \ldots, r\}\backslash\{i_1, \ldots, i_s\}$. If*

$$\begin{aligned}\mathbf{w}_j &= \mathbf{x}_{i_j} + \mathbf{x}_{i_{s+1}} + \mathbf{x}_{i_{s+2}} + \cdots + \mathbf{x}_{i_r} && (j = 1, \ldots, s),\\ \mathbf{w}_k &= \mathbf{x}_{i_k} && (k = s+1, \ldots, r),\end{aligned}$$

then

$$\mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_r)^2 + (\mathbf{x}_{i_1} + \cdots + \mathbf{x}_{i_s})^2 = \mathbf{w}_1^2 + \cdots + \mathbf{w}_r^2.$$

Moreover, for all $C \in S_n(\mathbb{F})$ we have

$$\operatorname{rank}\left([\mathbf{w}_i^\top C\mathbf{w}_j]_{i,j\in\{1,\dots,r\}}\right) = \operatorname{rank}\left([\mathbf{x}_i^\top C\mathbf{x}_j]_{i,j\in\{1,\dots,r\}}\right) \tag{8}$$

and

$$\operatorname{Tr}[\mathbf{w}_i^\top C\mathbf{w}_j]_{i,j\in\{1,\dots,r\}} = \sum_{j=1}^{s} \mathbf{x}_{i_j}^\top C\mathbf{x}_{i_j}.$$

Proof. By applying the equality $(\mathbf{a}+\mathbf{b})^2 = \mathbf{a}^2 + \mathbf{b}^2 + \mathbf{a}\circ\mathbf{b}$ where $\mathbf{b} = \mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r}$ several times, we deduce that

$$\begin{aligned}
\mathbf{w}_1^2 + \cdots + \mathbf{w}_r^2 &= \sum_{j=1}^{r} \mathbf{x}_{i_j}^2 + (\mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r})^2 \cdot s \\
&\qquad + (\mathbf{x}_{i_1} + \cdots + \mathbf{x}_{i_s}) \circ (\mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r}) \\
&= \sum_{j=1}^{r} \mathbf{x}_{i_j}^2 + (\mathbf{x}_{i_1} + \cdots + \mathbf{x}_{i_r})^2 + (\mathbf{x}_{i_1} + \cdots + \mathbf{x}_{i_s})^2 \\
&= \sum_{j=1}^{r} \mathbf{x}_{j}^2 + (\mathbf{x}_{1} + \cdots + \mathbf{x}_{r})^2 + (\mathbf{x}_{i_1} + \cdots + \mathbf{x}_{i_s})^2.
\end{aligned}$$

Let X and W be the $n \times r$ matrices with $\mathbf{x}_i$ and $\mathbf{w}_i$ as the i-th column, respectively. Then, $W = XR$ for some $R \in GL_r(\mathbb{F})$. Therefore,

$$[\mathbf{w}_i^\top C\mathbf{w}_j]_{i,j=1}^r = W^\top CW = R^\top X^\top CXR = R^\top [\mathbf{x}_i^\top C\mathbf{x}_j]_{i,j=1}^r R$$

and $\operatorname{rank}\left([\mathbf{w}_i^\top C\mathbf{w}_j]_{i,j=1}^r\right) = \operatorname{rank}\left([\mathbf{x}_i^\top C\mathbf{x}_j]_{i,j=1}^r\right)$. Since s is odd, we deduce

$$\begin{aligned}
\operatorname{Tr}[\mathbf{w}_i^\top C\mathbf{w}_j]_{i,j=1}^r &= \sum_{i=1}^{r} \mathbf{w}_i^\top C\mathbf{w}_i \\
&= \sum_{j=1}^{s} (\mathbf{x}_{i_j} + \mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r})^\top C(\mathbf{x}_{i_j} + \mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r}) \\
&+ \sum_{j=s+1}^{r} \mathbf{x}_{i_j}^\top C\mathbf{x}_{i_j} \\
&= \sum_{j=1}^{s} \mathbf{x}_{i_j}^\top C\mathbf{x}_{i_j} + s \cdot \sum_{j=s+1}^{r} \mathbf{x}_{i_j}^\top C\mathbf{x}_{i_j} + \sum_{j=s+1}^{r} \mathbf{x}_{i_j}^\top C\mathbf{x}_{i_j} \\
&= \sum_{j=1}^{s} \mathbf{x}_{i_j}^\top C\mathbf{x}_{i_j}. \quad \square
\end{aligned}$$

Lemma 4.6. *Let $1 \leqslant s < r \leqslant n$ where s and r are even integers, and let $\mathbf{x}_1, \dots, \mathbf{x}_r \in \mathbb{F}^n$ where $\operatorname{char}\mathbb{F} = 2$. Suppose $\{i_1, \dots, i_s\} \subseteq \{1, \dots, r\}$ is a subset with s elements and $\{i_{s+1}, \dots, i_r\} = \{1, \dots, r\} \backslash \{i_1, \dots, i_s\}$ is its complement. If*

$$\begin{aligned} \mathbf{w}_j &= \mathbf{x}_{i_j} + \mathbf{x}_{i_{s+1}} + \mathbf{x}_{i_{s+2}} + \cdots + \mathbf{x}_{i_r} && (j = 1, \dots, s-1), \\ \mathbf{w}_s &= \mathbf{x}_{i_s}, \\ \mathbf{w}_k &= \mathbf{x}_{i_s} + \mathbf{x}_{i_k} && (k = s+1, \dots, r), \end{aligned}$$

then the same claim as in Lemma 4.5 is true.

Proof. By applying the equality $(\mathbf{a} + \mathbf{b})^2 = \mathbf{a}^2 + \mathbf{b}^2 + \mathbf{a} \circ \mathbf{b}$ several times, and recalling that s, r are both even, we deduce that

$$\begin{aligned} \sum_{j=1}^{r} \mathbf{w}_j^2 &= \sum_{j=1}^{r} \mathbf{x}_{i_j}^2 + (s-1) \cdot (\mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r})^2 \\ &+ \sum_{j=1}^{s-1} \mathbf{x}_{i_j} \circ (\mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r}) + (r-s) \cdot \mathbf{x}_{i_s}^2 + \sum_{j=s+1}^{r} \mathbf{x}_{i_j} \circ \mathbf{x}_{i_s} \\ &= \sum_{j=1}^{r} \mathbf{x}_{i_j}^2 + (\mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r})^2 \\ &+ (\mathbf{x}_{i_1} + \cdots + \mathbf{x}_{i_{s-1}}) \circ (\mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r}) + \mathbf{x}_{i_s} \circ (\mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r}) \\ &= \sum_{j=1}^{r} \mathbf{x}_{i_j}^2 + (\mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r})^2 + (\mathbf{x}_{i_1} + \cdots + \mathbf{x}_{i_s}) \circ (\mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r}) \\ &= \sum_{j=1}^{r} \mathbf{x}_{i_j}^2 + (\mathbf{x}_{i_1} + \cdots + \mathbf{x}_{i_r})^2 + (\mathbf{x}_{i_1} + \cdots + \mathbf{x}_{i_s})^2 \\ &= \sum_{j=1}^{r} \mathbf{x}_j^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_r)^2 + (\mathbf{x}_{i_1} + \cdots + \mathbf{x}_{i_s})^2 \end{aligned}$$

as claimed. We prove (8) in the same way as in the proof of Lemma 4.5. Finally,

$$\begin{aligned} \operatorname{Tr}[\mathbf{w}_i^\top C \mathbf{w}_j]_{i,j=1}^r &= \sum_{i=1}^{r} \mathbf{w}_i^\top C \mathbf{w}_i \\ &= \sum_{j=1}^{s-1} (\mathbf{x}_{i_j} + \mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r})^\top C (\mathbf{x}_{i_j} + \mathbf{x}_{i_{s+1}} + \cdots + \mathbf{x}_{i_r}) \\ &+ \mathbf{x}_{i_s}^\top C \mathbf{x}_{i_s} + \sum_{j=s+1}^{r} (\mathbf{x}_{i_j} + \mathbf{x}_{i_s})^\top C (\mathbf{x}_{i_j} + \mathbf{x}_{i_s}) \end{aligned}$$

$$= \sum_{j=1}^{s-1} \mathbf{x}_{i_j}^\top C\mathbf{x}_{i_j} + (s-1)\cdot \sum_{j=s+1}^{r} \mathbf{x}_{i_j}^\top C\mathbf{x}_{i_j}$$

$$+ \mathbf{x}_{i_s}^\top C\mathbf{x}_{i_s} + \sum_{j=s+1}^{r} \mathbf{x}_{i_j}^\top C\mathbf{x}_{i_j} + (r-s)\cdot \mathbf{x}_{i_s}^\top C\mathbf{x}_{i_s}$$

$$= \sum_{j=1}^{s} \mathbf{x}_{i_j}^\top C\mathbf{x}_{i_j}. \quad \square$$

Lemma 4.7. *Let* $\mathbf{x}_1,\dots,\mathbf{x}_r,\mathbf{v}\in\mathbb{F}^n$ *where* r *is even and* $\operatorname{char}\mathbb{F}=2$. *Then,*

$$\mathbf{x}_1^2+\cdots+\mathbf{x}_r^2+(\mathbf{x}_1+\cdots+\mathbf{x}_r)^2+\mathbf{v}^2 = (\mathbf{x}_1+\cdots+\mathbf{x}_r+\mathbf{v})^2+(\mathbf{x}_1+\mathbf{v})^2+\cdots+(\mathbf{x}_r+\mathbf{v})^2. \quad (9)$$

Proof. Since $(\mathbf{z}+\mathbf{w})^2=\mathbf{z}^2+\mathbf{w}^2+\mathbf{z}\circ\mathbf{w}$, the right-hand side of (9) equals

$$(\mathbf{x}_1+\cdots+\mathbf{x}_r)^2+\mathbf{v}^2+(\mathbf{x}_1+\cdots+\mathbf{x}_r)\circ\mathbf{v}+\sum_{i=1}^{r}(\mathbf{x}_i^2+\mathbf{v}^2+\mathbf{x}_i\circ\mathbf{v})$$

$$=(\mathbf{x}_1+\cdots+\mathbf{x}_r)^2+\mathbf{v}^2+r\cdot\mathbf{v}^2+\sum_{i=1}^{r}\mathbf{x}_i^2,$$

which equals the left-hand side of (9) because r is even. □

Lemma 4.8 is a special case of [35, Theorem 3], which is a version of Witt theorem for nonalternate symmetric bilinear forms over a field with characteristic two. We apply it in the proofs of Lemmas 4.9 and 4.10, which are used in the proof of Theorem 3.1. We apply Lemma 4.8 also in the proof of Theorem 8.10.

Lemma 4.8. *Let* U *be a vector subspace in* $\mathbb{F}_2^n$ *and let* $\sigma: U\to\mathbb{F}_2^n$ *be an injective linear map such that*

$$\sigma(\mathbf{u}_1)^\top\sigma(\mathbf{u}_2)=\mathbf{u}_1^\top\mathbf{u}_2 \quad (10)$$

for all $\mathbf{u}_1,\mathbf{u}_2\in U$. *Then,* σ *can be extended to an injective linear map* $\sigma:\mathbb{F}_2^n\to\mathbb{F}_2^n$ *such that* (10) *holds for all* $\mathbf{u}_1,\mathbf{u}_2\in\mathbb{F}_2^n$ *if and only if the following two conditions are satisfied:*

(i) $\mathbf{j}_n\in U$ *if and only if* $\mathbf{j}_n\in\sigma(U)$,
(ii) *if* $\mathbf{j}_n\in U$, *then* $\sigma(\mathbf{j}_n)=\mathbf{j}_n$.

Lemma 4.9. *Let* $A\in SGL_n(\mathbb{F}_2)$ *be a nonalternate matrix where* $n\geqslant 5$ *and assume that vectors* $\mathbf{x}_1,\mathbf{x}_2,\mathbf{x}_3\in\mathbb{F}_2^n$ *are linearly independent. If*

$$[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

then there exists $\mathbf{w} \in \mathbb{F}_2^n$ *such that*

$$\mathbf{w}^\top A^{-1}\mathbf{w} = 1 = \mathbf{w}^\top A^{-1}\mathbf{x}_1, \quad \mathbf{w}^\top A^{-1}\mathbf{x}_2 = 0 = \mathbf{w}^\top A^{-1}\mathbf{x}_3 \tag{11}$$

or

$$\mathbf{w}^\top A^{-1}\mathbf{w} = 1 = \mathbf{w}^\top A^{-1}\mathbf{x}_2, \quad \mathbf{w}^\top A^{-1}\mathbf{x}_1 = 0 = \mathbf{w}^\top A^{-1}\mathbf{x}_3. \tag{12}$$

Proof. Since A^{-1} is nonalternate, there exists $P \in GL_n(\mathbb{F}_2)$ such that $A^{-1} = P^\top P$. Denote $\dot{\mathbf{x}}_i = P\mathbf{x}_i$ for all i. Then,

$$[\dot{\mathbf{x}}_i^\top \dot{\mathbf{x}}_j]_{i,j=1}^3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

We split the proof in two cases.

Case 1. Let $\mathbf{j}_n \in \langle \dot{\mathbf{x}}_1, \dot{\mathbf{x}}_2, \dot{\mathbf{x}}_3 \rangle$. Suppose that n is even. Then, $\mathbf{j}_n^\top \mathbf{j}_n = 0$ and $\mathbf{j}_n \in \{\dot{\mathbf{x}}_3, \dot{\mathbf{x}}_1 + \dot{\mathbf{x}}_2, \dot{\mathbf{x}}_1 + \dot{\mathbf{x}}_2 + \dot{\mathbf{x}}_3\}$. Since $\mathbf{j}_n^\top \dot{\mathbf{x}}_1 = \dot{\mathbf{x}}_1^\top \dot{\mathbf{x}}_1 = 1$, and values $\dot{\mathbf{x}}_3^\top \dot{\mathbf{x}}_1$, $(\dot{\mathbf{x}}_1 + \dot{\mathbf{x}}_2)^\top \dot{\mathbf{x}}_1$, $(\dot{\mathbf{x}}_1 + \dot{\mathbf{x}}_2 + \dot{\mathbf{x}}_3)^\top \dot{\mathbf{x}}_1$ are all zero, we have a contradiction. Hence, n is odd, $\mathbf{j}_n^\top \mathbf{j}_n = 1$, and $\mathbf{j}_n \in \{\dot{\mathbf{x}}_1, \dot{\mathbf{x}}_2, \dot{\mathbf{x}}_1 + \dot{\mathbf{x}}_3, \dot{\mathbf{x}}_2 + \dot{\mathbf{x}}_3\}$. We consider two subcases.

Subcase 1. Let $\mathbf{j}_n \in \{\dot{\mathbf{x}}_1, \dot{\mathbf{x}}_1 + \dot{\mathbf{x}}_3\}$. Define vectors $\mathbf{y}_1 = \mathbf{j}_n$, $\mathbf{y}_2 = \mathbf{e}_1$, $\mathbf{y}_3 = \mathbf{e}_2 + \mathbf{e}_3$ and the map $\sigma : \langle \mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \rangle \to \mathbb{F}_2^n$ by

$$\sigma(\alpha_1\mathbf{y}_1 + \alpha_2\mathbf{y}_2 + \alpha_3\mathbf{y}_3) = \alpha_1\mathbf{j}_n + \alpha_2\dot{\mathbf{x}}_2 + \alpha_3\dot{\mathbf{x}}_3 \qquad (\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_2).$$

Then, σ is linear and injective. Moreover,

$$\sigma(\mathbf{j}_n) = \mathbf{j}_n \in \langle \mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \rangle \cap \sigma(\langle \mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \rangle),$$

and

$$[\mathbf{y}_i^\top \mathbf{y}_j]_{i,j=1}^3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = [\sigma(\mathbf{y}_i)^\top \sigma(\mathbf{y}_j)]_{i,j=1}^3. \tag{13}$$

Consequently,

$$\sigma(\mathbf{y})^\top \sigma(\mathbf{z}) = \mathbf{y}^\top \mathbf{z} \tag{14}$$

for all $\mathbf{y}, \mathbf{z} \in \langle \mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \rangle$. By Lemma 4.8, we can extend σ to a linear map σ on $\mathbb{F}_2^n$ such that (14) holds for all $\mathbf{y}, \mathbf{z} \in \mathbb{F}_2^n$. Then $\mathbf{w} = P^{-1}\sigma(\mathbf{e}_5)$ satisfies

$$\begin{aligned}
\mathbf{w}^\top A^{-1}\mathbf{w} &= \sigma(\mathbf{e}_5)^\top \sigma(\mathbf{e}_5) = \mathbf{e}_5^\top \mathbf{e}_5 = 1, \\
\mathbf{w}^\top A^{-1}\mathbf{x}_1 &= \sigma(\mathbf{e}_5)^\top \dot{\mathbf{x}}_1 \in \{\sigma(\mathbf{e}_5)^\top \sigma(\mathbf{j}_n), \sigma(\mathbf{e}_5)^\top \sigma(\mathbf{j}_n + \mathbf{y}_3)\} \\
&\qquad\qquad\qquad = \{\mathbf{e}_5^\top \mathbf{j}_n, \mathbf{e}_5^\top(\mathbf{j}_n + \mathbf{y}_3)\} = \{1\}, \\
\mathbf{w}^\top A^{-1}\mathbf{x}_2 &= \sigma(\mathbf{e}_5)^\top \sigma(\mathbf{y}_2) = \mathbf{e}_5^\top \mathbf{y}_2 = 0, \\
\mathbf{w}^\top A^{-1}\mathbf{x}_3 &= \sigma(\mathbf{e}_5)^\top \sigma(\mathbf{y}_3) = \mathbf{e}_5^\top \mathbf{y}_3 = 0.
\end{aligned}$$

Hence, (11) is true.

Subcase 2. Let $\mathbf{j}_n \in \{\dot{\mathbf{x}}_2, \dot{\mathbf{x}}_2 + \dot{\mathbf{x}}_3\}$. Here we define vectors $\mathbf{y}_1 = \mathbf{e}_1$, $\mathbf{y}_2 = \mathbf{j}_n$, $\mathbf{y}_3 = \mathbf{e}_2 + \mathbf{e}_3$ and the map $\sigma : \langle \mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \rangle \to \mathbb{F}_2^n$ by

$$\sigma(\alpha_1\mathbf{y}_1 + \alpha_2\mathbf{y}_2 + \alpha_3\mathbf{y}_3) = \alpha_1\dot{\mathbf{x}}_1 + \alpha_2\mathbf{j}_n + \alpha_3\dot{\mathbf{x}}_3 \qquad (\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_2).$$

Then we continue as in Subcase 1 to deduce that $\mathbf{w} = P^{-1}\sigma(\mathbf{e}_5)$ satisfies (12).

Case 2. Let $\mathbf{j}_n \notin \langle \dot{\mathbf{x}}_1, \dot{\mathbf{x}}_2, \dot{\mathbf{x}}_3 \rangle$. Suppose $n = 5$ and let $\dot{\mathbf{x}}_3 = (\beta_1, \beta_2, \beta_3, \beta_4, \beta_5)^\top$. Since $\dot{\mathbf{x}}_1, \dot{\mathbf{x}}_2$ are linearly independent, $1 = \dot{\mathbf{x}}_1^\top \dot{\mathbf{x}}_1 = \dot{\mathbf{x}}_2^\top \dot{\mathbf{x}}_2 = \dot{\mathbf{x}}_1^\top \dot{\mathbf{x}}_2$, and $\dot{\mathbf{x}}_1, \dot{\mathbf{x}}_2$ differ from $\mathbf{j}_5$, it follows that either

$$\{\dot{\mathbf{x}}_1, \dot{\mathbf{x}}_2\} = \{\mathbf{e}_i, \mathbf{e}_i + \mathbf{e}_j + \mathbf{e}_k\} \quad \text{or} \quad \{\dot{\mathbf{x}}_1, \dot{\mathbf{x}}_2\} = \{\mathbf{e}_i + \mathbf{e}_j + \mathbf{e}_k, \mathbf{e}_i + \mathbf{e}_l + \mathbf{e}_m\}$$

for some indices $\{i, j, k, l, m\} = \{1, 2, 3, 4, 5\}$. In both cases, the equalities $0 = \dot{\mathbf{x}}_1^\top \dot{\mathbf{x}}_3 = \dot{\mathbf{x}}_2^\top \dot{\mathbf{x}}_3 = \dot{\mathbf{x}}_3^\top \dot{\mathbf{x}}_3$ imply that $\beta_i = 0$, $\beta_j = \beta_k$, and $\beta_l = \beta_m$. Hence, $\dot{\mathbf{x}}_1 + \dot{\mathbf{x}}_3 = \mathbf{j}_5$ or $\dot{\mathbf{x}}_2 + \dot{\mathbf{x}}_3 = \mathbf{j}_5$ or $\dot{\mathbf{x}}_1 + \dot{\mathbf{x}}_2 + \dot{\mathbf{x}}_3 = 0$, which contradicts the assumption of Case 2 or the linear independence of $\dot{\mathbf{x}}_1, \dot{\mathbf{x}}_2, \dot{\mathbf{x}}_3$.

Therefore, $n \geqslant 6$. Define vectors $\mathbf{y}_1 = \mathbf{e}_1 + \cdots + \mathbf{e}_5$, $\mathbf{y}_2 = \mathbf{e}_1$, $\mathbf{y}_3 = \mathbf{e}_2 + \mathbf{e}_3$ and the map $\sigma : \langle \mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \rangle \to \mathbb{F}_2^n$ by

$$\sigma(\alpha_1\mathbf{y}_1 + \alpha_2\mathbf{y}_2 + \alpha_3\mathbf{y}_3) = \alpha_1\dot{\mathbf{x}}_1 + \alpha_2\dot{\mathbf{x}}_2 + \alpha_3\dot{\mathbf{x}}_3 \qquad (\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_2).$$

Then, $\mathbf{j}_n \notin \langle \dot{\mathbf{x}}_1, \dot{\mathbf{x}}_2, \dot{\mathbf{x}}_3 \rangle = \sigma(\langle \mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \rangle)$. Since $n \geqslant 6$, it follows that $\mathbf{j}_n \notin \langle \mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \rangle$. Moreover, (13) is still true, which implies (14) for all $\mathbf{y}, \mathbf{z} \in \langle \mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \rangle$. We continue as in Subcase 1 to see that $\mathbf{w} = P^{-1}\sigma(\mathbf{e}_5)$ fits (11). $\square$

Lemma 4.10. *Let $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \mathbb{F}_2^n$ be linearly independent vectors where r is an even number such that $2 \leqslant r \leqslant n$. If $A \in SGL_n(\mathbb{F}_2)$ and $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 1$ for all $i, j \leqslant r$, then there exists $\mathbf{x}_{r+1} \in \mathbb{F}_2^n$ such that*

$$\mathbf{x}_s^\top A^{-1}\mathbf{x}_{r+1} = 1 \text{ for some } s \in \{1, \ldots, r\} \tag{15}$$

and

$$\mathbf{x}_t^\top A^{-1}\mathbf{x}_{r+1} = 0 \text{ for all } t \in \{1,\dots,r+1\}\backslash\{s\}. \tag{16}$$

Remark 4.11. Observe that vectors $\mathbf{x}_1,\dots,\mathbf{x}_{r+1}$ must be linearly independent. In fact, if we pre-multiply the equation $\mathbf{x}_{r+1} = \sum_{k=1}^r \alpha_k \mathbf{x}_k$ by $\mathbf{x}_s^\top A^{-1}$ and by $\mathbf{x}_t^\top A^{-1}$ where $t \in \{1,\dots,r\}\backslash\{s\}$, respectively, then we deduce that $1 = \sum_{k=1}^r \alpha_k = 0$, which is not possible.

Proof. Clearly, A^{-1} is not alternate. Hence, there exists $P \in GL_n(\mathbb{F}_2)$ such that $A^{-1} = P^\top P$. Define $\dot{\mathbf{x}}_i = P\mathbf{x}_i$ for all i. Then, $\dot{\mathbf{x}}_i^\top \dot{\mathbf{x}}_j = 1$ for all i,j. In particular, $\operatorname{rank}\left([\dot{\mathbf{x}}_i^\top \dot{\mathbf{x}}_j]_{i,j}^r\right) = 1$. By Lemma 2.7, $r \leqslant \left\lfloor \frac{n+1}{2} \right\rfloor$, i.e. $n \geqslant 2r-1$. Firstly, we prove that

$$\text{if } n = 2r-1, \text{ then } \mathbf{j}_n \in \langle \dot{\mathbf{x}}_1,\dots,\dot{\mathbf{x}}_r\rangle. \tag{17}$$

In fact, if $n = 2r-1$ and $\mathbf{j}_n \notin \langle \dot{\mathbf{x}}_1,\dots,\dot{\mathbf{x}}_r\rangle$, then $\dot{\mathbf{x}}_1,\dots,\dot{\mathbf{x}}_r,\mathbf{j}_n$ are linearly independent. Since n is odd it follows that $\mathbf{j}_n^\top \mathbf{j}_n = 1 = \dot{\mathbf{x}}_i^\top \dot{\mathbf{x}}_i = \dot{\mathbf{x}}_i^\top \mathbf{j}_n$ for all i. As above, Lemma 2.7 implies that $r+1 \leqslant \left\lfloor \frac{n+1}{2} \right\rfloor = r$, a contradiction.

We split the rest of the proof in two cases.

Case 1. Let $\mathbf{j}_n \notin \langle \dot{\mathbf{x}}_1,\dots,\dot{\mathbf{x}}_r\rangle$. Define vectors $\mathbf{y}_i = \sum_{j=1}^{2i-1} \mathbf{e}_j$ for $i \in \{1,\dots,r\}$ and the map $\sigma : \langle \mathbf{y}_1,\dots,\mathbf{y}_r\rangle \to \mathbb{F}_2^n$ by

$$\sigma\left(\sum_{i=1}^r \alpha_i \mathbf{y}_i\right) = \sum_{i=1}^r \alpha_i \dot{\mathbf{x}}_i \qquad (\alpha_i \in \mathbb{F}_2).$$

Since $n \geqslant 2r$ by (17), it follows that $\mathbf{j}_n \notin \langle \mathbf{y}_1,\dots,\mathbf{y}_r\rangle$. Since $\sigma(\langle \mathbf{y}_1,\dots,\mathbf{y}_r\rangle) = \langle \dot{\mathbf{x}}_1,\dots,\dot{\mathbf{x}}_r\rangle$, it follows that $\mathbf{j}_n \notin \sigma(\langle \mathbf{y}_1,\dots,\mathbf{y}_r\rangle)$. Since $\mathbf{y}_i^\top \mathbf{y}_j = 1 = \sigma(\mathbf{y}_i)^\top \sigma(\mathbf{y}_j)$ for all i,j, we deduce (14) for all $\mathbf{y},\mathbf{z} \in \langle \mathbf{y}_1,\dots,\mathbf{y}_r\rangle$. By Lemma 4.8, we can linearly extend σ on whole $\mathbb{F}_2^n$ such that (14) is true for all $\mathbf{y},\mathbf{z} \in \mathbb{F}_2^n$. If $\mathbf{x}_{r+1} := P^{-1}\sigma(\mathbf{e}_1+\mathbf{e}_2)$, then

$$\begin{aligned}
\mathbf{x}_1^\top A^{-1}\mathbf{x}_{r+1} &= \dot{\mathbf{x}}_1^\top \sigma(\mathbf{e}_1+\mathbf{e}_2) = \sigma(\mathbf{y}_1)^\top \sigma(\mathbf{e}_1+\mathbf{e}_2) = \mathbf{y}_1^\top(\mathbf{e}_1+\mathbf{e}_2) = 1,\\
\mathbf{x}_t^\top A^{-1}\mathbf{x}_{r+1} &= \mathbf{y}_t^\top(\mathbf{e}_1+\mathbf{e}_2) = 0 \qquad (t \in \{2,\dots,r\}),\\
\mathbf{x}_{r+1}^\top A^{-1}\mathbf{x}_{r+1} &= (\mathbf{e}_1+\mathbf{e}_2)^\top(\mathbf{e}_1+\mathbf{e}_2) = 0,
\end{aligned}$$

as claimed.

Case 2. Let $\mathbf{j}_n \in \langle \dot{\mathbf{x}}_1,\dots,\dot{\mathbf{x}}_r\rangle$. Then $\mathbf{j}_n = \sum_{i=1}^r \beta_i \dot{\mathbf{x}}_i$ for some $\beta_i \in \mathbb{F}_2$. Hence,

$$1 = \dot{\mathbf{x}}_j^\top \dot{\mathbf{x}}_j = \dot{\mathbf{x}}_j^\top \mathbf{j}_n = \sum_{i=1}^r \beta_i \dot{\mathbf{x}}_j^\top \dot{\mathbf{x}}_i = \sum_{i=1}^r \beta_i \tag{18}$$

for all j, and therefore

$$\mathbf{j}_n^\top \mathbf{j}_n = \left(\sum_{j=1}^r \beta_j \dot{\mathbf{x}}_j\right)^\top \left(\sum_{i=1}^r \beta_i \dot{\mathbf{x}}_i\right) = \sum_{i,j=1}^r \beta_i\beta_j \dot{\mathbf{x}}_j^\top \dot{\mathbf{x}}_i = \left(\sum_{i=1}^r \beta_i\right)^2 = 1,$$

i.e. n is odd. Since r is even, (18) implies the existence of $s, k \in \{1, \ldots, r\}$ such that $\beta_s = 0$ and $\beta_k = 1$. Hence, vectors in the set $\{\mathbf{j}_n, \dot{\mathbf{x}}_1, \ldots, \dot{\mathbf{x}}_r\} \backslash \{\dot{\mathbf{x}}_k\}$ are linearly independent. Denote them by $\ddot{\mathbf{x}}_1, \ldots, \ddot{\mathbf{x}}_r$ in some order where $\ddot{\mathbf{x}}_1 = \dot{\mathbf{x}}_s$ and $\ddot{\mathbf{x}}_r = \mathbf{j}_n$. Further let $\mathbf{y}_m = \sum_{j=1}^{2m-1} \mathbf{e}_j$ for $m \in \{1, \ldots, r-1\}$ and $\mathbf{y}_r = \mathbf{j}_n$. Then $\mathbf{y}_1, \ldots, \mathbf{y}_r$ are linearly independent and the map $\sigma : \langle \mathbf{y}_1, \ldots, \mathbf{y}_r \rangle \to \mathbb{F}_2^n$,

$$\sigma\left(\sum_{i=1}^r \alpha_i \mathbf{y}_i\right) = \sum_{i=1}^r \alpha_i \ddot{\mathbf{x}}_i \qquad (\alpha_i \in \mathbb{F}_2),$$

is well defined. Moreover,

$$\sigma(\mathbf{j}_n) = \mathbf{j}_n \in \langle \mathbf{y}_1, \ldots, \mathbf{y}_r \rangle \cap \sigma(\langle \mathbf{y}_1, \ldots, \mathbf{y}_r \rangle).$$

Since $\mathbf{y}_i^\top \mathbf{y}_j = 1 = \sigma(\mathbf{y}_i)^\top \sigma(\mathbf{y}_j)$ for all i, j, we can apply Lemma 4.8 as above to extend σ linearly on whole $\mathbb{F}_2^n$ such that (14) is true for all $\mathbf{y}, \mathbf{z} \in \mathbb{F}_2^n$. If $\mathbf{x}_{r+1} := P^{-1}\sigma(\mathbf{e}_1 + \mathbf{e}_2)$, then

$$\begin{aligned}
\mathbf{x}_s^\top A^{-1} \mathbf{x}_{r+1} &= \dot{\mathbf{x}}_s^\top \sigma(\mathbf{e}_1 + \mathbf{e}_2) = \sigma(\mathbf{y}_1)^\top \sigma(\mathbf{e}_1 + \mathbf{e}_2) = \mathbf{y}_1^\top (\mathbf{e}_1 + \mathbf{e}_2) = 1, \\
\mathbf{x}_t^\top A^{-1} \mathbf{x}_{r+1} &= \sigma(\mathbf{e}_1 + \mathbf{e}_2 + \cdots)^\top \sigma(\mathbf{e}_1 + \mathbf{e}_2) = 0 \qquad (t \in \{1, \ldots, r\} \backslash \{s, k\}), \\
\mathbf{x}_{r+1}^\top A^{-1} \mathbf{x}_{r+1} &= \sigma(\mathbf{e}_1 + \mathbf{e}_2)^\top \sigma(\mathbf{e}_1 + \mathbf{e}_2) = 0, \\
\mathbf{x}_k^\top A^{-1} \mathbf{x}_{r+1} &= \dot{\mathbf{x}}_k^\top \sigma(\mathbf{e}_1 + \mathbf{e}_2) = \left(\mathbf{j}_n + \sum_{j \neq k, s} \beta_j \dot{\mathbf{x}}_j\right)^\top \sigma(\mathbf{e}_1 + \mathbf{e}_2) \\
&= \sigma\left(\mathbf{j}_n + \sum_{j=2}^{r-1} \beta_j \mathbf{y}_j\right)^\top \sigma(\mathbf{e}_1 + \mathbf{e}_2) = \left(\mathbf{j}_n + \sum_{j=2}^{r-1} \beta_j \mathbf{y}_j\right)^\top (\mathbf{e}_1 + \mathbf{e}_2) \\
&= 0,
\end{aligned}$$

as claimed. □

Recall from Section 2, that each nonalternate or alternate matrix $A \in S_n(\mathbb{F})$ of rank $r > 0$ over a finite field of characteristic two can be written as $A = \sum_{i=1}^r \mathbf{x}_i^2$ or $A = \sum_{i=1}^r \mathbf{x}_i^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_r)^2$, respectively where vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ are linearly independent. Typically, these forms are not unique. Lemma 4.12 implies that the corresponding vectors always span the same vector space.

Lemma 4.12. *Let $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \mathbb{F}^n$ be linearly independent and* $\operatorname{char} \mathbb{F} = 2$*. If*

$$\sum_{i=1}^r \mathbf{x}_i^2 = \sum_{i=1}^r \mathbf{y}_i^2 \quad \textit{where} \quad r \in \{1, \ldots, n\}$$

or

$$\sum_{i=1}^{r} \mathbf{x}_i^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_r)^2 = \sum_{i=1}^{r} \mathbf{y}_i^2 + (\mathbf{y}_1 + \cdots + \mathbf{y}_r)^2 \text{ where } r \in \{1, \ldots, n\} \text{ is even}$$

for some $\mathbf{y}_1, \ldots, \mathbf{y}_r \in \mathbb{F}^n$, *then* $\langle \mathbf{x}_1, \ldots, \mathbf{x}_r \rangle = \langle \mathbf{y}_1, \ldots, \mathbf{y}_r \rangle$.

Proof. Let $A_x \in \{\sum_{i=1}^r \mathbf{x}_i^2, \sum_{i=1}^r \mathbf{x}_i^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_r)^2\}$. Then, $\operatorname{rank} A_x = r$. If there exists j such that $\mathbf{y}_j \notin \langle \mathbf{x}_1, \ldots, \mathbf{x}_r \rangle$, then the equation $A_x = A_y$ where A_y is defined analogously as A_x implies that $r + 1 = \operatorname{rank}(A_x - \mathbf{y}_j^2) = \operatorname{rank}(A_y - \mathbf{y}_j^2) \leqslant r$, a contradiction. Hence, $\mathbf{y}_j \in \langle \mathbf{x}_1, \ldots, \mathbf{x}_r \rangle$ for all j. Since $\operatorname{rank} A_y = r$, it follows that $\langle \mathbf{x}_1, \ldots, \mathbf{x}_r \rangle = \langle \mathbf{y}_1, \ldots, \mathbf{y}_r \rangle$. □

In the case of a binary field, more relations between vectors $\mathbf{y}_1, \ldots, \mathbf{y}_r$ and $\mathbf{x}_1, \ldots, \mathbf{x}_r$ are provided by Lemma 4.14 and Lemma 4.15 (ii). On the other hand, Lemma 4.13 and Lemma 4.15 (i) give us some tools for the inductive step in the proof of Theorem 3.1.

Lemma 4.13. *Let* $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \mathbb{F}_2^n$ *be linearly independent where* $4 \leqslant r \leqslant n$. *Further, let* $A, A + \sum_{i=1}^r \mathbf{x}_i^2 \in SGL_n(\mathbb{F}_2)$ *and assume that* $\mathbf{x}_i^\top A^{-1} \mathbf{x}_i = 0$ *for some* $i \in \{1, \ldots, r\}$. *Then there exist* $\mathbf{y}_1, \ldots, \mathbf{y}_r \in \mathbb{F}_2^n$ *such that* $\sum_{i=1}^r \mathbf{x}_i^2 = \sum_{i=1}^r \mathbf{y}_i^2$ *and both matrices* $A + \sum_{i=1}^{r-2} \mathbf{y}_i^2, A + \sum_{i=1}^{r-1} \mathbf{y}_i^2$ *are in* $SGL_n(\mathbb{F}_2)$.

Proof. Let $B = A + \sum_{i=1}^r \mathbf{x}_i^2$. Define $S_0 = \{i \in \{1, \ldots, r\} : \mathbf{x}_i^\top B^{-1} \mathbf{x}_i = 0\}$ and $S_1 = \{i \in \{1, \ldots, r\} : \mathbf{x}_i^\top B^{-1} \mathbf{x}_i = 1\}$. By Corollary 2.5, $|S_0| \geqslant 1$. If $|S_0| = 1$ and $S_0 = \{j\}$, then there exist $k, l, m \in S_1$ and we can define vectors $\dot{\mathbf{x}}_1, \ldots, \dot{\mathbf{x}}_r$ by

$$\dot{\mathbf{x}}_t := \begin{cases} \mathbf{x}_t & \text{if} \quad t \notin \{j, k, l, m\}, \\ \mathbf{x}_t + \mathbf{x}_j + \mathbf{x}_k + \mathbf{x}_l + \mathbf{x}_m & \text{if} \quad t \in \{j, k, l, m\}. \end{cases}$$

Then,

$$1 = \dot{\mathbf{x}}_j^\top B^{-1} \dot{\mathbf{x}}_j, \; 0 = \dot{\mathbf{x}}_k^\top B^{-1} \dot{\mathbf{x}}_k = \dot{\mathbf{x}}_l^\top B^{-1} \dot{\mathbf{x}}_l = \dot{\mathbf{x}}_m^\top B^{-1} \dot{\mathbf{x}}_m$$

so the set $\dot{S}_0 = \{i \in \{1, \ldots, r\} : \dot{\mathbf{x}}_i^\top B^{-1} \dot{\mathbf{x}}_i = 0\}$ has three elements and $\sum_{i=1}^r \mathbf{x}_i^2 = \sum_{i=1}^r \dot{\mathbf{x}}_i^2$. Since we can replace vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ by $\dot{\mathbf{x}}_1, \ldots, \dot{\mathbf{x}}_r$, we assume in the rest of the proof that $|S_0| \geqslant 2$.

Next, we claim that there exist $i_1, i_2 \in \{1, \ldots, r\}$ such that

$$\begin{gathered} 0 = \mathbf{x}_{i_1}^\top B^{-1} \mathbf{x}_{i_1} = \mathbf{x}_{i_2}^\top B^{-1} \mathbf{x}_{i_2} = \mathbf{x}_{i_1}^\top B^{-1} \mathbf{x}_{i_2} \\ \text{or} \\ 0 = \mathbf{x}_{i_1}^\top B^{-1} \mathbf{x}_{i_1}, \; 1 = \mathbf{x}_{i_2}^\top B^{-1} \mathbf{x}_{i_2} = \mathbf{x}_{i_1}^\top B^{-1} \mathbf{x}_{i_2}. \end{gathered} \tag{19}$$

Suppose (19) is not true. Then, for each $s \in S_0$ the row s of the matrix $I_r + [\mathbf{x}_{j_1}^\top B^{-1}\mathbf{x}_{j_2}]_{j_1,j_2=1}^r$ equals $(a_1, \dots, a_r)$ where $a_{j_2} = 1$ if and only if $j_2 \in S_0$. Since $|S_0| \geqslant 2$, it follows that

$$\det\left(I_r + [\mathbf{x}_{j_1}^\top B^{-1}\mathbf{x}_{j_2}]_{j_1,j_2=1}^r\right) = 0.$$

On the other hand, Lemma 2.4 implies that

$$1 = \det A = \det\left(B + \sum_{i=1}^r \mathbf{x}_i^2\right) = \det\left(I_r + [\mathbf{x}_{j_1}^\top B^{-1}\mathbf{x}_{j_2}]_{j_1,j_2=1}^r\right),$$

a contradiction.

Let $\{\mathbf{y}_1, \dots, \mathbf{y}_r\} = \{\mathbf{x}_1, \dots, \mathbf{x}_r\}$ where $\mathbf{y}_{r-1} = \mathbf{x}_{i_2}$ and $\mathbf{y}_r = \mathbf{x}_{i_1}$. Then,

$$\det\left(A + \sum_{i=1}^{r-1} \mathbf{y}_i^2\right) = \det(B + \mathbf{y}_r^2) = 1 + \mathbf{y}_r^\top B^{-1}\mathbf{y}_r = 1,$$

$$\det\left(A + \sum_{i=1}^{r-2} \mathbf{y}_i^2\right) = \det(B + \mathbf{y}_{r-1}^2 + \mathbf{y}_r^2)$$

$$= \det\left(I_2 + \begin{pmatrix} \mathbf{y}_{r-1}^\top B^{-1}\mathbf{y}_{r-1} & \mathbf{y}_{r-1}^\top B^{-1}\mathbf{y}_r \\ \mathbf{y}_r^\top B^{-1}\mathbf{y}_{r-1} & \mathbf{y}_r^\top B^{-1}\mathbf{y}_r \end{pmatrix}\right) = 1,$$

as claimed. □

Lemma 4.14. *Suppose* $1 \leqslant r \leqslant n$*,* $A \in SGL_n(\mathbb{F}_2)$*, and* $\mathbf{x}_1, \dots, \mathbf{x}_r \in \mathbb{F}_2^n$ *are linearly independent. If* $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 1$ *for all* i, j*, and* $\sum_{i=1}^r \mathbf{x}_i^2 = \sum_{i=1}^r \mathbf{y}_i^2$ *for some vectors* $\mathbf{y}_1, \dots, \mathbf{y}_r \in \mathbb{F}_2^n$*, then* $\mathbf{y}_i^\top A^{-1}\mathbf{y}_j = 1$ *for all* i, j*.*

Proof. By Lemma 4.12, $\langle \mathbf{y}_1, \dots, \mathbf{y}_r \rangle = \langle \mathbf{x}_1, \dots, \mathbf{x}_r \rangle$. Hence, for each i there exist constants $\alpha_k^{(i)} \in \mathbb{F}_2$ s.t. $\mathbf{y}_i = \sum_{j=1}^r \alpha_k^{(i)}\mathbf{x}_k$. Let $X, Y \in M_{n\times r}(\mathbb{F}_2)$ and $P \in M_{r\times r}(\mathbb{F}_2)$ be the matrices with the i-th column equal to $\mathbf{x}_i$, $\mathbf{y}_i$ and $\mathbf{p}_i = (\alpha_1^i, \dots, \alpha_r^i)^\top$, respectively. Obviously, $Y = XP$. Therefore,

$$XX^\top = \mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2 = \mathbf{y}_1^2 + \cdots + \mathbf{y}_r^2 = YY^\top = XPP^\top X^\top,$$

i.e. $X(I_r - PP^\top)X^\top = 0$. Since $\operatorname{rank} X = r$, we deduce that $P^\top = P^{-1}$. Hence,

$$[\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^r = Y^\top A^{-1} Y = P^\top X^\top A^{-1} X P = P^\top J P =: \mathbf{z}^2$$

where $\mathbf{z} = (z_1, \dots, z_r)^\top = P^\top \mathbf{j}_r$. Since $I_r = P^\top P = [\mathbf{p}_i^\top \mathbf{p}_j]_{i,j=1}^r$, it follows that $\mathbf{p}_i^\top \mathbf{p}_i = 1$ for all i. Since the underlying field is $\mathbb{F}_2$, we deduce that $z_i = \mathbf{p}_i^\top \mathbf{j}_r = \mathbf{p}_i^\top \mathbf{p}_i = 1$ for all i. Hence, $[\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^r = J$ as claimed. □

Lemma 4.15. *Let $A \in SGL_n(\mathbb{F}_2)$ and let $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \mathbb{F}_2^n$ be linearly independent where $2 \leqslant r \leqslant n$, $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r \in \mathcal{R}_1^{\mathrm{Tr}_0}$, and $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 0$ for some i, j.*

(i) *Let $k \in \{2, \ldots, r-1\}$ be even. Then, there exist linearly independent vectors $\mathbf{y}_1, \ldots, \mathbf{y}_r \in \mathbb{F}_2^n$ and a permutation matrix $Q \in GL_r(\mathbb{F}_2)$ such that*

$$\sum_{i=1}^r \mathbf{x}_i^2 = \sum_{i=1}^r \mathbf{y}_i^2, \quad \sum_{i=1}^r \mathbf{x}_i = \sum_{i=1}^r \mathbf{y}_i, \tag{20}$$

and

$$[\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^r = Q \begin{pmatrix} J_{k\times k} & O \\ O & O \end{pmatrix} Q^\top.$$

(ii) *If $\sum_{i=1}^r \mathbf{x}_i^2 = \sum_{i=1}^r \mathbf{y}_i^2$ for some $\mathbf{y}_1, \ldots, \mathbf{y}_r \in \mathbb{F}_2^n$, then $[\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^r \in \mathcal{R}_1^{\mathrm{Tr}_0}$ and $\mathbf{y}_{i'}^\top A^{-1}\mathbf{y}_{j'} = 0$ for some i', j'.*

Proof. (i) The linear independence of $\mathbf{y}_1, \ldots, \mathbf{y}_r$ will follow from Lemma 4.12 and (20). By Lemma 2.2, there is a permutation matrix $Q \in GL_r(\mathbb{F}_2)$ s.t.

$$[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r = Q \begin{pmatrix} J_{l\times l} & O \\ O & O \end{pmatrix} Q^\top \tag{21}$$

for some even $l \in \{2, \ldots, r\}$. By the assumption, $l \leqslant r-1$. To simplify writings we assume that $Q = I_r$. The claim is obvious if $k = l$. Moreover, since we can apply an induction process, it suffices to prove the claim for the case $k = l+2$ whenever $l+2 \leqslant r-1$ and for the case $k = l-2$ whenever $l-2 \geqslant 2$.

Case 1. Let $k = l+2$ and $l+3 \leqslant r$. Define vectors $\mathbf{y}_1, \ldots, \mathbf{y}_r$ by

$$\mathbf{y}_i := \begin{cases} \mathbf{x}_i & \text{if} \quad i \notin \{l, l+1, l+2, l+3\}, \\ \mathbf{x}_i + \mathbf{x}_l + \mathbf{x}_{l+1} + \mathbf{x}_{l+2} + \mathbf{x}_{l+3} & \text{if} \quad i \in \{l, l+1, l+2, l+3\}. \end{cases}$$

Then, (20) is true and

$$\begin{aligned} [\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^r &= \begin{pmatrix} J_{(l-1)\times(l-1)} & O_{(l-1)\times 1} & J_{(l-1)\times 3} & O \\ O_{1\times(l-1)} & 0 & O_{1\times 3} & O \\ J_{3\times(l-1)} & O_{3\times 1} & J_{3\times 3} & O \\ O & O & O & O \end{pmatrix} \\ &= \dot{Q} \begin{pmatrix} J_{(l+2)\times(l+2)} & O \\ O & O \end{pmatrix} \dot{Q}^\top \end{aligned}$$

for appropriate permutation matrix $\dot{Q}$.

Case 2. Let $k = l - 2$ and $l \geqslant 4$. Define vectors $\mathbf{y}_1, \ldots, \mathbf{y}_r$ by

$$\mathbf{y}_i := \begin{cases} \mathbf{x}_i & \text{if} \quad i \notin \{l-2, l-1, l, l+1\}, \\ \mathbf{x}_i + \mathbf{x}_{l-2} + \mathbf{x}_{l-1} + \mathbf{x}_l + \mathbf{x}_{l+1} & \text{if} \quad i \in \{l-2, l-1, l, l+1\}. \end{cases}$$

Then, (20) is true and

$$[\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^r = \begin{pmatrix} J_{(l-3)\times(l-3)} & O_{(l-3)\times 3} & \mathbf{j}_{l-3} & O \\ O_{3\times(l-3)} & O_{3\times 3} & O_{3\times 1} & O \\ \mathbf{j}_{l-3}^\top & O_{1\times 3} & 1 & O \\ O & O & O & O \end{pmatrix}$$

$$= \dot{Q} \begin{pmatrix} J_{(l-2)\times(l-2)} & O \\ O & O \end{pmatrix} \dot{Q}^\top$$

for appropriate permutation matrix $\dot{Q}$.

(ii) By Lemma 4.12, $\langle \mathbf{y}_1, \ldots, \mathbf{y}_r \rangle = \langle \mathbf{x}_1, \ldots, \mathbf{x}_r \rangle$ so $\mathbf{y}_1, \ldots, \mathbf{y}_r$ are linearly independent. By (i), we may assume that in (21), $l = 2$ and $Q = I_r$. If we multiply the equation

$$\mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2 = \mathbf{y}_1^2 + \cdots + \mathbf{y}_r^2 \tag{22}$$

from the right-hand side by $A^{-1}\mathbf{x}_1$ and $A^{-1}\mathbf{x}_2$, respectively, we deduce that

$$\sum_{i=1}^r \mathbf{y}_i \cdot \mathbf{y}_i^\top A^{-1}\mathbf{x}_1 = \mathbf{x}_1 + \mathbf{x}_2 = \sum_{i=1}^r \mathbf{y}_i \cdot \mathbf{y}_i^\top A^{-1}\mathbf{x}_2.$$

The linear independence of $\mathbf{y}_1, \ldots, \mathbf{y}_r$ implies that $\mathbf{y}_i^\top A^{-1}\mathbf{x}_1 = \mathbf{y}_i^\top A^{-1}\mathbf{x}_2 =: b_i$ for all $i \in \{1, \ldots, r\}$. Moreover, there exists $i_0 \in \{1, \ldots, r\}$ such that $b_{i_0} = 1$. If we multiply (22) by $A^{-1}\mathbf{x}_j$, we deduce that

$$\mathbf{y}_i^\top A^{-1}\mathbf{x}_j = 0 \qquad (i \in \{1, \ldots, r\}, j \in \{3, \ldots, r\}). \tag{23}$$

Let $c_{ij} := \mathbf{y}_i^\top A^{-1}\mathbf{y}_j$. Then $c_{ji} = c_{ij}$. If we multiply (22) by $A^{-1}\mathbf{y}_i$, (23) implies

$$b_i(\mathbf{x}_1 + \mathbf{x}_2) = \sum_{j=1}^r c_{ji}\mathbf{y}_j \qquad (i \in \{1, \ldots, r\}). \tag{24}$$

Let $S_1 = \{i \in \{1, \ldots, r\} : b_i = 1\}$ and $S_0 = \{i \in \{1, \ldots, r\} : b_i = 0\}$. If $i \in S_0$, then (24) and the linear independence of $\mathbf{y}_1, \ldots, \mathbf{y}_r$ show that

$$c_{ij} = c_{ji} = 0 \qquad (j \in \{1, \ldots, r\}). \tag{25}$$

Moreover, if $i_1, i_2 \in S_1$, then the same arguments imply that

$$c_{ji_1} = c_{ji_2} = c_{i_2j} = c_{i_1j} \qquad (j \in \{1, \dots, r\}). \tag{26}$$

Since $i_0 \in S_1$, (24) implies the existence of $j \in \{1, \dots, r\}$ such that $c_{ji_0} = 1$. By (25), $j \in S_1$. Consequently, (26) implies that $c_{i_1 i_0} = 1$ for all $i_1 \in S_1$ and therefore $c_{i_1 i_2} = 1$ for all $i_1, i_2 \in S_1$. Along (25), it implies that the matrix $[c_{ij}]_{i,j=1}^r = [\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^r$ is of rank one. Moreover, (24) implies that $\mathbf{x}_1 + \mathbf{x}_2 = \sum_{j\in S_1} \mathbf{y}_j$ and consequently

$$\begin{aligned} 0 &= \mathbf{x}_1^\top A^{-1}\mathbf{x}_1 + \mathbf{x}_2^\top A^{-1}\mathbf{x}_2 \\ &= (\mathbf{x}_1 + \mathbf{x}_2)^\top A^{-1}(\mathbf{x}_1 + \mathbf{x}_2) = \sum_{j\in S_1} \mathbf{y}_j^\top A^{-1}\mathbf{y}_j = |S_1| \pmod 2, \end{aligned}$$

i.e. $[\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^r \in \mathcal{R}_1^{\mathrm{Tr}_0}$. By Lemma 4.14, $\mathbf{y}_{i'}^\top A^{-1}\mathbf{y}_{j'} = 0$ for some i', j'. □

5. Proof of Theorem 3.1

Firstly, we prove the cases $r \leqslant 2$ and $r = 3$.

Proof of Theorem 3.1 for $r \leqslant 2$. If $r = 1$, then obviously $d(A, B) = r$. This is also claimed by Theorem 3.1 because $1 = \det B = \det(A + \mathbf{x}_1^2) = 1 + \mathbf{x}_1^\top A^{-1}\mathbf{x}_1$ implies that $\mathbf{x}_1^\top A^{-1}\mathbf{x}_1 = 0$, and therefore the assumption (iii) holds.

Let $r = 2$. By Lemma 2.4, $1 = \det B = \det(I_2 + [\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^2)$, i.e.

$$\mathbf{x}_1^\top A^{-1}\mathbf{x}_1 + \mathbf{x}_2^\top A^{-1}\mathbf{x}_2 + \mathbf{x}_1^\top A^{-1}\mathbf{x}_1 \cdot \mathbf{x}_2^\top A^{-1}\mathbf{x}_2 - (\mathbf{x}_1^\top A^{-1}\mathbf{x}_2)^2 = 0. \tag{27}$$

We separate two cases.

Case 1. Let $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 0$ for some $i \in \{1, 2\}$. If $j \in \{1, 2\}\backslash\{i\}$, then (27) implies that $\mathbf{x}_j^\top A^{-1}\mathbf{x}_j = \mathbf{x}_i^\top A^{-1}\mathbf{x}_j$, and therefore the assumption (iii) holds. Moreover, $\det(A + \mathbf{x}_i^2) = 1 + \mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1$. Hence, $A + \mathbf{x}_i^2$ is adjacent to both A and B, i.e. $d(A, B) \leqslant 2$. From (2) we deduce that $d(A, B) = 2$ as claimed.

Case 2. Let $\mathbf{x}_1^\top A^{-1}\mathbf{x}_1 = 1 = \mathbf{x}_2^\top A^{-1}\mathbf{x}_2$. Then, (27) implies that $\mathbf{x}_1^\top A^{-1}\mathbf{x}_2 = 1$. As indicated in Remark 3.2, we need to prove that $d(A, B) = 4$. Since $\mathbf{x}_1^\top A^{-1}\mathbf{x}_1 \neq 0$, it follows that A^{-1} is nonalternate. Hence, $A^{-1} = P^\top P$ for some $P \in GL_n(\mathbb{F}_2)$. Since vectors $P\mathbf{x}_1, P\mathbf{x}_2$ are linearly independent, they are nonzero, and at least one of them is different from $\mathbf{j}_n$. We may assume that $P\mathbf{x}_1 =: (\alpha_1, \dots, \alpha_n)^\top$ is such. Then there exist j, k such that $\alpha_j = 0$ and $\alpha_k = 1$. Let $\mathbf{y} = P^{-1}(\mathbf{e}_j + \mathbf{e}_k)$. Then $\mathbf{y}^\top A^{-1}\mathbf{y} = 0$ and $\mathbf{y}^\top A^{-1}\mathbf{x}_1 = 1$. Consequently, regardless of the value $\mathbf{y}^\top A^{-1}\mathbf{x}_2$, Lemma 2.4 implies that

$$\begin{aligned} &\det(A + \mathbf{y}^2) = 1 + \mathbf{y}^\top A^{-1}\mathbf{y} = 1, \\ &\det(A + \mathbf{y}^2 + \mathbf{x}_1^2) = \det\left(I_2 + \begin{pmatrix} \mathbf{y}^\top A^{-1}\mathbf{y} & \mathbf{y}^\top A^{-1}\mathbf{x}_1 \\ \mathbf{y}^\top A^{-1}\mathbf{x}_1 & \mathbf{x}_1^\top A^{-1}\mathbf{x}_1 \end{pmatrix}\right) = 1, \end{aligned}$$

$$\det(A + \mathbf{y}^2 + \mathbf{x}_1^2 + \mathbf{x}_2^2)$$
$$= \det\left(I_3 + \begin{pmatrix} \mathbf{y}^\top A^{-1}\mathbf{y} & \mathbf{y}^\top A^{-1}\mathbf{x}_1 & \mathbf{y}^\top A^{-1}\mathbf{x}_2 \\ \mathbf{y}^\top A^{-1}\mathbf{x}_1 & \mathbf{x}_1^\top A^{-1}\mathbf{x}_1 & \mathbf{x}_1^\top A^{-1}\mathbf{x}_2 \\ \mathbf{y}^\top A^{-1}\mathbf{x}_2 & \mathbf{x}_1^\top A^{-1}\mathbf{x}_2 & \mathbf{x}_2^\top A^{-1}\mathbf{x}_2 \end{pmatrix}\right) = 1,$$

which means that $A \sim A+\mathbf{y}^2 \sim A+\mathbf{y}^2+\mathbf{x}_1^2 \sim A+\mathbf{y}^2+\mathbf{x}_1^2+\mathbf{x}_2^2 \sim B$. Hence, $d(A,B) \leqslant 4$. By Lemma 4.4, $d(A,B) = 4$. □

Proof of Theorem 3.1 for $r = 3$. By Lemma 2.4,

$$1 = \det B = \det\left(I_3 + [\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^3\right). \tag{28}$$

Since alternate matrices have even rank, there exists $k \in \{1,2,3\}$ such that $\mathbf{x}_k^\top A^{-1}\mathbf{x}_k = 0$. We separate two cases.

Case 1. Let $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^3 \in \mathcal{R}_1^{\mathrm{Tr}0}$. Then we may assume that

$$[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^3 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{29}$$

(otherwise we permute vectors $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$). Let $Q \in GL_n(\mathbb{F}_2)$ be any invertible matrix with $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ as the first three columns. Then, (29) is the top-left 3×3 block of the invertible matrix $Q^\top A^{-1} Q \in SGL_n(\mathbb{F}_2)$. Hence, $n > 3$. Moreover, a straightforward computation of the determinant shows that no member of $SGL_4(\mathbb{F}_2)$ has (29) in the top-left corner. Hence, $n \geqslant 5$. By Lemma 4.9, there exists $\mathbf{w} \in \mathbb{F}_2^n$ such that (11) or (12) is true. We may assume (11) (otherwise we permute vectors $\mathbf{x}_1, \mathbf{x}_2$). Now, we can apply Lemma 2.4 as in the proof for $r = 2$ to deduce that matrices in the path

$$\begin{aligned} A &\sim A + (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^2 \\ &\sim A + (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^2 + \mathbf{w}^2 \\ &\sim A + (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^2 + \mathbf{w}^2 + (\mathbf{x}_1 + \mathbf{x}_3 + \mathbf{w})^2 \\ &\sim A + (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^2 + \mathbf{w}^2 + (\mathbf{x}_1 + \mathbf{x}_3 + \mathbf{w})^2 + (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{w})^2 \\ &= A + \mathbf{x}_1^2 + \mathbf{x}_2^2 + \mathbf{x}_3^2 + (\mathbf{x}_2 + \mathbf{x}_3 + \mathbf{w})^2 \sim B \end{aligned}$$

have determinant one. Hence, $d(A,B) \leqslant 5$. By Lemma 4.4, $d(A,B) = 5$.

Case 2. Let $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^3 \notin \mathcal{R}_1^{\mathrm{Tr}0}$. Since $\mathbf{x}_k^\top A^{-1}\mathbf{x}_k = 0$, the assumption of (iii) is satisfied. We may assume that $k = 3$ (otherwise we suitably permute vectors $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_3$). We claim that there exist distinct $i, j \in \{1,2,3\}$ such that

$$0 = \mathbf{x}_i^\top A^{-1}\mathbf{x}_i = \mathbf{x}_j^\top A^{-1}\mathbf{x}_j = \mathbf{x}_i^\top A^{-1}\mathbf{x}_j$$
$$\text{or} \tag{30}$$
$$0 = \mathbf{x}_i^\top A^{-1}\mathbf{x}_i,\ 1 = \mathbf{x}_j^\top A^{-1}\mathbf{x}_j = \mathbf{x}_i^\top A^{-1}\mathbf{x}_j.$$

To prove (30) we separate three subcases.

Subcase 1. Let $\mathbf{x}_1^\top A^{-1}\mathbf{x}_1 = 0 = \mathbf{x}_2^\top A^{-1}\mathbf{x}_2$. If (30) is not true, then the invertible matrix in the right-hand side of (28) equals $J_{3\times 3}$, a contradiction.

Subcase 2. Let $\mathbf{x}_1^\top A^{-1}\mathbf{x}_1 = 1 = \mathbf{x}_2^\top A^{-1}\mathbf{x}_2$. If (30) is not true, then $\mathbf{x}_1^\top A^{-1}\mathbf{x}_3 = 0 = \mathbf{x}_2^\top A^{-1}\mathbf{x}_3$. Since $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^3 \notin \mathcal{R}_1^{\mathrm{Tr}_0}$, we have $\mathbf{x}_1^\top A^{-1}\mathbf{x}_2 = 0$. This is a contradiction because the invertible matrix in the right-hand side of (28) is

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Subcase 3. Let $\{\mathbf{x}_1^\top A^{-1}\mathbf{x}_1, \mathbf{x}_2^\top A^{-1}\mathbf{x}_2\} = \{0, 1\}$. If (30) is not true, then we get in contradiction as above, i.e. the matrix in the right-hand side of (28) equals

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Now, if i, j are as in (30), then Lemma 2.4 implies that matrices in the path

$$A \sim A + \mathbf{x}_i^2 \sim A + \mathbf{x}_i^2 + \mathbf{x}_j^2 \sim A + \mathbf{x}_1^2 + \mathbf{x}_2^2 + \mathbf{x}_3^2 = B$$

have determinant one. Hence, $d(A, B) \leqslant 3$. By (2), $d(A, B) = 3$ as claimed. □

The proof of Theorem 3.1 for $r \geqslant 4$ applies the induction process. In it, we say that a pair of matrices (A, B) in $SGL_n(\mathbb{F}_2)$ satisfy the condition (i), (ii), or (iii) with respect to vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ if the conditions (i), (ii), or (iii) in the statement of Theorem 3.1 are satisfied, respectively.

Proof of Theorem 3.1 for $r \geqslant 4$**.** We already know that the claim is true for $r \in \{1, 2, 3\}$. Let $r \geqslant 4$ and assume the claim is true for values $1, 2, \ldots, r-1$. We separate three cases.

Case 1. Let (ii) be satisfied and assume (i) is not, i.e. $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r \neq J_{r\times r}$. By Lemma 2.2, there exists i_0 such that $\mathbf{x}_{i_0}^\top A^{-1}\mathbf{x}_j = 0 = \mathbf{x}_j^\top A^{-1}\mathbf{x}_{i_0}$ for all j. Hence, $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j\in\{1,\ldots,r\}\setminus\{i_0\}} \in \mathcal{R}_1^{\mathrm{Tr}_0}$. By Lemma 2.2, there exists a permutation matrix $Q \in GL_{r-1}(\mathbb{F}_2)$ such that

$$[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j\in\{1,\ldots,r\}\setminus\{i_0\}} = Q\begin{pmatrix} J_{k\times k} & O \\ O & O \end{pmatrix} Q^\top$$

for some even $k \geqslant 2$. Let $B' = A + \sum_{i\neq i_0} \mathbf{x}_i^2$. By Lemma 2.4,

$$\begin{aligned}\det B' &= \det\left(I_{r-1} + [\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j\in\{1,\ldots,r\}\setminus\{i_0\}}\right)\\ &= \det\left(Q\begin{pmatrix} I_k + J_{k\times k} & O \\ O & I_{r-1-k}\end{pmatrix} Q^\top\right)\\ &= \det(I_k + \mathbf{j}_k^2)\\ &= 1 + \mathbf{j}_k^\top \mathbf{j}_k = 1\end{aligned}$$

because k is even. Hence, $B' \in SGL_n(\mathbb{F}_2)$. By the induction hypothesis, $d(A, B') \leqslant (r-1) + 2 = r+1$. Consequently, $d(A, B) \leqslant d(A, B') + d(B', B) \leqslant r+2$. By Lemma 4.4, $d(A, B) = r+2$ as claimed.

Case 2. Let (iii) be satisfied. Then, there exists i such that $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 0$. By Lemma 4.13, there exist $\mathbf{y}_1, \ldots, \mathbf{y}_r \in \mathbb{F}_2^n$ such that $\sum_{i=1}^r \mathbf{x}_i^2 = \sum_{i=1}^r \mathbf{y}_i^2$ and both matrices $B'' = A + \sum_{i=1}^{r-2} \mathbf{y}_i^2$ and $B' = A + \sum_{i=1}^{r-1} \mathbf{y}_i^2$ are in $SGL_n(\mathbb{F}_2)$. Moreover, $\mathbf{y}_1, \ldots, \mathbf{y}_r$ are linearly independent by Lemma 4.12. By Lemma 2.4,

$$1 = \det B' = \det\left(I_{r-1} + [\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^{r-1}\right) \tag{31}$$

and

$$1 = \det B'' = \det\left(I_{r-2} + [\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^{r-2}\right). \tag{32}$$

Therefore, there exist $i_0, j_0 \leqslant r-1$ such that

$$\mathbf{y}_{i_0}^\top A^{-1}\mathbf{y}_{j_0} = 0. \tag{33}$$

In fact, the opposite would force the matrices in the right-hand side of (31), (32) to be alternate, a contradiction because such matrices have even rank, while one of the numbers $r-2$ and $r-1$ is odd. We split Case 2 into three subcases, depending on the type of the pair (A, B') with respect to vectors $\mathbf{y}_1, \ldots, \mathbf{y}_{r-1}$.

Subcase 1. Suppose that (A, B') satisfy the condition (ii). By Lemma 4.15 (i) and (33), we may assume that

$$[\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^{r-1} = Q\begin{pmatrix} J_{2\times 2} & O \\ O & O\end{pmatrix} Q^\top$$

for some permutation matrix $Q \in GL_{r-1}(\mathbb{F}_2)$. If $\dot{Q} \in GL_r(\mathbb{F}_2)$ is the permutation matrix with Q in the top-left corner and 1 in the (r, r)-entry, then

$$[\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^r = \dot{Q}\begin{pmatrix} J_{2\times 2} & O & \dot{\mathbf{b}} \\ O & O & \ddot{\mathbf{b}} \\ \dot{\mathbf{b}}^\top & \ddot{\mathbf{b}}^\top & b_r \end{pmatrix}\dot{Q}^\top \tag{34}$$

for some $\dot{\mathbf{b}} = (b_1, b_2)^\top \in \mathbb{F}_2^2$, $\ddot{\mathbf{b}} = (b_3, \ldots, b_{r-1})^\top \in \mathbb{F}_2^{r-3}$, $b_r \in \mathbb{F}_2$. Since

$$\begin{aligned} 1 = \det B &= \det\left(I_r + [\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^r\right) \\ &= \det\left(\dot{Q}\begin{pmatrix} J_{2\times 2}+I_2 & O & \dot{\mathbf{b}} \\ O & I_{r-3} & \ddot{\mathbf{b}} \\ \dot{\mathbf{b}}^\top & \ddot{\mathbf{b}}^\top & 1+b_r \end{pmatrix}\dot{Q}^\top\right) \\ &= \det\begin{pmatrix} J_{2\times 2}+I_2 & O & \dot{\mathbf{b}} \\ O & I_{r-3} & \ddot{\mathbf{b}} \\ \dot{\mathbf{b}}^\top & \ddot{\mathbf{b}}^\top & 1+b_r \end{pmatrix}, \end{aligned} \tag{35}$$

the last column of the matrix in (35) is not a linear combination of the other columns. Hence, $1 + b_r \neq b_3 + \cdots + b_{r-1}$, i.e.

$$b_r = b_3 + \cdots + b_{r-1}. \tag{36}$$

Since $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r \notin \mathcal{R}_1^{\mathrm{Tr}_0}$ by the assumption of Case 2, Lemma 4.15 (ii) implies that $(b_1, \ldots, b_r)$ is not the zero vector. Moreover, (34) implies that

$$[\mathbf{y}_{\sigma(i)}^\top A^{-1}\mathbf{y}_{\sigma(j)}]_{i,j=1}^r = \begin{pmatrix} J_{2\times 2} & O & \dot{\mathbf{b}} \\ O & O & \ddot{\mathbf{b}} \\ \dot{\mathbf{b}}^\top & \ddot{\mathbf{b}}^\top & b_r \end{pmatrix}$$

for some permutation σ of the set $\{1, \ldots, r\}$.

If there exists $s \in \{1, 2\}$ such that $b_s = 1$ and $\{t\} = \{1, 2\}\backslash\{s\}$, then we can consider the matrix $\dot{B}' = A + \sum_{i\neq\sigma(t)} \mathbf{y}_i^2$. Since

$$[\mathbf{y}_{\sigma(i)}^\top A^{-1}\mathbf{y}_{\sigma(j)}]_{i,j\in\{1,\ldots,r\}\backslash\{t\}} = \begin{pmatrix} 1 & O & 1 \\ O & O & \ddot{\mathbf{b}} \\ 1 & \ddot{\mathbf{b}}^\top & b_r \end{pmatrix},$$

we have $\dot{B}' \in SGL_n(\mathbb{F}_2)$ by Lemma 2.4. If $(A, \dot{B}')$ is of type (ii) for vectors $\mathbf{y}_{\sigma(1)}, \ldots, \mathbf{y}_{\sigma(t-1)}, \mathbf{y}_{\sigma(t+1)}, \ldots, \mathbf{y}_{\sigma(r)}$, then $b_r = 1$ and $\ddot{\mathbf{b}} = 0$, which contradicts (36). Clearly, $(A, \dot{B}')$ is not of type (i). Hence, $(A, \dot{B}')$ is of type (iii). By the induction hypothesis, $d(A, \dot{B}') = r - 1$. Consequently, $d(A, B) \leqslant d(A, \dot{B}') + d(\dot{B}', B) = r$. Therefore, (2) implies that $d(A, B) = r$.

If $b_1 = 0 = b_2$ and there exists $k \in \{3, \ldots, r-1\}$ such that $b_k = 0$, then consider the matrix $\ddot{B}' = A + \sum_{i\neq\sigma(k)} \mathbf{y}_i^2$. Since

$$[\mathbf{y}_{\sigma(i)}^\top A^{-1}\mathbf{y}_{\sigma(j)}]_{i,j\in\{1,\ldots,r\}\setminus\{k\}} = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & b_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & b_{k-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & b_{k+1} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & b_{r-1} \\ 0 & 0 & b_3 & \cdots & b_{k-1} & b_{k+1} & \cdots & b_{r-1} & b_r \end{pmatrix}$$

and $b_r = \sum_{i=3,i\neq k}^{r-1} b_i$, Lemma 2.4 implies that

$$\det \ddot{B}' = \det\left(I_{r-1} + [\mathbf{y}_{\sigma(i)}^\top A^{-1}\mathbf{y}_{\sigma(j)}]_{i,j\in\{1,\ldots,r\}\setminus\{k\}}\right) = 1,$$

i.e. $\ddot{B}' \in SGL_n(\mathbb{F}_2)$. Clearly, the pair $(A, \ddot{B}')$ is not of type (i) with respect to vectors $\mathbf{y}_{\sigma(1)}, \ldots, \mathbf{y}_{\sigma(k-1)}, \mathbf{y}_{\sigma(k+1)}, \ldots, \mathbf{y}_{\sigma(r)}$. It is not of type (ii) either because $(b_1, \ldots, b_r)$ is not the zero vector. Therefore, it is of type (iii). As above, we now deduce $d(A, \ddot{B}') = r-1$ and $d(A, B) = r$ by applying the induction step.

Finally, to end Subcase 1, let $b_1 = 0 = b_2$ and $1 = b_3 = \cdots = b_{r-1}$. By (36),

$$b_r = \begin{cases} 1 & \text{if } r \text{ is even}, \\ 0 & \text{if } r \text{ is odd}. \end{cases}$$

Define vectors $\mathbf{z}_1, \ldots, \mathbf{z}_r$ by

$$\mathbf{z}_i := \begin{cases} \mathbf{y}_{\sigma(i)} & \text{if } \ i \notin \{1,2,3,r\}, \\ \mathbf{y}_{\sigma(i)} + \mathbf{y}_{\sigma(1)} + \mathbf{y}_{\sigma(2)} + \mathbf{y}_{\sigma(3)} + \mathbf{y}_{\sigma(r)} & \text{if } \ i \in \{1,2,3,r\}. \end{cases}$$

Then $\sum_{i=1}^r \mathbf{z}_i^2 = \sum_{i=1}^r \mathbf{y}_i^2$, and a straightforward computation shows that

$$[\mathbf{z}_i^\top A^{-1}\mathbf{z}_j]_{i,j\in\{2,\ldots,r\}} = \begin{pmatrix} (1+b_r)J_{2\times 2} & J_{2\times(r-3)} \\ J_{(r-3)\times 2} & O_{(r-3)\times(r-3)} \end{pmatrix} + \mathbf{e}_2^2. \tag{37}$$

Let $\dddot{B}' = A + \sum_{i=2}^r \mathbf{z}_i^2$. By Lemma 2.4, $\dddot{B}'$ has the same determinant as matrix $I_{r-1} + [\mathbf{z}_i^\top A^{-1}\mathbf{z}_j]_{i,j\in\{2,\ldots,r\}}$, which equals the invertible matrix (4) from Lemma 4.1 where $a = b_r$ and $m = r-3$. Therefore, $\dddot{B}' \in SGL_n(\mathbb{F}_2)$. Since $r \geqslant 4$, it is clear from (37) that the pair $(A, \dddot{B}')$ is of type (iii) with respect to vectors $\mathbf{z}_2, \ldots, \mathbf{z}_r$. Hence, we deduce that $d(A, B) = r$ as above.

Subcase 2. Suppose that (A, B') satisfy the condition (iii). Then by induction hypothesis, $d(A, B') = r-1$ and consequently, $d(A, B) \leqslant d(A, B') + d(B', B) = r$. As above, (2) implies that $d(A, B) = r$.

Subcase 3. Suppose that (A, B') satisfy the condition (i). Then $\mathbf{y}_i^\top A^{-1}\mathbf{y}_i = 1$ for all $i \in \{1, \dots, r-1\}$. Since $B'', B' \in SGL_n(\mathbb{F}_2)$ and one of the numbers $r-2, r-1$ is odd, we get a contradiction by Corollary 2.6.

Case 3. Let (i) be satisfied. By Corollary 2.6, r is even. Suppose firstly that $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 1$ for all i, j. By Lemma 4.10, there exists $\mathbf{x}_{r+1} \in \mathbb{F}_2^n$ such that (15) and (16) is true. We may assume that $s = 1$ in (15)-(16) (otherwise we permute vectors $\mathbf{x}_1, \dots, \mathbf{x}_r$). Let $B_1 = A + \sum_{j=1}^{r+1} \mathbf{x}_j^2$. By Lemmas 2.4 and 2.3,

$$\begin{aligned} \det B_1 &= \det\left(I_{r+1} + [\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j\in\{1,\dots,r+1\}}\right) \\ &= \det\begin{pmatrix} J_{r\times r} + I_r & \mathbf{e}_1 \\ \mathbf{e}_1^\top & 1 \end{pmatrix} \\ &= \det(J_{r\times r} + I_r + \mathbf{e}_1^2). \end{aligned} \tag{38}$$

Clearly, the columns space of matrix $J_{r\times r} + I_r + \mathbf{e}_1^2$ equals the whole space $\mathbb{F}_2^r$. Hence, $B_1 \in SGL_n(\mathbb{F}_2)$. Let $B_2 = A + \sum_{j=1, j\neq 2}^{r+1} \mathbf{x}_j^2$. As in (38), we deduce that $\det B_2 = \det(J_{(r-1)\times(r-1)} + I_{r-1} + \mathbf{e}_1^2)$ and $B_2 \in SGL_n(\mathbb{F}_2)$. Moreover, the pair (A, B_2) is of the type (iii) with respect to the vectors $\mathbf{x}_1, \mathbf{x}_3, \dots, \mathbf{x}_{r+1}$, which are linearly independent by Remark 4.11. By Case 2, $d(A, B_2) = r$. Consequently,

$$d(A, B) \leqslant d(A, B_2) + d(B_2, B_1) + d(B_1, B) = r + 2.$$

By Lemma 4.4, $d(A, B) = r + 2$.

Suppose now that there exist i, j such that $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 0$. By Lemma 4.3, $d(A, B) \geqslant r + 1$. Define vectors $\mathbf{y}_1, \dots, \mathbf{y}_{r+1}$ by

$$\begin{aligned} \mathbf{y}_i &= \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 + \mathbf{x}_i \qquad (i = 1, 2, 3), \\ \mathbf{y}_4 &= \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3, \\ \mathbf{y}_i &= \mathbf{x}_{i-1} \qquad (i = 5, \dots, r+1). \end{aligned}$$

Then, $\sum_{i=1}^{r+1} \mathbf{y}_i^2 = \sum_{i=1}^{r} \mathbf{x}_i^2$. Let the matrix $D = [d_{ij}]_{i,j=1}^{r+1}$ be defined by

$$D = I_{r+1} + [\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=1}^{r+1},$$

and let D_{ij} denote the determinant of the $r \times r$ submatrix of D, which is obtained by deleting the i-th row and the j-th column. By Lemma 2.4,

$$1 = \det B = \det D.$$

The Laplace expansion along the i-th row yields $1 = \sum_{j=1}^{r+1} d_{ij} D_{ij}$ for all i. Since

$$d_{ii} = \begin{cases} 1 & \text{if } i \in \{1,2,3\}, \\ 0 & \text{if } i \in \{4,\ldots,r+1\}, \end{cases}$$

r is even, $d_{ij} = d_{ji}$, and $D_{ij} = D_{ji}$, in characteristic two we deduce that $1 = \sum_{i=1}^{r+1}\sum_{j=1}^{r+1} d_{ij}D_{ij} = D_{11} + D_{22} + D_{33}$. Consequently, there exists $i \in \{1,2,3\}$ such that $D_{ii} = 1$. We may assume that $D_{11} = 1$. Let $B' = A + \sum_{i=2}^{r+1} \mathbf{y}_i^2$. Since

$$\det B' = \det(I_r + [\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=2}^{r+1}) = D_{11} = 1,$$

we have $B' \in SGL_n(\mathbb{F}_2)$. The diagonal of $[\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=2}^{r+1}$ is $(0,0,1,\ldots,1)$. If

$$[\mathbf{y}_i^\top A^{-1}\mathbf{y}_j]_{i,j=2}^{r+1} \neq \begin{pmatrix} O_{2\times 2} & O_{2\times(r-2)} \\ O_{(r-2)\times 2} & J_{(r-2)\times(r-2)} \end{pmatrix}, \tag{39}$$

then (A, B') is of type (iii) with respect to the vectors $\mathbf{y}_2, \ldots, \mathbf{y}_{r+1}$, which are linearly independent. Consequently, $d(A, B') = r$ by Case 2 and therefore $d(A, B) \leqslant d(A, B') + d(B', B) = r + 1$. Hence, $d(A, B) = r + 1$ as claimed.

Finally, assume that the two matrices in (39) are the same. Then, for each $i \geqslant 5$ we have $0 = \mathbf{y}_2^\top A^{-1}\mathbf{y}_i = \mathbf{x}_1^\top A^{-1}\mathbf{x}_{i-1} + \mathbf{x}_3^\top A^{-1}\mathbf{x}_{i-1}$, i.e. $\mathbf{x}_1^\top A^{-1}\mathbf{x}_{i-1} = \mathbf{x}_3^\top A^{-1}\mathbf{x}_{i-1}$. If we replace $\mathbf{y}_2$ by $\mathbf{y}_3$ in this computation we further deduce that

$$\mathbf{x}_1^\top A^{-1}\mathbf{x}_{i-1} = \mathbf{x}_2^\top A^{-1}\mathbf{x}_{i-1} = \mathbf{x}_3^\top A^{-1}\mathbf{x}_{i-1} =: a_{i-1} \qquad (5 \leqslant i \leqslant r+1).$$

Consequently, for $i, j \geqslant 5$ we have

$$\begin{aligned} 0 = 1 + 1 &= \mathbf{y}_4^\top A^{-1}\mathbf{y}_i + \mathbf{y}_4^\top A^{-1}\mathbf{y}_j \\ &= (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^\top A^{-1}\mathbf{x}_{i-1} + (\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3)^\top A^{-1}\mathbf{x}_{j-1} \\ &= a_{i-1} + a_{j-1}. \end{aligned}$$

Hence, $a_4 = \cdots = a_r$. Moreover, for $i, j \geqslant 5$ we have also

$$1 = \mathbf{y}_i^\top A^{-1}\mathbf{y}_j = \mathbf{x}_{i-1}^\top A^{-1}\mathbf{x}_{j-1}.$$

Since $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1$ for all i, the expansion of the equalities $\mathbf{y}_2^\top A^{-1}\mathbf{y}_4 = 0 = \mathbf{y}_3^\top A^{-1}\mathbf{y}_4$ implies that

$$\mathbf{x}_1^\top A^{-1}\mathbf{x}_2 = \mathbf{x}_1^\top A^{-1}\mathbf{x}_3 = \mathbf{x}_2^\top A^{-1}\mathbf{x}_3. \tag{40}$$

Consequently,

$$0 = \mathbf{y}_2^\top A^{-1}\mathbf{y}_3 = \mathbf{x}_1^\top A^{-1}\mathbf{x}_1 + \mathbf{x}_1^\top A^{-1}\mathbf{x}_2 + \mathbf{x}_3^\top A^{-1}\mathbf{x}_1 + \mathbf{x}_3^\top A^{-1}\mathbf{x}_2 = 1 + \mathbf{x}_1^\top A^{-1}\mathbf{x}_2,$$

which means that all values in (40) equal 1. Hence,

$$[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r = \begin{pmatrix} J_{3\times 3} & a_4 J_{3\times(r-3)} \\ a_4 J_{(r-3)\times 3} & J_{(r-3)\times(r-3)} \end{pmatrix}.$$

Since $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 0$ for some i, j, it follows that $a_4 = 0$. Consequently, Lemma 2.4 implies that

$$1 = \det B = \det \begin{pmatrix} J_{3\times 3} + I_3 & O \\ O & J_{(r-3)\times(r-3)} + I_{r-3} \end{pmatrix},$$

a contradiction because matrix $J_{3\times 3} + I_3$ is not invertible. □

6. Proof of Theorem 3.3

We prove the parts (i) and (ii) separately. In both we rely on Theorem 3.1.

Proof of Theorem 3.3 (i). Since $A - B$ is an alternate matrix of rank r and (2) holds, it suffices to prove that $d(A, B) \leqslant r + 1$. Define

$$S_0 = \left\{i \in \{1, \dots, r+1\} : \mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 0\right\}, \tag{41}$$

$$S_1 = \left\{i \in \{1, \dots, r+1\} : \mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1\right\}. \tag{42}$$

Since $\mathbf{x}_{r+1}^\top A^{-1}\mathbf{x}_{r+1} = \sum_{i=1}^r \mathbf{x}_i^\top A^{-1}\mathbf{x}_i$ and r is even, it follows that $|S_0| \geqslant 1$. We separate three cases.

Case 1. Let $|S_0| = 1$ and $r = 2$. Since $\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 = 0$ and each pair of vectors among $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ are linearly independent, we may assume that $S_0 = \{1\}$ and $S_1 = \{2, 3\}$. Let $a = \mathbf{x}_1^\top A^{-1}\mathbf{x}_2$. Then,

$$\mathbf{x}_1^\top A^{-1}\mathbf{x}_3 = a, \quad \mathbf{x}_2^\top A^{-1}\mathbf{x}_3 = 1 + a.$$

If X is the $n \times 3$ matrix with $\mathbf{x}_i$ as its i-th column, then Lemma 2.4 implies that

$$1 = \det B = \det(A + XX^\top) = \det(I_3 + X^\top A^{-1}X) = \det \begin{pmatrix} 1 & a & a \\ a & 0 & 1+a \\ a & 1+a & 0 \end{pmatrix}. \tag{43}$$

Consequently, $a = 0$. Hence, $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1}$ is of rank-one, a contradiction.

Case 2. Let $|S_0| > 1$ and $r = 2$. Since $\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 = 0$, we deduce that $|S_0| = 3$, i.e. $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 0$ for $i = 1, 2, 3$. Let $a = \mathbf{x}_1^\top A^{-1}\mathbf{x}_2$. Then,

$$\mathbf{x}_1^\top A^{-1}\mathbf{x}_3 = a = \mathbf{x}_2^\top A^{-1}\mathbf{x}_3.$$

As in (43) we deduce that

$$1 = \det B = \det \begin{pmatrix} 1 & a & a \\ a & 1 & a \\ a & a & 1 \end{pmatrix},$$

i.e. $a = 0$. Define $B' = A + \mathbf{x}_1^2 + \mathbf{x}_2^2$. Then

$$\det B' = \det \left(I_2 + \begin{pmatrix} \mathbf{x}_1^\top A^{-1}\mathbf{x}_1 & \mathbf{x}_1^\top A^{-1}\mathbf{x}_2 \\ \mathbf{x}_1^\top A^{-1}\mathbf{x}_2 & \mathbf{x}_3^\top A^{-1}\mathbf{x}_3 \end{pmatrix} \right) = 1.$$

By Theorem 3.1, $d(A, B') = 2$. Hence, $d(A, B) \leqslant d(A, B') + d(B', B) = 3 = r + 1$.

Case 3. Let $r \geqslant 4$. If $|S_0| = 1$, i.e. $S_0 = \{i_0\}$ for some $i_0 \in \{1, \dots, r+1\}$, then there exist $j_1, k_1, l_1 \in S_1$ and we can define $\mathbf{y}_1, \dots, \mathbf{y}_{r+1}$ by

$$\begin{aligned} \mathbf{y}_{i_0} &= \mathbf{x}_{j_1} + \mathbf{x}_{k_1} + \mathbf{x}_{l_1}, \\ \mathbf{y}_{j_1} &= \mathbf{x}_{i_0} + \mathbf{x}_{k_1} + \mathbf{x}_{l_1}, \\ \mathbf{y}_{k_1} &= \mathbf{x}_{i_0} + \mathbf{x}_{j_1} + \mathbf{x}_{l_1}, \\ \mathbf{y}_{l_1} &= \mathbf{x}_{i_0} + \mathbf{x}_{j_1} + \mathbf{x}_{k_1}, \end{aligned}$$

and $\mathbf{y}_i = \mathbf{x}_i$ for all $i \in \{1, \dots, r+1\} \backslash \{i_0, j_1, k_1, l_1\}$. Then $\sum_{i=1}^{r+1} \mathbf{x}_i^2 = \sum_{i=1}^{r+1} \mathbf{y}_i^2$, $\mathbf{y}_{r+1} = \sum_{i=1}^{r} \mathbf{y}_i$, vectors $\mathbf{y}_1, \dots, \mathbf{y}_r$ are linearly independent, and

$$\left| \left\{ i \in \{1, \dots, r+1\} : \mathbf{y}_i^\top A^{-1} \mathbf{y}_i = 0 \right\} \right| = |\{j_1, k_1, l_1\}| = 3.$$

Moreover, if X and Y are the $n \times (r+1)$ matrices with $\mathbf{x}_i$ and $\mathbf{y}_i$ as its i-th column, respectively, then $Y = XR$ for appropriate $R \in GL_{r+1}(\mathbb{F}_2)$, and matrices $[\mathbf{y}_i A^{-1} \mathbf{y}_j]_{i,j=1}^{r+1} = Y^\top A^{-1} Y$, $[\mathbf{x}_i A^{-1} \mathbf{x}_j]_{i,j=1}^{r+1} = X^\top A^{-1} X$ have equal rank. By replacing $\mathbf{x}_1, \dots, \mathbf{x}_{r+1}$ with $\mathbf{y}_1, \dots, \mathbf{y}_{r+1}$, we may assume that $|S_0| \geqslant 2$.

To proceed, observe that as in (43) we can deduce that $\det D = 1$ where $D = [d_{ij}]_{i,j=1}^{r+1} := I_{r+1} + X^\top A^{-1} X$. Let D_{ij} be the determinant of the submatrix obtained by removing the i-th row and the j-th column of D. Then, for each $i \in \{1, \dots, r+1\}$, the Laplace expansion along the i-th row yields $1 = \sum_{j=1}^{r+1} d_{ij} D_{ij}$. Since D is symmetric, we have $d_{ij} = d_{ji}$ and $D_{ij} = D_{ji}$. Since r is even,

$$1 = \sum_{i=1}^{r+1} \sum_{j=1}^{r+1} d_{ij} D_{ij} = \sum_{i=1}^{r+1} d_{ii} D_{ii}.$$

Therefore, there exists $i \in \{1, \dots, r+1\}$ such that $d_{ii} = 1 = D_{ii}$. We may assume that $i = r+1$ (otherwise we permute vectors $\mathbf{x}_1, \dots, \mathbf{x}_{r+1}$ in appropriate order). Define $B' := A + \mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2$. Then,

$$\det B' = \det\left(I_r + [\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r\right) = \det D_{r+1,r+1} = 1.$$

Since $|S_0| \geqslant 2$, the matrix $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r$ must have at least one zero on the diagonal. By Remark 3.4, $\operatorname{rank}([\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r) = \operatorname{rank}([\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1}) \neq 1$. By Theorem 3.1, $d(A, B') = r$. Hence, $d(A, B) \leqslant d(A, B') + d(B', B) = r + 1$. $\square$

Proof of Theorem 3.3 (ii). Let S_0, S_1 be as in (41), (42). By Remark 3.4, $0 = \operatorname{Tr}([\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1}) = \sum_{i=1}^{r+1} \mathbf{x}_i^\top A^{-1}\mathbf{x}_i$, so $|S_1| = 2t$ for some $t \leqslant \frac{r}{2}$. Since the matrix $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1}$ is of rank one, it is not alternate. Hence, its diagonal is not zero everywhere, and therefore $t \geqslant 1$. We may assume that

$$S_1 = \{1, 2, \dots, 2t\} \quad \text{and} \quad S_0 = \{2t+1, 2t+2, \dots, r+1\}; \tag{44}$$

(otherwise we permute the vectors $\mathbf{x}_1, \dots, \mathbf{x}_{r+1}$). Since $B - A$ is an alternate matrix of rank r, (2) implies that

$$d(A, B) \geqslant r + 1.$$

Moreover, Lemma 2.4, Lemma 2.2, and (44) imply that

$$\begin{aligned} B^{-1} &= A^{-1} - A^{-1}X(I_{r+1} + X^\top A^{-1}X)X^\top A^{-1} \\ &= A^{-1} - A^{-1}X \begin{pmatrix} I_{2t} + J_{(2t)\times(2t)} & O \\ O & I_{r+1-2t} \end{pmatrix} X^\top A^{-1}, \end{aligned} \tag{45}$$

where X is the $n \times (r+1)$ matrix with $\mathbf{x}_i$ as its i-th column. We divide the rest of the proof into three steps.

Step 1. We claim that $d(A, B) \geqslant r + 2$.

Suppose that $d(A, B) = r + 1$. Then, $\operatorname{rank}(B' - B) = 1$ and $d(A, B') = r$ for some $B' \in SGL_n(\mathbb{F}_2)$. In particular, $B' = B + \mathbf{y}^2$ for some nonzero $\mathbf{y} \in \mathbb{F}_2^n$.

If $\mathbf{y} \notin \langle \mathbf{x}_1, \dots, \mathbf{x}_r \rangle$, then

$$B' - A = B - A + \mathbf{y}^2 = P \begin{pmatrix} J_{r\times r} + I_r & O_{r\times 1} & O \\ O_{1\times r} & 1 & O \\ O & O & O \end{pmatrix} P^\top,$$

for any $P \in GL_n(\mathbb{F}_2)$ with $\mathbf{x}_1, \dots, \mathbf{x}_r, \mathbf{y}$ as the first $r+1$ columns. In particular, $\operatorname{rank}(B' - A) = r + 1$. Hence, (2) implies that $d(A, B') \geqslant r + 1$, a contradiction.

Therefore, $\mathbf{y} \in \langle \mathbf{x}_1, \dots, \mathbf{x}_r \rangle$, i.e. $\mathbf{y} = \sum_{j=1}^s \mathbf{x}_{i_j}$ for some subset $\{i_1, \dots, i_s\} \subseteq \{1, \dots, r\}$ of distinct indices. If $s = r$, then $B' = A + \mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2$. From Remark 3.4 and (44) we deduce that $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r \in \mathcal{R}_1^{\mathrm{Tr}_0}$. Consequently, $d(A, B') = r + 2$ by Theorem 3.1, a contradiction. Therefore $1 \leqslant s < r$. If $S_1' := \{j \in \{1, \dots, s\} : i_j \leqslant 2t\}$ and $j \leqslant s$, then (45) implies

$$\begin{aligned}
\mathbf{x}_{i_j}^\top B^{-1}\mathbf{x}_{i_j} &= \mathbf{x}_{i_j}^\top A^{-1}\mathbf{x}_{i_j} - \mathbf{x}_{i_j}^\top A^{-1}X\begin{pmatrix} I_{2t}+J_{(2t)\times(2t)} & O\\ O & I_{r+1-2t}\end{pmatrix}X^\top A^{-1}\mathbf{x}_{i_j}\\
&= \begin{cases} 1-(\underbrace{1\cdots 1}_{2t}\,0\cdots 0)\begin{pmatrix} I_{2t}+J_{(2t)\times(2t)} & O\\ O & I_{r+1-2t}\end{pmatrix}\begin{pmatrix}1\\ \vdots\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix} & \text{if} \quad j\in S_1',\\[2ex] 0-(0\cdots 0)\begin{pmatrix} I_{2t}+J_{(2t)\times(2t)} & O\\ O & I_{r+1-2t}\end{pmatrix}\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix} & \text{if} \quad j\notin S_1',\end{cases}\\
&= \begin{cases} 1 & \text{if} \quad j\in S_1',\\ 0 & \text{if} \quad j\notin S_1'.\end{cases}
\end{aligned}$$

By Lemma 2.4,

$$1=\det B' = \det(B+\mathbf{y}^2) = 1+\mathbf{y}^\top B^{-1}\mathbf{y} = 1+\sum_{j=1}^{s}\mathbf{x}_{i_j}^\top B^{-1}\mathbf{x}_{i_j} = 1+|S_1'| \pmod 2,$$

which means that $|S_1'|$ is even. We denote $\{i_{s+1},\ldots,i_r\}=\{1,\ldots,r\}\backslash\{i_1,\ldots,i_s\}$ and separate two cases to end the proof of Step 1.

Case 1. Let s be odd. Then we define $\mathbf{w}_1,\ldots,\mathbf{w}_r$ as in Lemma 4.5, which together with Remark 3.4 imply that

$$\begin{aligned}
&B' = A+\mathbf{w}_1^2+\cdots+\mathbf{w}_r^2, \qquad \operatorname{rank}\left([\mathbf{w}_i^\top A^{-1}\mathbf{w}_j]_{i,j=1}^r\right)=1,\\
&\operatorname{Tr}[\mathbf{w}_i^\top A^{-1}\mathbf{w}_j]_{i,j\in\{1,\ldots,r\}} = \sum_{j=1}^{s}\mathbf{x}_{i_j}^\top A^{-1}\mathbf{x}_{i_j} = |S_1'| \pmod 2 = 0.
\end{aligned}$$

By Theorem 3.1, $d(A,B')=r+2$, a contradiction. Hence, $d(A,B)\geqslant r+2$.

Case 2. Let s be even. Then we repeat the proof in Case 1 where we replace Lemma 4.5 by Lemma 4.6.

Step 2. We claim the matrix $B^{-1}-A^{-1}$ is not alternate.

If $B^{-1}-A^{-1}$ is alternate, then it follows from (45) that

$$X\begin{pmatrix} I_{2t}+J_{(2t)\times(2t)} & O\\ O & I_{r+1-2t}\end{pmatrix}X^\top = \sum_{1\leqslant i<j\leqslant 2t}\mathbf{x}_i\circ\mathbf{x}_j+\mathbf{x}_{2t+1}^2+\cdots+\mathbf{x}_{r+1}^2$$

is alternate. Therefore, $\mathbf{x}_{2t+1}^2 + \cdots + \mathbf{x}_{r+1}^2$ is alternate as well. If we select a matrix $P \in GL_n(\mathbb{F}_2)$ such that $P\mathbf{x}_i = \mathbf{e}_i$ for $i = 1, \ldots, r$, then the equality $\mathbf{x}_{r+1} = \sum_{i=1}^r \mathbf{x}_i$ implies that matrix

$$P(\mathbf{x}_{2t+1}^2 + \cdots + \mathbf{x}_{r+1}^2)P^\top = \begin{pmatrix} O_{(2t)\times(2t)} & O_{(2t)\times(r-2t)} & O \\ O_{(r-2t)\times(2t)} & I_{r-2t} & O \\ O & O & O \end{pmatrix} + \begin{pmatrix} J_{r\times r} & O \\ O & O \end{pmatrix}$$

is alternate, which is not true.

Step 3. We claim that $d(A, B) = r + 2$.

Since $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1} = X^\top A^{-1} X$ is of rank one, it follows from (44) that

$$[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1} = \begin{pmatrix} J_{(2t)\times(2t)} & O \\ O & O \end{pmatrix}.$$

In particular,

$$\mathbf{x}_i^\top A^{-1} X = \begin{cases} (0, \ldots, 0, 0, \ldots, 0) & \text{if} \quad i > 2t, \\ (\underbrace{1, \ldots, 1}_{2t}, 0, \ldots, 0) & \text{if} \quad i \leqslant 2t. \end{cases}$$

Consequently, (45) implies that

$$\mathbf{x}_i^\top (B^{-1} - A^{-1})\mathbf{x}_j = 0 \qquad (i, j \in \{1, \ldots, r+1\}). \tag{46}$$

By Step 2, there exists nonzero $\mathbf{z} \in \mathbb{F}_2^n$ such that

$$\mathbf{z}^\top (B^{-1} - A^{-1})\mathbf{z} = 1. \tag{47}$$

From (46) we deduce that $\mathbf{z} \notin \langle \mathbf{x}_1, \ldots, \mathbf{x}_r \rangle$. Define column vector

$$\mathbf{v} = \begin{cases} \mathbf{z} & \text{if} \quad \mathbf{z}^\top B^{-1}\mathbf{z} = 0, \\ \mathbf{z} + \mathbf{x}_1 & \text{if} \quad \mathbf{z}^\top B^{-1}\mathbf{z} = 1. \end{cases}$$

Then, (44), (46), (47) imply that $\mathbf{v}^\top B^{-1}\mathbf{v} = 0$ and $\mathbf{v}^\top A^{-1}\mathbf{v} = 1$. In particular, $B' = B + \mathbf{v}^2$ is an invertible matrix. From Lemma 4.7 we deduce that $B' = A + \sum_{i=1}^{r+1} \mathbf{v}_i^2$ where $\mathbf{v}_i = \mathbf{x}_i + \mathbf{v}$ for all $i \in \{1, \ldots, r+1\}$. Since vectors $\mathbf{v}_1, \ldots, \mathbf{v}_{r+1}$ span the vector space $\langle \mathbf{x}_1, \ldots, \mathbf{x}_r, \mathbf{z} \rangle$, they are linearly independent. Moreover,

$$\mathrm{Tr}[\mathbf{v}_i^\top A^{-1}\mathbf{v}_j]_{i,j\in\{1,\ldots,r+1\}} = \sum_{i=1}^{r+1} \mathbf{v}_i^\top A^{-1}\mathbf{v}_i$$

$$= \sum_{i=1}^{r+1} \mathbf{x}_i^\top A^{-1}\mathbf{x}_i + (r+1)\mathbf{v}^\top A^{-1}\mathbf{v}$$
$$= \mathrm{Tr}[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j\in\{1,\ldots,r+1\}} + (r+1)\mathbf{v}^\top A^{-1}\mathbf{v}$$
$$= 0 + 1 = 1.$$

Since $r+1$ is odd, it follows from Corollary 2.6 that $\mathbf{v}_i^\top A^{-1}\mathbf{v}_i = 0$ for some i. Consequently, Theorem 3.1 implies that $d(A, B') = r+1$ and therefore $d(A,B) \leqslant d(A,B') + d(B',B) = r+2$. From Step 1 we infer that $d(A,B) = r+2$. $\square$

7. Diameter of Γ_n

To determine the diameter of graph Γ_n we need two more lemmas.

Lemma 7.1. *Let $n \geqslant 2$.*

(i) *A pair (A,B) of matrices in $SGL_n(\mathbb{F}_2)$ that satisfy the condition (i) from Theorem 3.1 where $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 1$ for all i,j exists if and only if $r \in \{1,\ldots,\lfloor\frac{n+1}{2}\rfloor\}$ is even.*

(ii) *A pair (A,B) of matrices in $SGL_n(\mathbb{F}_2)$ that satisfy the condition (i) from Theorem 3.1 where $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 0$ for some i,j exists if and only if $r \in \{1,\ldots,n\}\backslash\{2\}$ is even.*

(iii) *A pair (A,B) of matrices in $SGL_n(\mathbb{F}_2)$ that satisfy the condition (ii) from Theorem 3.1 exists if and only if $r \in \{2,3,\ldots,\lfloor\frac{n+1}{2}\rfloor\}$.*

(iv) *A pair (A,B) of matrices in $SGL_n(\mathbb{F}_2)$ that satisfy the condition (iii) from Theorem 3.1 exists for each $r \in \{1,\ldots,n\}$.*

Proof. (i) If $\mathbf{x}_i^\top A^{-1}\mathbf{x}_j = 1$ for all i,j, then r is even by Corollary 2.6. Moreover, A^{-1} is nonalternate. Hence, $A^{-1} = PP^\top$ for some $P \in GL_n(\mathbb{F}_2)$ and vectors $\mathbf{y}_i := P^\top\mathbf{x}_i$ satisfy $\mathbf{y}_i^\top\mathbf{y}_j = 1$ for all i,j. In particular, $\operatorname{rank}\big([\mathbf{y}_i^\top\mathbf{y}_j]_{i,j=1}^r\big) = 1$. By Lemma 2.7, $r \leqslant \lfloor\frac{n+1}{2}\rfloor$.

Conversely, if $r \leqslant \lfloor\frac{n+1}{2}\rfloor$, then vectors $\mathbf{x}_i = \sum_{k=1}^{2i-1}\mathbf{e}_k$ for $i = 1,\ldots,r$ satisfy $\mathbf{x}_i^\top\mathbf{x}_j = 1$ for all i,j. By Lemma 2.4, the matrix $B := I_n + \sum_{i=1}^r \mathbf{x}_i^2$ satisfies $\det B = \det(I_r + J_r) = \det(I_r + \mathbf{j}_r^2) = 1 + \mathbf{j}_r^\top\mathbf{j}_r = 1$ whenever r is even. Hence, (A,B) where $A = I_n$ is a required pair.

(ii) If (A,B) is any such pair, then, as above, r is even by Corollary 2.6. In the case $r = 2$ we would necessarily have $\mathbf{x}_1^\top A^{-1}\mathbf{x}_2 = 0$. Consequently, Lemma 2.4 would imply that $1 = \det B = \det(I_2 + I_2) = 0$, a contradiction.

Suppose now that $r \in \{1,\ldots,n\}\backslash\{2\}$ is even. If $r = 4k$ for some $k \geqslant 1$, then we set $A = I_n$ and $B = I_n + \sum_{i=1}^r \mathbf{x}_i^2$ where

$$\mathbf{x}_i = \begin{cases} \mathbf{e}_i & \text{if } i \in \{1,\ldots,2k\}, \\ \mathbf{e}_{i-2k} + \mathbf{e}_{i-2k+1} + \cdots + \mathbf{e}_i & \text{if } i \in \{2k+1,\ldots,4k\}. \end{cases} \tag{48}$$

Clearly, $\mathbf{x}_1, \dots, \mathbf{x}_r$ are linearly independent and $A \in SGL_n(\mathbb{F}_2)$. By Lemma 2.4, B and $I_r + [\mathbf{x}_i^\top \mathbf{x}_j]_{i,j=1}^r$ have the same determinant. Observe that

$$I_r + [\mathbf{x}_i^\top \mathbf{x}_j]_{i,j=1}^r = \begin{pmatrix} O & L \\ L^\top & A_{22} \end{pmatrix}$$

where $A_{22} \in S_{2k}(\mathbb{F}_2)$ and $L = [l_{ij}]_{i,j=1}^{2k}$ is the lower triangular matrix with $l_{ij} = 1$ if and only if $i \geqslant j$. Consequently, L is invertible and therefore $B \in SGL_n(\mathbb{F}_2)$. If $r = 4k - 2$ for some $k \geqslant 2$, then we replace vectors (48) by

$$\mathbf{x}_i = \begin{cases} \mathbf{e}_i & \text{if } i \in \{1, \dots, 2k-1\}, \\ \mathbf{e}_1 + \mathbf{e}_2 + \cdots + \mathbf{e}_{2k+1} & \text{if } i = 2k, \\ \mathbf{e}_{i+1-2k} + \mathbf{e}_{i+2-2k} + \cdots + \mathbf{e}_{i+1} & \text{if } i \in \{2k+1, \dots, 4k-3\}, \\ \mathbf{e}_1 + \mathbf{e}_{2k-1} + \mathbf{e}_{2k} & \text{if } i = 4k-2. \end{cases}$$

Now, the only difference is that $L = [l_{ij}]_{i,j=1}^{2k-1}$ satisfies $l_{ij} = 1$ if and only if $i \geqslant j$ or $(i,j) = (1, 2k-1)$. Again, $L \in GL_{2k-1}(\mathbb{F}_2)$ and therefore $B \in SGL_n(\mathbb{F}_2)$.

(iii) Let the pair (A, B) satisfy $[\mathbf{x}_i^\top A^{-1} \mathbf{x}_j]_{i,j=1}^r \in \mathcal{R}_1^{\mathrm{Tr}_0}$. By Lemma 2.2, $r \geqslant 2$. Moreover, $\mathbf{x}_i^\top A^{-1} \mathbf{x}_i = 1$ for some i. Hence, A^{-1} is not alternate and there exists $P \in GL_n(\mathbb{F}_2)$ such that $A^{-1} = PP^\top$. Linearly independent vectors $\mathbf{y}_j := P^\top \mathbf{x}_j$ satisfy $[\mathbf{y}_i^\top \mathbf{y}_j]_{i,j=1}^r \in \mathcal{R}_1^{\mathrm{Tr}_0}$. By Lemma 2.7, $r \leqslant \lfloor \frac{n+1}{2} \rfloor$.

Conversely, let $r \in \{2, 3, \dots, \lfloor \frac{n+1}{2} \rfloor\}$, in particular $n \geqslant 3$. Define $A = I_n$ and $B = I_n + \sum_{i=1}^r \mathbf{x}_i^2$ where

$$\mathbf{x}_1 = \mathbf{e}_1, \quad \mathbf{x}_2 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3, \quad \mathbf{x}_i = \mathbf{e}_{2i-2} + \mathbf{e}_{2i-1} \text{ if } i \in \{3, \dots, r\}.$$

Then, $A \in SGL_n(\mathbb{F}_2)$,

$$[\mathbf{x}_i^\top A^{-1} \mathbf{x}_j]_{i,j=1}^r = \begin{pmatrix} J_{2\times 2} & O \\ O & O \end{pmatrix} \in \mathcal{R}_1^{\mathrm{Tr}_0},$$

and $\det B = \det(I_r + [\mathbf{x}_i^\top A^{-1} \mathbf{x}_j]_{i,j=1}^r) = 1$ by Lemma 2.4, i.e. $B \in SGL_n(\mathbb{F}_2)$.

(iv) Let $r \in \{1, \dots, n\}$, $A = I_n$, and $B = I_n + \sum_{i=1}^r \mathbf{x}_i^2$ where

$$\mathbf{x}_i = \begin{cases} \mathbf{e}_i & \text{if } i \text{ is even}, \\ \mathbf{e}_{n-2} + \mathbf{e}_n & \text{if } i = r = n \text{ is odd}, \\ \mathbf{e}_i + \mathbf{e}_{i+1} & \text{otherwise}. \end{cases}$$

It is straightforward to check that $\mathbf{x}_1, \dots, \mathbf{x}_r$ are linearly independent and $A, B \in SGL_n(\mathbb{F}_2)$. If $r = 1$, then $\mathbf{x}_1^\top A^{-1} \mathbf{x}_1 = 0$ implies that the pair (A, B) does not fit the assumptions (i), (ii) from Theorem 3.1. If $r \geqslant 2$, then the same conclusion is obtained by observing in addition that $\mathbf{x}_2^\top A^{-1} \mathbf{x}_2 = 1 = \mathbf{x}_1^\top A^{-1} \mathbf{x}_2$. $\square$

Lemma 7.2. *Let $n \geqslant 2$ and suppose $0 < r \leqslant n$ is even.*

(i) *A pair (A, B) of matrices in $SGL_n(\mathbb{F}_2)$ that satisfy the condition (i) from Theorem 3.3 exists if and only if $(r, n) \notin \{(2, 2), (2, 3)\}$.*

(ii) *A pair (A, B) of matrices in $SGL_n(\mathbb{F}_2)$ that satisfy the condition (ii) from Theorem 3.3 exists if and only if $r \leqslant \lfloor \frac{n+1}{2} \rfloor$.*

Proof. (i) Let $A = I_n$. If $r = 2$ and $n \geqslant 4$, then it is easy to check that, for $\mathbf{x}_1 = \mathbf{e}_1 + \mathbf{e}_2$, $\mathbf{x}_2 = \mathbf{e}_3 + \mathbf{e}_4$, we have $B = A + \mathbf{x}_1^2 + \mathbf{x}_2^2 + (\mathbf{x}_1 + \mathbf{x}_2)^2 \in SGL_n(\mathbb{F}_2)$ and $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1} = O$. If $r = 4k$ or $r = 4k + 2$ for some $k \geqslant 1$, then define

$$B = A + \begin{pmatrix} C & & & & \\ & C & & & \\ & & \ddots & & \\ & & & C & \\ & & & & 0 \end{pmatrix} \quad \text{and} \quad B = A + \begin{pmatrix} C & & & & & \\ & C & & & & \\ & & \ddots & & & \\ & & & C & & \\ & & & & D & \\ & & & & & 0 \end{pmatrix}, \tag{49}$$

respectively where

$$C = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

In (49), C appears k and $k - 1$ times respectively. Clearly, $B \in SGL_n(\mathbb{F}_2)$. Since $C = \mathbf{e}_1 \circ \mathbf{e}_2 + \mathbf{e}_3 \circ (\mathbf{e}_2 + \mathbf{e}_4)$ and $D = \mathbf{e}_1 \circ \mathbf{e}_2 + \mathbf{e}_3 \circ (\mathbf{e}_2 + \mathbf{e}_4) + \mathbf{e}_5 \circ (\mathbf{e}_4 + \mathbf{e}_6)$, we deduce that in both cases $B - A = \mathbf{y}_1 \circ \mathbf{y}_2 + \cdots + \mathbf{y}_{r-1} \circ \mathbf{y}_r$ for some linearly independent vectors $\mathbf{y}_1, \ldots, \mathbf{y}_r \in \mathbb{F}_2^n$ where $\mathbf{y}_1 = \mathbf{e}_1$, $\mathbf{y}_2 = \mathbf{e}_2$, $\mathbf{y}_3 = \mathbf{e}_3$, $\mathbf{y}_4 = \mathbf{e}_2 + \mathbf{e}_4$. By Lemma 2.1, $B - A = \mathbf{x}_1^2 + \cdots + \mathbf{x}_r^2 + (\mathbf{x}_1 + \cdots + \mathbf{x}_r)^2$ where $\mathbf{x}_1 = \mathbf{e}_1$, $\mathbf{x}_2 = \mathbf{e}_2$, $\mathbf{x}_3 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$, $\mathbf{x}_4 = \mathbf{e}_1 + \mathbf{e}_4$. Hence, $\mathbf{x}_1^\top A^{-1}\mathbf{x}_1 = 1 = \mathbf{x}_1^\top A^{-1}\mathbf{x}_4$ and $\mathbf{x}_4^\top A^{-1}\mathbf{x}_4 = 0$, which means that $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1}$ has rank at least two.

Conversely, suppose that $r = 2$, $n \in \{2, 3\}$, $A \in SGL_n(\mathbb{F}_2)$, and $B = A + \mathbf{x}_1^2 + \mathbf{x}_2^2 + (\mathbf{x}_1 + \mathbf{x}_2)^2 \in SGL_n(\mathbb{F}_2)$ where $\mathbf{x}_1, \mathbf{x}_2$ are linearly independent, and $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1}$ is not of rank one. Let $\alpha = \mathbf{x}_1^\top A^{-1}\mathbf{x}_1$, $\beta = \mathbf{x}_2^\top A^{-1}\mathbf{x}_2$, $\gamma = \mathbf{x}_1^\top A^{-1}\mathbf{x}_2$. In characteristic two, Lemma 2.4 implies that

$$1 = \det B = \det(I_3 + [\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1})$$

$$= \det \begin{pmatrix} 1+\alpha & \gamma & \alpha+\gamma \\ \gamma & 1+\beta & \beta+\gamma \\ \alpha+\gamma & \beta+\gamma & 1+\alpha+\beta \end{pmatrix} = 1+\alpha\beta-\gamma^2.$$

Hence, $\alpha\beta = \gamma^2$. By Remark 3.4, $\operatorname{rank}[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^2 \neq 1$, i.e. α, β, γ are all zero. If A^{-1} is not alternate, then $A^{-1} = PP^\top$ for some $P \in GL_n(\mathbb{F}_2)$, and $\langle P^\top \mathbf{x}_1, P^\top \mathbf{x}_2\rangle$ is a self-orthogonal code of length n and dimension 2. Hence, $n \geqslant 4$, a contradiction. If A^{-1} is alternate, then $n = 2$, $A^{-1} = \mathbf{e}_1 \circ \mathbf{e}_2$, and $\{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_1 + \mathbf{x}_2\} = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_1 + \mathbf{e}_2\}$. Consequently $B = O$, a contradiction.

(ii) If $0 < r \leqslant \lfloor \frac{n+1}{2} \rfloor$ is even, then define $A = I_n$, $B = A + \sum_{i=1}^{r+1} \mathbf{x}_i^2$ where

$$\mathbf{x}_1 = \mathbf{e}_1, \quad \mathbf{x}_i = \mathbf{e}_{2i-2} + \mathbf{e}_{2i-1} \ (i = 2, \dots, r), \quad \mathbf{x}_{r+1} = \mathbf{x}_1 + \dots + \mathbf{x}_r.$$

Then, $[\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^{r+1} = (\mathbf{e}_1 + \mathbf{e}_{r+1})^2$ is of rank one and $A, B \in SGL_n(\mathbb{F}_2)$.

Conversely, suppose that a pair (A, B) of matrices in $SGL_n(\mathbb{F}_2)$ satisfies the condition (ii) in Theorem 3.3. By Remark 3.4, $\operatorname{rank}\left([\mathbf{x}_i^\top A^{-1}\mathbf{x}_j]_{i,j=1}^r\right) = 1$. In particular, $\mathbf{x}_i^\top A^{-1}\mathbf{x}_i = 1$ for some i, which means that A^{-1} is not alternate. Hence, there exists $P \in GL_n(\mathbb{F}_2)$ such that $A^{-1} = PP^\top$ and $\operatorname{rank}\left([\mathbf{y}_i^\top \mathbf{y}_j]_{i,j=1}^r\right) = 1$ for linearly independent vectors $\mathbf{y}_j := P^\top \mathbf{x}_j$. By Lemma 2.7, $r \leqslant \lfloor \frac{n+1}{2} \rfloor$. □

Theorems 3.1, 3.3 and Lemmas 7.1, 7.2 imply Corollary 7.3.

Corollary 7.3. *The diameter of graph Γ_n equals*

$$\operatorname{diam}(\Gamma_n) = \begin{cases} 2 & \text{if } n = 2, \\ 4 & \text{if } n = 3, \\ n+1 & \text{if } n \geqslant 4 \text{ is even}, \\ n & \text{if } n \geqslant 5 \text{ is odd}. \end{cases}$$

Corollary 7.3 and the formula for $d_{\widehat{\Gamma}_n}(A, B)$ (cf. (2)) imply that

$$\operatorname{diam}(\widehat{\Gamma}_{2k}) = \operatorname{diam}(\Gamma_{2k}) = \operatorname{diam}(\Gamma_{2k+1}) = \operatorname{diam}(\widehat{\Gamma}_{2k+1}) = 2k+1$$

is an odd number for $k \geqslant 2$.

8. Binary self-dual codes and Γ_n

In this section, we provide an identification of binary self-dual codes in $\mathbb{F}_2^{n+1}$ with certain subsets of matrices in $SGL_n(\mathbb{F}_2)$. The identification relies on the distance function in graph Γ_n. Since the self-dual codes exist in even dimension, we assume that $n \geqslant 3$ is odd in this section. Recall that, given $\mathbf{x} \in \mathbb{F}_2^n$, we defined

$$\overline{\mathbf{x}} = \begin{pmatrix} \mathbf{x} \\ \mathbf{x}^\top \mathbf{x} \end{pmatrix} \in \mathbb{F}_2^{n+1}.$$

For $\mathbf{y} \in \mathbb{F}_2^{n+1}$, let $\underline{\mathbf{y}} \in \mathbb{F}_2^n$ be obtained from $\mathbf{y}$ by deleting the last entry. Then,

$$\overline{\mathbf{x}_1 + \mathbf{x}_2} = \overline{\mathbf{x}}_1 + \overline{\mathbf{x}}_2, \qquad \underline{\mathbf{y}_1 + \mathbf{y}_2} = \underline{\mathbf{y}_1} + \underline{\mathbf{y}_2},$$

$\overline{\mathbf{x}}^\top \overline{\mathbf{x}} = 0$, and $\dim\langle \overline{\mathbf{x}}_1, \dots, \overline{\mathbf{x}}_r \rangle = \dim\langle \mathbf{x}_1, \dots, \mathbf{x}_r \rangle$ for all column vectors. Moreover, $\mathbf{y} = \overline{(\underline{\mathbf{y}})}$ whenever $\mathbf{y}^\top \mathbf{y} = 0$. Hence, if self-dual codes $C = \langle \mathbf{y}_1, \dots, \mathbf{y}_{\frac{n+1}{2}} \rangle$ and $D = \langle \mathbf{z}_1, \dots, \mathbf{z}_{\frac{n+1}{2}} \rangle$ satisfy $\langle \underline{\mathbf{y}_1}, \dots, \underline{\mathbf{y}_{\frac{n+1}{2}}} \rangle = \langle \underline{\mathbf{z}_1}, \dots, \underline{\mathbf{z}_{\frac{n+1}{2}}} \rangle$, then $C = D$.

Let $\mathcal{SD}_n \subseteq SGL_n(\mathbb{F}_2)$ be the subset of all matrices A such that

$$d(A, I_n) = \frac{n+5}{2} \quad \text{and} \quad \operatorname{rank}(A - I_n) = \frac{n+1}{2}.$$

If $A \in \mathcal{SD}_n$, then Theorems 3.1, 3.3, and Remark 3.4 imply that $A - I_n$ is nonalternate and $A - I_n = \sum_{i=1}^{\frac{n+1}{2}} \mathbf{x}_i^2$ or $A - I_n$ is alternate, $\frac{n+1}{2}$ is even, and $A - I_n = \sum_{i=1}^{\frac{n+1}{2}} \mathbf{x}_i^2 + \left(\sum_{i=1}^{\frac{n+1}{2}} \mathbf{x}_i\right)^2$, for some linearly independent $\mathbf{x}_1, \dots, \mathbf{x}_{\frac{n+1}{2}} \in \mathbb{F}_2^n$ such that $[\mathbf{x}_i^\top \mathbf{x}_j]_{i,j=1}^{\frac{n+1}{2}}$ is of rank one. In the nonalternate case, $\operatorname{Tr}\left([\mathbf{x}_i^\top \mathbf{x}_j]_{i,j=1}^{\frac{n+1}{2}}\right) = 0$.

Proposition 8.1. *Each $A \in \mathcal{SD}_n$ determines a unique self-dual code $C = \langle \overline{\mathbf{x}}_1, \dots, \overline{\mathbf{x}}_{\frac{n+1}{2}} \rangle$ in $\mathbb{F}_2^{n+1}$ where $\mathbf{x}_1, \dots, \mathbf{x}_{\frac{n+1}{2}}$ are as in the previous paragraph.*

Proof. By Lemma 2.7, the code C is self-orthogonal. Since

$$\dim\langle \overline{\mathbf{x}}_1, \dots, \overline{\mathbf{x}}_{\frac{n+1}{2}} \rangle = \dim\langle \mathbf{x}_1, \dots, \mathbf{x}_{\frac{n+1}{2}} \rangle = \frac{n+1}{2},$$

C is self-dual. By Lemma 4.12, C is uniquely determined by A. $\square$

Conversely, assume now that C is any self-dual code in $\mathbb{F}_2^{n+1}$. Let $\mathfrak{B}_C$ be the set of all its bases. Then $\mathfrak{B}_C = \mathfrak{B}_C^1 \cup \mathfrak{B}_C^2$ where $\mathfrak{B}_C^1$ consists of bases having an odd number of member-vectors with the last entry 1. Similarly, bases in $\mathfrak{B}_C^2$ have an even number of vectors with the last entry 1. Given a basis $\mathcal{B} = \{\mathbf{y}_1, \dots, \mathbf{y}_{\frac{n+1}{2}}\} \in \mathfrak{B}_C$, consider the matrices

$$A'_{\mathcal{B}} := I_n + \sum_{i=1}^{\frac{n+1}{2}} \underline{\mathbf{y}_i}^2, \tag{50}$$

$$A''_{\mathcal{B}} := I_n + \sum_{i=1}^{\frac{n+1}{2}} \underline{\mathbf{y}_i}^2 + (\underline{\mathbf{y}_1} + \cdots + \underline{\mathbf{y}_{\frac{n+1}{2}}})^2. \tag{51}$$

From the proof of Theorem 8.3 we will be able to observe that

$$A'_{\mathcal{B}} \text{ is invertible} \iff \mathcal{B} \in \mathfrak{B}_C^2 \tag{52}$$

whereas $A''_{\mathcal{B}}$ is always invertible. Nevertheless, $A''_{\mathcal{B}}$ turns out to be 'relevant' for even $\frac{n+1}{2}$ only. To each self-dual code C in $\mathbb{F}_2^{n+1}$ we associate the set

$$\mathcal{F}_C := \begin{cases} \{A'_{\mathcal{B}} : \mathcal{B} \in \mathfrak{B}_C^2\} \cup \{A''_{\mathcal{B}} : \mathcal{B} \in \mathfrak{B}_C\} & \text{if } \frac{n+1}{2} \text{ is even,} \\ \{A'_{\mathcal{B}} : \mathcal{B} \in \mathfrak{B}_C^2\} & \text{if } \frac{n+1}{2} \text{ is odd.} \end{cases}$$

Remark 8.2. For $n \geqslant 7$, there exist distinct bases $\mathcal{B}$ and $\widehat{\mathcal{B}}$ of a self-dual code C such that $A'_{\mathcal{B}} = A'_{\widehat{\mathcal{B}}}$ and $A''_{\mathcal{B}} = A''_{\widehat{\mathcal{B}}}$. For example, we can obtain such $\widehat{\mathcal{B}}$ from $\mathcal{B}$ by replacing vectors $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3, \mathbf{y}_4$ with $\mathbf{y}_1 + \mathbf{y}_2 + \mathbf{y}_3 + \mathbf{y}_4 + \mathbf{y}_i$ ($i = 1, 2, 3, 4$). Moreover, for arbitrary $n \geqslant 3$, $A''_{\mathcal{B}} = A''_{\widehat{\widehat{\mathcal{B}}}}$ whenever $\widehat{\widehat{\mathcal{B}}}$ is obtained from $\mathcal{B}$ by replacing one of the vectors $\mathbf{y}_1, \ldots, \mathbf{y}_{\frac{n+1}{2}}$ in $\mathcal{B}$ with $\mathbf{y}_1 + \cdots + \mathbf{y}_{\frac{n+1}{2}}$.

Theorem 8.3. *$\{\mathcal{F}_C : C$ is a self-dual code in $\mathbb{F}_2^{n+1}\}$ is a partition of $\mathcal{SD}_n$.*

Proof. As explained in Proposition 8.1 and in the paragraph above it, each matrix $A \in \mathcal{SD}_n$ is of the form $A = A'_{\mathcal{B}}$ or $A = A''_{\mathcal{B}}$ where $\mathcal{B} = \{\overline{\mathbf{x}}_1, \ldots, \overline{\mathbf{x}}_{\frac{n+1}{2}}\}$ is a basis of a self-dual code $C = \langle \overline{\mathbf{x}}_1, \ldots, \overline{\mathbf{x}}_{\frac{n+1}{2}} \rangle$. Moreover, in the second case $\frac{n+1}{2}$ is even, while in the first case $0 = \operatorname{Tr}\left([\mathbf{x}_i^\top \mathbf{x}_j]_{i,j=1}^{\frac{n+1}{2}}\right) = \sum_{i=1}^{\frac{n+1}{2}} \mathbf{x}_i^\top \mathbf{x}_i$ meaning that $\mathbf{x}_i^\top \mathbf{x}_i = 1$ for an even number of indices $i \in \{1, \ldots, \frac{n+1}{2}\}$. Therefore, $\mathcal{B} \in \mathfrak{B}_C^2$ in the case $A = A'_{\mathcal{B}}$. Hence, $A \in \mathcal{F}_C$.

The uniqueness part of Proposition 8.1 implies that $\mathcal{F}_C \cap \mathcal{F}_{\widetilde{C}} = \varnothing$ whenever the self-dual codes C and $\widetilde{C}$ are distinct. It remains to prove that $\mathcal{F}_C \subseteq \mathcal{SD}_n$ for each self-dual code C in $\mathbb{F}_2^{n+1}$.

Let $\mathcal{B} = \{\mathbf{y}_1, \ldots, \mathbf{y}_{\frac{n+1}{2}}\} \in \mathfrak{B}_C$ for some self-dual code C. By Lemma 2.4,

$$\det A'_{\mathcal{B}} = \det\left(I_{\frac{n+1}{2}} + [\underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_j}]_{i,j=1}^{\frac{n+1}{2}}\right), \tag{53}$$

$$\det A''_{\mathcal{B}} = \det\left(I_{\frac{n+3}{2}} + [\underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_j}]_{i,j=1}^{\frac{n+3}{2}}\right) \tag{54}$$

where $\underline{\mathbf{y}_{\frac{n+3}{2}}} = \underline{\mathbf{y}_1} + \cdots + \underline{\mathbf{y}_{\frac{n+1}{2}}}$. Since $\mathbf{y}_i^\top \mathbf{y}_j = 0$ for $i, j \leqslant \frac{n+1}{2}$, it follows that

$$\underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_j} = \begin{cases} 1 & \text{if the last entries of } \mathbf{y}_i, \mathbf{y}_j \text{ are both 1,} \\ 0 & \text{otherwise,} \end{cases} \tag{55}$$

$$\underline{\mathbf{y}_{\frac{n+3}{2}}}^\top \underline{\mathbf{y}_{\frac{n+3}{2}}} = \begin{cases} 1 & \text{if } \mathcal{B} \in \mathfrak{B}_C^1, \\ 0 & \text{if } \mathcal{B} \in \mathfrak{B}_C^2, \end{cases}$$

$$\underline{\mathbf{y}_{\frac{n+3}{2}}}^\top \underline{\mathbf{y}_i} = \underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_{\frac{n+3}{2}}} = \begin{cases} 1 & \text{if } \mathcal{B} \in \mathfrak{B}_C^1 \text{ and the last entry of } \mathbf{y}_i \text{ is 1,} \\ 0 & \text{otherwise.} \end{cases}$$

Observe that at least one vector in $\mathcal{B}$ has the last entry equal to 1 because the opposite would imply that $\mathbf{e}_{n+1} \in C^\perp$, which contradicts the self-duality and the fact that

$\mathbf{e}_{n+1}^\top \mathbf{e}_{n+1} = 1$. Hence, matrices $[\underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_j}]_{i,j=1}^{\frac{n+1}{2}}$ and $[\underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_j}]_{i,j=1}^{\frac{n+3}{2}}$ are both of rank one. Moreover, $\mathrm{Tr}\left([\underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_j}]_{i,j=1}^{\frac{n+3}{2}}\right) = 0$, whereas $\mathrm{Tr}\left([\underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_j}]_{i,j=1}^{\frac{n+1}{2}}\right) = 0$ if and only if $\mathcal{B} \in \mathfrak{B}_C^2$. By Lemma 2.2 and (53)-(54), $A''_{\mathcal{B}} \in SGL_n(\mathbb{F}_2)$ while $A'_{\mathcal{B}} \in SGL_n(\mathbb{F}_2)$ whenever $\mathcal{B} \in \mathfrak{B}_C^2$. Since $\mathbf{y}_1, \ldots, \mathbf{y}_{\frac{n+1}{2}}$ are linearly independent, it follows that $\mathrm{rank}(A'_{\mathcal{B}} - I_n) = \frac{n+1}{2}$. On the other hand,

$$A''_{\mathcal{B}} - I_n = P \begin{pmatrix} I_{\frac{n+1}{2}} + J_{\frac{n+1}{2}} & O \\ O & O \end{pmatrix} P^\top$$

for any $P \in GL_n(\mathbb{F}_2)$ that has $\underline{\mathbf{y}_1}, \ldots, \underline{\mathbf{y}_{\frac{n+1}{2}}}$ as the first $\frac{n+1}{2}$ columns. Since $\det\left(I_{\frac{n+1}{2}} + J_{\frac{n+1}{2}}\right) = 1 + \mathbf{j}_{\frac{n+1}{2}}^\top \mathbf{j}_{\frac{n+1}{2}}$ by Lemma 2.4, it follows that $\mathrm{rank}(A''_{\mathcal{B}} - I_n) = \frac{n+1}{2}$ whenever $\frac{n+1}{2}$ is even. It now follows from Theorems 3.1 and 3.3 that $A'_{\mathcal{B}}, A''_{\mathcal{B}} \in \mathcal{SD}_n$ whenever $A'_{\mathcal{B}}, A''_{\mathcal{B}} \in \mathcal{F}_C$. $\square$

Example 8.4. It is well-known (cf. [21, Theorem 9.5.1]) that there exist three self-dual codes in $\mathbb{F}_2^4$, namely $C_1 = \langle \mathbf{e}_1 + \mathbf{e}_2, \mathbf{j}_4 \rangle$, $C_2 = \langle \mathbf{e}_1 + \mathbf{e}_3, \mathbf{j}_4 \rangle$, $C_3 = \langle \mathbf{e}_1 + \mathbf{e}_4, \mathbf{j}_4 \rangle$. Their families are

$$\mathcal{F}_{C_1} = \left\{ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \right\},$$

$$\mathcal{F}_{C_2} = \left\{ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \right\},$$

$$\mathcal{F}_{C_3} = \left\{ \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \right\}.$$

The set $\mathcal{SD}_3 = \bigcup_{i=1}^3 \mathcal{F}_{C_i}$ can be determined also with the help of Fig. 1.

In view of Theorem 8.3 and the identification $C \leftrightarrow \mathcal{F}_C$, Theorem 8.5 says that self-dual codes are detected by graph parameters $d(A, I_n)$ and $d_{\widehat{\Gamma}_n}(A, I_n)$.

Theorem 8.5. *If $\frac{n+1}{2}$ is odd, then*

$$\mathcal{SD}_n = \left\{ A \in SGL_n(\mathbb{F}_2) \ : \ d(A, I_n) = \tfrac{n+5}{2},\ d_{\widehat{\Gamma}_n}(A, I_n) = \tfrac{n+1}{2} \right\}. \tag{56}$$

If $\frac{n+1}{2}$ is even, then

$$\mathcal{SD}_n = \left\{ A \in SGL_n(\mathbb{F}_2) \ : \ d(A, I_n) = \tfrac{n+5}{2},\ d_{\widehat{\Gamma}_n}(A, I_n) \in \{\tfrac{n+1}{2}, \tfrac{n+3}{2}\} \right\}. \tag{57}$$

Proof. Let $\mathcal{M}$ be the set in the right-hand side of (56)-(57). If $A \in \mathcal{SD}_n$, then $\text{rank}(A - I_n) = \frac{n+1}{2}$ and $A - I_n$ is nonzero. Hence, either $A - I_n$ is nonalternate and $d_{\widehat{\Gamma}_n}(A, I_n) = \text{rank}(A - I_n) = \frac{n+1}{2}$, or $A - I_n$ is alternate with even rank $\frac{n+1}{2}$, in which case $d_{\widehat{\Gamma}_n}(A, I_n) = \text{rank}(A - I_n) + 1 = \frac{n+3}{2}$. Therefore, $A \in \mathcal{M}$.

Conversely, assume that $A \in \mathcal{M}$. Let $r = \text{rank}(A - I_n)$. We split two cases.

Case 1. Let $d_{\widehat{\Gamma}_n}(A, I_n) = \frac{n+1}{2}$. Then, $\frac{n+1}{2} \geqslant r$. Since $\frac{n+5}{2} - r = d(A, I_n) - r \leqslant 2$ by Theorems 3.1 and 3.3, it follows that $r = \frac{n+1}{2}$, i.e. $A \in \mathcal{SD}_n$.

Case 2. Let $d_{\widehat{\Gamma}_n}(A, I_n) = \frac{n+3}{2}$ and $\frac{n+1}{2}$ be even. If $A - I_n$ is alternate, then $r = d_{\widehat{\Gamma}_n}(A, I_n) - 1 = \frac{n+1}{2}$ and $A \in \mathcal{SD}_n$. Assume now that $A - I_n$ is nonalternate. Then, $r = d_{\widehat{\Gamma}_n}(A, I_n) = \frac{n+3}{2}$ is odd and $d(A, I_n) = r + 1$. By Theorem 3.1, $A - I_n = \sum_{i=1}^{r} \mathbf{x}_i^2$ for some linearly independent $\mathbf{x}_1, \ldots, \mathbf{x}_r \in \mathbb{F}_2^n$ such that $\mathbf{x}_i^\top \mathbf{x}_i = 1$ for all i, and there exist i, j such that $\mathbf{x}_i^\top \mathbf{x}_j = 0$. We get a contradiction by Lemma 7.1 (ii) because r is odd. □

In the rest of the paper, we describe how 'classical' automorphisms of the graph Γ_n that fix the identity matrix I_n, namely the maps

$$\Phi(A) = A^{-1} \quad \text{and} \quad \Phi(A) = PAP^\top \text{ where } P^\top = P^{-1} \quad (A \in SGL_n(\mathbb{F}_2)),$$

act on $\mathcal{SD}_n$ (the classification of all automorphisms of Γ_n is expected in [34]). Observe that we really have $\Phi(\mathcal{SD}_n) = \mathcal{SD}_n$ for both automorphisms because

$$\begin{aligned} d\big(\Phi(A), I_n\big) &= d\big(\Phi(A), \Phi(I_n)\big) = d(A, I), \\ \text{rank}(A^{-1} - I_n) &= \text{rank}\,\big(A(A^{-1} - I_n)\big) = \text{rank}(A - I_n), \\ \text{rank}(PAP^\top - I_n) &= \text{rank}\,\big(P(A - I_n)P^\top\big) = \text{rank}(A - I_n) \end{aligned}$$

for all $A \in SGL_n(\mathbb{F}_2)$. We denote $\mathcal{F}_C^{-1} = \{A^{-1} : A \in \mathcal{F}_C\}$, $P\mathcal{F}_C P^\top = \{PAP^\top : A \in \mathcal{F}_C\}$, and refer $P \in GL_n(\mathbb{F}_2)$ with $P^\top = P^{-1}$ as an *orthogonal* matrix. Orthogonal matrices form a group, here denoted by $\mathcal{O}_n(\mathbb{F}_2)$. Given $P \in \mathcal{O}_n(\mathbb{F}_2)$, let $P \oplus 1 \in \mathcal{O}_{n+1}(\mathbb{F}_2)$ be defined by

$$\begin{pmatrix} P & O_{n\times 1} \\ O_{1\times n} & 1 \end{pmatrix}.$$

Observe that $(P \oplus 1)\mathbf{y} = \overline{P\mathbf{y}}$ whenever $\mathbf{y} \in \mathbb{F}_2^{n+1}$ satisfies $\mathbf{y}^\top \mathbf{y} = 0$. Given a self-dual code C in $\mathbb{F}_2^{n+1}$, we denote $(P \oplus 1)C = \{(P \oplus 1)\mathbf{y} : \mathbf{y} \in C\}$.

Theorem 8.6. *$\mathcal{F}_C^{-1} = \mathcal{F}_C$ for each self-dual code C in $\mathbb{F}_2^{n+1}$.*

Proof. Let $A \in \mathcal{F}_C$. Observe from (50)-(51) that there exists a basis $\mathcal{B} = \{\mathbf{y}_1, \ldots, \mathbf{y}_{\frac{n+1}{2}}\} \in \mathfrak{B}_C$ such that either $A = I_n + YY^\top$ or $A = I_n + Y(I_{\frac{n+1}{2}} + J_{\frac{n+1}{2}})Y^\top$ where Y is the

$n \times \left(\frac{n+1}{2}\right)$ matrix with $\underline{\mathbf{y}_i}$ as the i-th column. By Lemma 2.4, $A^{-1} = I_n + YBY^\top$ for a suitable matrix $B \in S_{\frac{n+1}{2}}(\mathbb{F}_2)$. Since $A^{-1} \in \mathcal{SD}_n$, it follows that $\operatorname{rank}(YBY^\top) = \frac{n+1}{2}$, i.e. $B \in SGL_{\frac{n+1}{2}}(\mathbb{F}_2)$. By Lemma 2.1, either $YBY^\top = \sum_{i=1}^{\frac{n+1}{2}} \mathbf{z}_i^2 + (\mathbf{z}_1 + \cdots + \mathbf{z}_{\frac{n+1}{2}})^2$ or $YBY^\top = \sum_{i=1}^{\frac{n+1}{2}} \mathbf{z}_i^2$ for some linearly independent vectors $\mathbf{z}_1, \ldots, \mathbf{z}_{\frac{n+1}{2}} \in \mathbb{F}_2^n$, depending on whether $YBY^\top$ is alternate or not. The alternate case is possible only if $\frac{n+1}{2}$ is even.

We claim that $\langle \mathbf{z}_1, \ldots, \mathbf{z}_{\frac{n+1}{2}} \rangle = \overline{\langle \underline{\mathbf{y}_1}, \ldots, \mathbf{y}_{\frac{n+1}{2}} \rangle}$. If this is not true, then $\mathbf{z}_j \notin \overline{\langle \underline{\mathbf{y}_1}, \ldots, \mathbf{y}_{\frac{n+1}{2}} \rangle}$ for some j. Let $R \in GL_n(\mathbb{F}_2)$ be any invertible matrix with Y as its $n \times \left(\frac{n+1}{2}\right)$ left block and $\mathbf{z}_j$ as its $\left(\frac{n+3}{2}\right)$-th column. Then,

$$R \begin{pmatrix} B & O & O \\ O & -1 & O \\ O & O & O \end{pmatrix} R^\top = YBY^\top - \mathbf{z}_j^2 \in \left\{ \sum_{i \neq j} \mathbf{z}_i^2, \sum_{i \neq j} \mathbf{z}_i^2 + (\mathbf{z}_1 + \cdots + \mathbf{z}_{\frac{n+1}{2}})^2 \right\}$$

is a contradiction because the left-hand side is a matrix of rank $\frac{n+3}{2}$, while the right-hand side is a matrix with rank at most $\frac{n+1}{2}$. Therefore, the set $\dot{\mathcal{B}} = \{\overline{\mathbf{z}}_1, \ldots, \overline{\mathbf{z}}_{\frac{n+1}{2}}\}$ is a basis of C and either $A^{-1} = A''_{\dot{\mathcal{B}}}$ with $\frac{n+1}{2}$ even or $A^{-1} = A'_{\dot{\mathcal{B}}}$. In the last case, (52) yields $\dot{\mathcal{B}} \in \mathfrak{B}_C^2$. Hence, $A^{-1} \in \mathcal{F}_C$. $\square$

Remark 8.7. If $\frac{n+1}{2}$ is even and all members of a basis $\mathcal{B} = \{\mathbf{y}_1, \ldots, \mathbf{y}_{\frac{n+1}{2}}\} \in \mathfrak{B}_C$ have the last entry 1 (i.e. $\underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_j} = 1$ for all i, j), then it follows from Lemma 2.4 and Lemma 2.2 that $(A'_{\mathcal{B}})^{-1} = A''_{\mathcal{B}}$ and $(A''_{\mathcal{B}})^{-1} = A'_{\mathcal{B}}$.

To understand how automorphisms of the form $A \mapsto PAP^\top$, with P orthogonal, act on $\mathcal{SD}_n$, we need two more lemmas. The proof of Lemma 8.8 is straightforward and left to the reader.

Lemma 8.8. *Let C be a self-dual code in $\mathbb{F}_2^{n+1}$ and $P \in \mathcal{O}_n(\mathbb{F}_2)$. Then, $\widetilde{C} = (P \oplus 1)C$ is a self-dual code. Moreover, if $\mathcal{B} = \{\mathbf{y}_1, \ldots, \mathbf{y}_{\frac{n+1}{2}}\} \in \mathfrak{B}_C$, then $\widetilde{\mathcal{B}} = \{(P \oplus 1)\mathbf{y}_1, \ldots, (P \oplus 1)\mathbf{y}_{\frac{n+1}{2}}\} \in \mathfrak{B}_{\widetilde{C}}$ and:*

(i) *$\mathcal{B} \in \mathfrak{B}_C^2$ if and only if $\widetilde{\mathcal{B}} \in \mathfrak{B}_{\widetilde{C}}^2$;*
(ii) *if $A'_{\mathcal{B}} \in \mathcal{F}_C$, then $PA'_{\mathcal{B}}P^\top = A'_{\widetilde{\mathcal{B}}} \in \mathcal{F}_{\widetilde{C}}$;*
(iii) *if $A''_{\mathcal{B}} \in \mathcal{F}_C$, then $PA''_{\mathcal{B}}P^\top = A''_{\widetilde{\mathcal{B}}} \in \mathcal{F}_{\widetilde{C}}$;*
(iv) *$P\mathcal{F}_C P^\top = \mathcal{F}_{\widetilde{C}}$.*

Lemma 8.9. *Each self-dual code C in $\mathbb{F}_2^{n+1}$ has a basis $\{\mathbf{y}_1, \ldots, \mathbf{y}_{\frac{n+1}{2}}\}$ such that $\mathbf{y}_1 + \cdots + \mathbf{y}_{\frac{n+1}{2}} = \mathbf{j}_{n+1}$.*

Proof. Let $\{\mathbf{z}_1, \ldots, \mathbf{z}_{\frac{n+1}{2}}\}$ be an arbitrary basis of C. Since $\mathbf{j}_{n+1} \in C$, there exists a nonempty subset $S \subseteq \{1, \ldots, \frac{n+1}{2}\}$ such that $\mathbf{j}_{n+1} = \sum_{i \in S} \mathbf{z}_i$.

If $S^c = \varnothing$, we select $\mathbf{y}_i = \mathbf{z}_i$. Otherwise, we fix $s \in S$ and $t \in S^c$ to define

$$\mathbf{w}_i = \begin{cases} \mathbf{z}_i & \text{if } i \neq s, \\ \mathbf{z}_s + \mathbf{z}_t & \text{if } i = s. \end{cases}$$

Then, $\mathbf{j}_{n+1} = \sum_{i\in S\cup\{t\}} \mathbf{w}_i$ and $\{\mathbf{w}_1, \dots, \mathbf{w}_{\frac{n+1}{2}}\} \in \mathfrak{B}_C$. Now we repeat the last paragraph (possibly several times) with $S, \mathbf{z}_i$ replaced by $S \cup \{t\}, \mathbf{w}_i$. $\square$

Theorem 8.10. *If $C, \widetilde{C}$ are self-dual codes in $\mathbb{F}_2^{n+1}$, then there exists $P \in \mathcal{O}_n(\mathbb{F}_2)$ such that $\widetilde{C} = (P \oplus 1)C$ and statements (i)-(iv) in Lemma 8.8 are true.*

Proof. It suffices to find $P \in \mathcal{O}_n(\mathbb{F}_2)$ with $\widetilde{C} = (P \oplus 1)C$. The rest follows from Lemma 8.8. If $n = 3$, then it is easily deduced from Example 8.4 that $\mathcal{F}_{\widetilde{C}} = P\mathcal{F}_C P^\top$ for an appropriate permutation matrix P. A straightforward argument shows that the same permutation matrix P satisfies $\widetilde{C} = (P \oplus 1)C$.

Hence, we may assume that $n \geqslant 5$. We claim that there exist $\{\mathbf{z}_1, \dots, \mathbf{z}_{\frac{n+1}{2}}\} \in \mathfrak{B}_C$ and $\{\widetilde{\mathbf{z}}_1, \dots, \widetilde{\mathbf{z}}_{\frac{n+1}{2}}\} \in \mathfrak{B}_{\widetilde{C}}$ such that

$$\underline{\mathbf{z}_1} + \dots + \underline{\mathbf{z}_{\frac{n+1}{2}}} = \mathbf{j}_n = \underline{\widetilde{\mathbf{z}}_1} + \dots + \underline{\widetilde{\mathbf{z}}_{\frac{n+1}{2}}} \tag{58}$$

and

$$\underline{\mathbf{z}_i}^\top \underline{\mathbf{z}_j} = \underline{\widetilde{\mathbf{z}}_i}^\top \underline{\widetilde{\mathbf{z}}_j} \qquad \left(1 \leqslant i, j \leqslant \frac{n+1}{2}\right). \tag{59}$$

Lemma 8.9 provides $\mathcal{B} = \{\mathbf{y}_1, \dots, \mathbf{y}_{\frac{n+1}{2}}\} \in \mathfrak{B}_C, \widetilde{\mathcal{B}} = \{\widetilde{\mathbf{y}}_1, \dots, \widetilde{\mathbf{y}}_{\frac{n+1}{2}}\} \in \mathfrak{B}_{\widetilde{C}}$ with

$$\mathbf{y}_1 + \dots + \mathbf{y}_{\frac{n+1}{2}} = \mathbf{j}_{n+1} = \widetilde{\mathbf{y}}_1 + \dots + \widetilde{\mathbf{y}}_{\frac{n+1}{2}} \tag{60}$$

and therefore

$$\underline{\mathbf{y}_1} + \dots + \underline{\mathbf{y}_{\frac{n+1}{2}}} = \mathbf{j}_n = \underline{\widetilde{\mathbf{y}}_1} + \dots + \underline{\widetilde{\mathbf{y}}_{\frac{n+1}{2}}}. \tag{61}$$

We separate two cases.

Case 1. Let $n = 5$. By (60), either all vectors $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3$ have the last entry 1, or there exist i and distinct $j, k \in \{1, \dots, \frac{n+1}{2}\}\backslash\{i\}$ such that $\mathbf{y}_i$ has the last entry 1, whereas $\mathbf{y}_j, \mathbf{y}_k$ have the last entry 0. In the first case we select $\{\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3\} = \{\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3\}$ whereas in the second case we define $\mathbf{z}_i = \mathbf{y}_i$, $\mathbf{z}_j = \mathbf{y}_j + \mathbf{y}_i$, $\mathbf{z}_k = \mathbf{y}_k + \mathbf{y}_i$. We define $\widetilde{\mathbf{z}}_1, \widetilde{\mathbf{z}}_2, \widetilde{\mathbf{z}}_3$ analogously and achieve (58), (59).

Case 2. Let $n \geqslant 7$. We may assume that each of the bases $\mathcal{B}, \widetilde{\mathcal{B}}$ contains at least one vector with the last entry 0, and at least two vectors with the last entry 1. In fact, if for example $\mathcal{B}$ does not meet this criteria, then as in Case 1 either all vectors in $\mathcal{B}$ have the last entry 1, or $\mathbf{y}_i$, for some i, is the only such vector. In both cases, we select distinct $j, k \in \{1, \dots, \frac{n+1}{2}\} \backslash \{i\}$ and replace $\mathbf{y}_j, \mathbf{y}_k$ by $\mathbf{y}_j + \mathbf{y}_i, \mathbf{y}_k + \mathbf{y}_i$. Since $n \geqslant 7$, we get the desired property while keeping (60).

Further, by permuting the indices we may assume the last entries of $\mathbf{y}_{\frac{n+1}{2}}$ and $\widetilde{\mathbf{y}}_{\frac{n+1}{2}}$ are both 1. Hence,

$$\underline{\mathbf{y}_{\frac{n+1}{2}}}^\top \underline{\mathbf{y}_{\frac{n+1}{2}}} = 1 = \underline{\widetilde{\mathbf{y}}_{\frac{n+1}{2}}}^\top \underline{\widetilde{\mathbf{y}}_{\frac{n+1}{2}}}, \tag{62}$$

$$\underline{\mathbf{y}_{i_1}}^\top \underline{\mathbf{y}_{i_1}} = 1 = \underline{\widetilde{\mathbf{y}}_{j_1}}^\top \underline{\widetilde{\mathbf{y}}_{j_1}}, \tag{63}$$

$$\underline{\mathbf{y}_{i_2}}^\top \underline{\mathbf{y}_{i_2}} = 0 = \underline{\widetilde{\mathbf{y}}_{j_2}}^\top \underline{\widetilde{\mathbf{y}}_{j_2}} \tag{64}$$

for some $i_1, i_2, j_1, j_2 \in \{1, \dots, \frac{n-1}{2}\}$ and (61) is true. Recall from the proof of Theorem 8.3 that matrices $[\underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_j}]_{i,j=1}^{\frac{n+1}{2}}$ and $[\underline{\widetilde{\mathbf{y}}_i}^\top \underline{\widetilde{\mathbf{y}}_j}]_{i,j=1}^{\frac{n+1}{2}}$ are both of rank one, but their traces are 1, as (60) implies that $\mathcal{B} \in \mathfrak{B}_C^1$ and $\widetilde{\mathcal{B}} \in \mathfrak{B}_{\widetilde{C}}^1$. By (62)-(64), we deduce that matrices $[\underline{\mathbf{y}_i}^\top \underline{\mathbf{y}_j}]_{i,j=1}^{\frac{n-1}{2}}$, $[\underline{\widetilde{\mathbf{y}}_i}^\top \underline{\widetilde{\mathbf{y}}_j}]_{i,j=1}^{\frac{n-1}{2}}$ are both in $\mathcal{R}_1^{\mathrm{Tr}_0}$ and they have at least one zero entry. Consequently, by Lemmas 4.15 (i), 4.12, and (61), there exist linearly independent $\mathbf{w}_1, \dots, \mathbf{w}_{\frac{n-1}{2}} \in \mathbb{F}_2^n$, linearly independent $\widetilde{\mathbf{w}}_1, \dots, \widetilde{\mathbf{w}}_{\frac{n-1}{2}} \in \mathbb{F}_2^n$, and permutation matrices $Q, \widetilde{Q} \in GL_{\frac{n-1}{2}}(\mathbb{F}_2)$ such that $\langle \mathbf{w}_1, \dots, \mathbf{w}_{\frac{n-1}{2}} \rangle = \langle \underline{\mathbf{y}_1}, \dots, \underline{\mathbf{y}_{\frac{n-1}{2}}} \rangle$, $\langle \widetilde{\mathbf{w}}_1, \dots, \widetilde{\mathbf{w}}_{\frac{n-1}{2}} \rangle = \langle \underline{\widetilde{\mathbf{y}}_1}, \dots, \underline{\widetilde{\mathbf{y}}_{\frac{n-1}{2}}} \rangle$,

$$\mathbf{w}_1 + \cdots + \mathbf{w}_{\frac{n-1}{2}} + \underline{\mathbf{y}_{\frac{n+1}{2}}} = \mathbf{j}_n = \widetilde{\mathbf{w}}_1 + \cdots + \widetilde{\mathbf{w}}_{\frac{n-1}{2}} + \underline{\widetilde{\mathbf{y}}_{\frac{n+1}{2}}} \tag{65}$$

and

$$[\mathbf{w}_i^\top \mathbf{w}_j]_{i,j=1}^{\frac{n-1}{2}} = Q \begin{pmatrix} J_{2\times 2} & O \\ O & O \end{pmatrix} Q^\top, \quad [\widetilde{\mathbf{w}}_i^\top \widetilde{\mathbf{w}}_j]_{i,j=1}^{\frac{n-1}{2}} = \widetilde{Q} \begin{pmatrix} J_{2\times 2} & O \\ O & O \end{pmatrix} \widetilde{Q}^\top.$$

Hence, by permuting the indices in $\widetilde{\mathbf{w}}_1, \dots, \widetilde{\mathbf{w}}_{\frac{n-1}{2}}$ we may assume that $\mathbf{w}_i^\top \mathbf{w}_j = \widetilde{\mathbf{w}}_i^\top \widetilde{\mathbf{w}}_j$ for all i, j. If we define $\mathbf{z}_i = \overline{\mathbf{w}}_i$, $\widetilde{\mathbf{z}}_i = \overline{\widetilde{\mathbf{w}}_i}$ for $i \leqslant \frac{n-1}{2}$ and $\mathbf{z}_{\frac{n+1}{2}} = \mathbf{y}_{\frac{n+1}{2}}, \widetilde{\mathbf{z}}_{\frac{n+1}{2}} = \widetilde{\mathbf{y}}_{\frac{n+1}{2}}$, then (59) is automatically guaranteed for $i, j \leqslant \frac{n-1}{2}$, while (62) covers the case $i = \frac{n+1}{2} = j$. Moreover, $\{\mathbf{z}_1, \dots, \mathbf{z}_{\frac{n+1}{2}}\} \in \mathfrak{B}_C$, $\{\widetilde{\mathbf{z}}_1, \dots, \widetilde{\mathbf{z}}_{\frac{n+1}{2}}\} \in \mathfrak{B}_{\widetilde{C}}$, and (65) implies (58). Lastly, the equality (58) for $i \leqslant \frac{n-1}{2}$ implies that

$$\begin{aligned}
\underline{\mathbf{z}_i}^\top \underline{\mathbf{z}_{\frac{n+1}{2}}} &= \underline{\mathbf{z}_i}^\top \left(\underline{\mathbf{z}_1} + \cdots + \underline{\mathbf{z}_{\frac{n-1}{2}}} + \mathbf{j}_n \right) \\
&= \underline{\mathbf{z}_i}^\top \left(\underline{\mathbf{z}_1} + \cdots + \underline{\mathbf{z}_{\frac{n-1}{2}}} + \underline{\mathbf{z}_i} \right) \\
&= \underline{\widetilde{\mathbf{z}}_i}^\top \left(\underline{\widetilde{\mathbf{z}}_1} + \cdots + \underline{\widetilde{\mathbf{z}}_{\frac{n-1}{2}}} + \underline{\widetilde{\mathbf{z}}_i} \right) \\
&= \underline{\widetilde{\mathbf{z}}_i}^\top \left(\underline{\widetilde{\mathbf{z}}_1} + \cdots + \underline{\widetilde{\mathbf{z}}_{\frac{n-1}{2}}} + \mathbf{j}_n \right)
\end{aligned}$$

$$= \underline{\widetilde{\mathbf{z}}_i}^\top \underline{\widetilde{\mathbf{z}}_{\frac{n+1}{2}}},$$

which completes the proof of the claim (58)-(59).

Consider the linear map $\sigma : \langle \underline{\mathbf{z}_1}, \ldots, \underline{\mathbf{z}_{\frac{n+1}{2}}} \rangle \to \mathbb{F}_2^n$ defined by $\sigma\left(\underline{\mathbf{z}_i}\right) = \underline{\widetilde{\mathbf{z}}_i}$ for all i. By (58)-(59), $\sigma(\mathbf{j}_n) = \mathbf{j}_n$ and (10) is satisfied for all $\mathbf{u}_1, \mathbf{u}_2 \in \langle \underline{\mathbf{z}_1}, \ldots, \underline{\mathbf{z}_{\frac{n+1}{2}}} \rangle$. By Lemma 4.8, σ can be linearly and injectively extended on $\mathbb{F}_2^n$ such that (10) holds for all $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{F}_2^n$. Consequently, $\sigma(\mathbf{x}) = P\mathbf{x}$ for all $\mathbf{x} \in \mathbb{F}_2$ where $P \in GL_n(\mathbb{F}_2)$ has $\sigma(\mathbf{e}_i)$ as its i-th column. Since the (i,j)-th entry of $P^\top P$ equals $\sigma(\mathbf{e}_i)^\top \sigma(\mathbf{e}_j) = \mathbf{e}_i^\top \mathbf{e}_j$ for all i, j, it follows that P is orthogonal. Since, $\langle P\underline{\mathbf{z}_1}, \ldots, P\underline{\mathbf{z}_{\frac{n+1}{2}}} \rangle = \langle \underline{\widetilde{\mathbf{z}}_1}, \ldots, \underline{\widetilde{\mathbf{z}}_{\frac{n+1}{2}}} \rangle$, we deduce that $\widetilde{C} = \langle \widetilde{\mathbf{z}}_1, \ldots, \widetilde{\mathbf{z}}_{\frac{n+1}{2}} \rangle = \langle \overline{P\underline{\mathbf{z}_1}}, \ldots, \overline{P\underline{\mathbf{z}_{\frac{n+1}{2}}}} \rangle = \langle (P \oplus 1)\mathbf{z}_1, \ldots, (P \oplus 1)\mathbf{z}_{\frac{n+1}{2}} \rangle = (P \oplus 1)C.$ $\square$

By Theorem 8.10, the subgroup $\{P \oplus 1 : P \in \mathcal{O}_n(\mathbb{F}_2)\}$ in $\mathcal{O}_{n+1}(\mathbb{F}_2)$, which is isomorphic to $\mathcal{O}_n(\mathbb{F}_2)$, acts transitively on the set of all self-dual codes in $\mathbb{F}_2^{n+1}$. This improves the result of Janusz [23, Theorem 10], which states that $\mathcal{O}_{n+1}(\mathbb{F}_2)$ acts transitively. Some generators of $\mathcal{O}_n(\mathbb{F}_2)$ can be found in [23,39].

9. Conclusion

The main contribution of this paper is the computation of the distance formula $d(A, B)$ in the graph Γ_n, which generalizes the Coxeter graph (Theorems 3.1 and 3.3). In contrast with the distance formula in graph $\widehat{\Gamma}_n$, which is easy to compute, and equals $d_{\widehat{\Gamma}_n}(A, B) = \operatorname{rank}(A - B)$ whenever $A - B$ is nonalternate or zero, and $d_{\widehat{\Gamma}_n}(A, B) = \operatorname{rank}(A - B) + 1$ otherwise, the formula for $d(A, B)$ is much more complicated. Since Γ_n is an induced subgraph in $\widehat{\Gamma}_n$, we obviously have $d(A, B) \geqslant d_{\widehat{\Gamma}_n}(A, B)$ for all $A, B \in SGL_n(\mathbb{F}_2)$. Theorems 3.1 and 3.3 compute $d(A, B)$ explicitly. In particular, they imply that

$$d(A, B) \in \left\{ d_{\widehat{\Gamma}_n}(A, B), d_{\widehat{\Gamma}_n}(A, B) + 1, d_{\widehat{\Gamma}_n}(A, B) + 2 \right\}$$

for all $A, B \in SGL_n(\mathbb{F}_2)$. With that said, Corollary 7.3 implies that graphs Γ_n and $\widehat{\Gamma}_n$ have the same diameters for $n \geqslant 4$ despite that there exist $A, B \in SGL_n(\mathbb{F}_2)$ such that $\operatorname{diam}(\widehat{\Gamma}_n) = \operatorname{diam}(\Gamma_n) = d(A, B) > d_{\widehat{\Gamma}_n}(A, B)$ as it follows from Theorem 3.1 and Lemma 7.1.

In Section 8, we showed that the graph Γ_n can be used to study binary linear self-dual codes in $\mathbb{F}_2^{n+1}$ where $n \geqslant 3$ is odd. In fact, each matrix in the set

$$\mathcal{SD}_n = \left\{ A \in SGL_n(\mathbb{F}_2) : d(A, I_n) = \tfrac{n+5}{2}, \operatorname{rank}(A - I_n) = \tfrac{n+1}{2} \right\},$$

which equals

$$\left\{ A \in SGL_n(\mathbb{F}_2) \ : \ d(A, I_n) = \tfrac{n+5}{2}, \ d_{\widehat{\Gamma}_n}(A, I_n) = \tfrac{n+1}{2} \right\} \text{ if } \tfrac{n+1}{2} \text{ is odd,} \tag{66}$$

and

$$\left\{A \in SGL_n(\mathbb{F}_2) \ : \ d(A, I_n) = \tfrac{n+5}{2}, \ d_{\widehat{\Gamma}_n}(A, I_n) \in \{\tfrac{n+1}{2}, \tfrac{n+3}{2}\}\right\} \text{if } \tfrac{n+1}{2} \text{ is even,} \qquad (67)$$

induces a self-dual code C in $\mathbb{F}_2^{n+1}$. Conversely, to each self-dual code C we associated a family $\mathcal{F}_C \subseteq \mathcal{SD}_n$. Since $\{\mathcal{F}_C : C \text{ is a self-dual code in } \mathbb{F}_2^{n+1}\}$ is a partition of $\mathcal{SD}_n$ by Theorem 8.3, we can identify C with $\mathcal{F}_C$. With this identification, equations (66)-(67) (i.e. Theorem 8.5) imply that self-dual codes can be described by two graph parameters, $d(A, I_n)$ and $d_{\widehat{\Gamma}_n}(A, I_n)$. It is of great interest in coding theory to know/study which self-dual codes are permutation (in)equivalent. That is, in general it is not known for which self-dual codes C and $\widetilde{C}$ in $\mathbb{F}_2^{n+1}$ there exists a permutation matrix $Q \in GL_{n+1}(\mathbb{F}_2)$ such that $\widetilde{C} = QC$. By considering this problem, Janusz [23, Theorem 10] proved that there always exists an orthogonal matrix $P \in GL_{n+1}(\mathbb{F}_2)$ such that $\widetilde{C} = PC$. In Theorem 8.10, we improved this result and showed that there exists an orthogonal matrix $P \in GL_n(\mathbb{F}_2)$ such that $\widetilde{C} = (P \oplus 1)C$. For any such matrix P, the map $A \mapsto PAP^\top$ is an automorphism of Γ_n that fixes the identity matrix. Theorem 8.10 and Lemma 8.8 imply that such an automorphism acts very naturally on the families $\mathcal{F}_C$ that are associated to self-dual codes. Hence, the identification $C \leftrightarrow \mathcal{F}_C$ gains on the meaning. The parameters $d(A, I_n)$ and $d_{\widehat{\Gamma}_n}(A, I_n)$ that determine the self-dual codes are very basic from a graph theoretical point of view. We expect that a deeper analysis of the graph Γ_n could provide new insights in coding theory in the future.

We could also study matrices in $SGL_n(\mathbb{F}_q)$ over an arbitrary (finite) field $\mathbb{F}_q$ and the distance function in the corresponding graph $\Gamma_n(q)$. However, as briefly mentioned in the introduction, it is expected that, for q large enough, $d_{\Gamma_n(q)}(A, B) = d_{\widehat{\Gamma}_n(q)}(A, B)$ for all $A, B \in SGL_n(\mathbb{F}_q)$ where $\widehat{\Gamma}_n(q)$ is defined analogously as the graph $\widehat{\Gamma}_n = \widehat{\Gamma}_n(2)$. Actually, some computer programming showed us that this equality holds already if $q = 5$ and $n = 3$. A more interesting generalization of the work presented in this paper seems the study of the distance function in the subgraph of $\widehat{\Gamma}_n(q)$, which is induced by the set $\{A \in S_n(\mathbb{F}_q) : \det A = \lambda\}$ for a fixed nonzero $\lambda \in \mathbb{F}_q$. Some basic properties of such a graph are mentioned in [33, Example 3.18].[2] It is possible that this graph contains information about the self-dual codes in $\mathbb{F}_q^{n+1}$ also for some values $q > 2$.

Acknowledgments

The authors thank both referees for their helpful comments, which improved the presentation of the results. The work of Marko Orel is supported in part by The Slovenian Research and Innovation Agency (research program P1-0285 and research projects N1-0140, N1-0208, N1-0210, J1-4084, N1-0296 and J1-50000). The work of Draženka Višnjić is supported in part by The Slovenian Research and Innovation Agency (research program P1-0285 and Young Researchers Grant).

[2] Depending on λ, there are two nonisomorphic graphs if n is even and q is odd.

Data availability

No data was used for the research described in the article.

References

[1] L. Babai, Automorphism groups, isomorphism, reconstruction, in: G.L. Graham, M. Grötschel, L. Lovász (Eds.), Handbook of Combinatorics, vol. 1, 2, Elsevier Sci. B. V., Amsterdam, 1995, pp. 1447–1540.
[2] E. Bannai, T. Ito, Algebraic Combinatorics. I. Association Schemes, The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, 1984.
[3] J.-C. Bermond, Hamiltonian graphs, in: L.W. Beinke, R.J. Wilson (Eds.), Selected Topics in Graph Theory, Academic Press, London, 1978, pp. 127–167.
[4] A.E. Brouwer, A.M. Cohen, A. Neumaier, Distance-Regular Graphs, Ergeb. Math. Grenzgeb. (3), vol. 18, Springer-Verlag, Berlin, 1989.
[5] J.H. Conway, V. Pless, On the enumeration of self-dual codes, J. Comb. Theory, Ser. A 28 (1980) 26–53, https://doi.org/10.1016/0097-3165(80)90057-6.
[6] J.H. Conway, V. Pless, N.J.A. Sloane, The binary self-dual codes of length up to 32: a revised enumeration, J. Comb. Theory, Ser. A 60 (1992) 183–195, https://doi.org/10.1016/0097-3165(92)90003-D.
[7] A. Cossidente, G. Marino, F. Pavese, On symmetric and Hermitian rank distance codes, J. Comb. Theory, Ser. A 188 (2022) 105597, https://doi.org/10.1016/j.jcta.2022.105597.
[8] H.S.M. Coxeter, My graph, Proc. Lond. Math. Soc. 46 (1983) 117–136.
[9] B. Csajbók, G. Marino, O. Polverino, C. Zanella, A new family of MRD-codes, Linear Algebra Appl. 548 (2018) 203–220, https://doi.org/10.1016/j.laa.2018.02.027.
[10] C. de Seguins Pazzis, P. Šemrl, Hua's fundamental theorem of geometry of rectangular matrices over EAS division rings, J. Algebra 439 (2015) 159–187.
[11] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, J. Comb. Theory, Ser. A 25 (1978) 226–241, https://doi.org/10.1016/0097-3165(78)90015-8.
[12] T. Dobson, A. Malnič, D. Marušič, Symmetry in Graphs, Cambridge Studies in Advanced Mathematics, vol. 198, Cambridge University Press, Cambridge, 2022.
[13] È.M. Gabidulin, Theory of codes with maximum rank distance, Probl. Pereda. Inf. 21 (1985) 3–16.
[14] È.M. Gabidulin, N.I. Pilipchuk, Symmetric rank codes, Probl. Pereda. Inf. 40 (2004) 3–18 (in Russian); English translation in Probl. Inf. Transm. 40 (2004) 103–117, https://doi.org/10.1023/B:PRIT.0000043925.67309.c6.
[15] X. Hou, On the asymptotic number of inequivalent binary self-dual codes, J. Comb. Theory, Ser. A 114 (2007) 522–544, https://doi.org/10.1016/j.jcta.2006.07.003.
[16] R. Gow, M. Lavrauw, J. Sheekey, F. Vanhove, Constant rank-distance sets of Hermitian matrices and partial spreads in Hermitian polar spaces, Electron. J. Comb. 21 (2014) P1.26, https://doi.org/10.37236/3534.
[17] L.-P. Huang, Z. Huang, C.-K. Li, N.-S. Sze, Graphs associated with matrices over finite fields and their endomorphisms, Linear Algebra Appl. 447 (2014) 2–25, https://doi.org/10.1016/j.laa.2013.12.030.
[18] L.-P. Huang, J.-Q. Huang, K. Zhao, On endomorphisms of alternating forms graph, Discrete Math. 338 (2015) 110–121, https://doi.org/10.1016/j.disc.2014.10.017.
[19] W.-L. Huang, P. Šemrl, Adjacency preserving maps on Hermitian matrices, Can. J. Math. 60 (2008) 1050–1066, https://doi.org/10.4153/CJM-2008-047-1.
[20] W.-L. Huang, P. Šemrl, The optimal version of Hua's fundamental theorem of geometry of square matrices–the low dimensional case, Linear Algebra Appl. 498 (2016) 21–57.
[21] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[22] A.A. Ivanov, S.V. Shpectorov, A characterization of the association schemes of Hermitian forms, J. Math. Soc. Jpn. 43 (1991) 25–48, https://doi.org/10.2969/jmsj/04310025.
[23] G.J. Janusz, Parametrization of self-dual codes by orthogonal matrices, Finite Fields Appl. 13 (2007) 450–491, https://doi.org/10.1016/j.ffa.2006.05.001.
[24] K. Kutnar, D. Marušič, Hamilton cycles and paths in vertex-transitive graphs–current directions, Discrete Math. 309 (2009) 5491–5500, https://doi.org/10.1016/j.disc.2009.02.017.

[25] B. Kuzma, M. Orel, Additive mappings on symmetric matrices, Linear Algebra Appl. 418 (2006) 277–291, https://doi.org/10.1016/j.laa.2006.02.010.

[26] L. Lovász, Combinatorial structures and their applications, in: Proc. Calgary Internat. Conf., Calgary, Alberta, 1969, Gordon and Breach, New York, 1970, pp. 243–246, Problem 11.

[27] D. Marušič, Hamiltonian circuits in Cayley graphs, Discrete Math. 46 (1983) 49–54, https://doi.org/10.1016/0012-365X(83)90269-8.

[28] M. Orel, A note on adjacency preservers on Hermitian matrices over finite fields, Finite Fields Appl. 15 (2009) 441–449, https://doi.org/10.1016/j.ffa.2009.02.005.

[29] M. Orel, Adjacency preservers on invertible Hermitian matrices I, Linear Algebra Appl. 499 (2016) 99–128, https://doi.org/10.1016/j.laa.2014.10.034.

[30] M. Orel, Adjacency preservers on invertible Hermitian matrices II, Linear Algebra Appl. 499 (2016) 129–146, https://doi.org/10.1016/j.laa.2014.10.033.

[31] M. Orel, Adjacency preservers, symmetric matrices, and cores, J. Algebraic Comb. 35 (2012) 633–647, https://doi.org/10.1007/s10801-011-0318-0.

[32] M. Orel, On generalizations of the Petersen and the Coxeter graph, Electron. J. Comb. 22 (2015) P.4.27, https://doi.org/10.37236/3759.

[33] M. Orel, Preserver problems over finite fields, in: J. Simmons (Ed.), Finite Fields: Theory, Fundamental Properties and Applications, Nova Science Publishers, New York, 2017, pp. 1–54.

[34] M. Orel, D. Višnjić, Homomorphisms from the Coxeter-like graphs, in preparation.

[35] V. Pless, On Witt's theorem for nonalternating symmetric bilinear forms over a field of characteristic 2, Proc. Am. Math. Soc. 15 (1964) 979–983, https://doi.org/10.2307/2034921.

[36] A. Ravagnani, Rank-metric codes and their duality theory, Des. Codes Cryptogr. 80 (2016) 197–216, https://doi.org/10.1007/s10623-015-0077-3.

[37] K.-U. Schmidt, Quadratic and symmetric bilinear forms over finite fields and their association schemes, Algebraic Combin. 3 (2020) 161–189, https://doi.org/10.5802/alco.88.

[38] M. Shi, D.S. Krotov, F. Özbudak, Constructing MRD codes by switching, J. Comb. Des. 32 (2024) 219–237, https://doi.org/10.1002/jcd.21931.

[39] M. Shi, L. Sok, P. Solé, S. Çalkavur, Self-dual codes and orthogonal matrices over large finite fields, Finite Fields Appl. 54 (2018) 297–314, https://doi.org/10.1016/j.ffa.2018.08.011.

[40] P. Šemrl, The optimal version of Hua's fundamental theorem of geometry of rectangular matrices, Mem. Am. Math. Soc. 232 (1089) (2014), https://doi.org/10.1090/memo/1089, vi+74 pp.

[41] J. Sheekey, A new family of linear maximum rank distance codes, Adv. Math. Commun. 10 (2016) 475–488, https://doi.org/10.3934/amc.2016019.

[42] D. Silva, F.R. Kschischang, R. Kötter, A rank-metric approach to error control in random network coding, IEEE Trans. Inf. Theory 54 (2008) 3951–3967, https://doi.org/10.1109/TIT.2008.928291.

[43] M. Tsatsomeros, Matrix equalities and inequalities, in: L. Hogben (Ed.), Handbook of Linear Algebra, second ed., CRC Press, Boca Raton (FL), 2014, 16.

[44] Z.-X. Wan, Geometry of Matrices, World Scientific Publishing Co., Inc., Singapore, 1996.

[45] F. Zhang, Matrix Theory, Basic Results and Techniques, 2nd ed., Universitext, Springer, New York, 2011.