Range of Symmetric Matrices over $GF(2)$

Yuval Filmus

January 2010

Abstract

We prove that the range of a symmetric matrix over $GF(2)$ always contains its diagonal. This is best possible in several ways, for example $GF(2)$ cannot be replaced by any other field.

1 Introduction

We prove the following theorem:

Definition 1.1. *The* diagonal *of a matrix M, notated* $\operatorname{diag} M$*, is the vector composed of the diagonal elements of M.*

Theorem 1.1. *Let M be a symmetric matrix over $GF(2)$. Then* $\operatorname{diag} M \in \operatorname{range} M$*.*

This theorem is best possible in several ways:

1. We can't drop the assumption that M is symmetric. The simplest example is $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$.
2. We can't replace $GF(2)$ with any other field. The matrix $\begin{pmatrix} 1 & x \\ x & x^2 \end{pmatrix}$ is an example, for any $x \neq 0, 1$.
3. We can't guarantee the existence of any other non-zero vector in $\operatorname{range} M$. Indeed, if M is a block matrix composed of an all-ones block and an all-zeroes block, $\operatorname{range} M = \{0, \operatorname{diag} M\}$.

2 Proof

We begin with a definition:

Definition 2.1. *A matrix M over $GF(2)$ is called* realizable *if* $\operatorname{diag} M \in \operatorname{range} M$.

Our goal is to show that all symmetric matrices are realizable. We will do so by applying a reduction operation which preserves realizability, until the matrix reduces to a very simple form which is trivially realizable.

Definition 2.2. *Let M be a symmetric matrix, S be a subset of the indices, and i an index not in S. The* reduction of M obtained by adding S to i, *$N = M[S \to i]$, is defined as follows:*

$$N_{pq} = M_{pq} + \delta(p,i) \sum_{j \in S} M_{jq} + \delta(q,i) \sum_{j \in S} M_{pj}.$$

The notation $\delta(x,y)$ means 1 if $x = y$ and 0 if $x \neq y$.

Definition 2.3. *The set S is* admissible *with respect to a matrix M if*

$$\sum_{j \in S} M_{jj} = 0.$$

A reduction with an admissible set is an admissible reduction*.*

Applying a reduction to a symmetric matrix results in a symmetric matrix with the same diagonal.

Lemma 2.1. *If M is a symmetric matrix, S is a subset of the indices, and $i \notin S$, then $N = M[S \to i]$ is a symmetric matrix and* $\operatorname{diag} M = \operatorname{diag} N$.

Proof. First, we show that N is symmetric:

$$\begin{aligned} N_{pq} &= M_{pq} + \delta(p,i) \sum_{j \in S} M_{jq} + \delta(q,i) \sum_{j \in S} M_{pj} \\ &= M_{qp} + \delta(q,i) \sum_{j \in S} M_{jp} + \delta(p,i) \sum_{j \in S} M_{qj} = N_{qp}. \end{aligned}$$

Second, we calculate the diagonal of N:

$$N_{pp} = M_{pp} + \delta(p,i) \sum_{j \in S} M_{jp} + \delta(p,i) \sum_{j \in S} M_{pj} = M_{pp}. \qquad \square$$

Reduction is a reversible operation.

Lemma 2.2. *If $N = M[S \to i]$ then $M = N[S \to i]$.*

Proof. This is an easy computation. Let $L = N[S \to i]$. Then

$$\begin{aligned} L_{pq} &= N_{pq} + \delta(p,i) \sum_{j \in S} N_{jq} + \delta(q,i) \sum_{j \in S} N_{pj} \\ &= M_{pq} + \delta(p,i) \sum_{j \in S} (M_{jq} + N_{jq}) + \delta(q,i) \sum_{j \in S} (M_{pj} + N_{pj}) \\ &= M_{pq} + \delta(p,i)\delta(q,i) \sum_{j \in S} \sum_{k \in S} M_{jk} + \delta(q,i)\delta(p,i) \sum_{j \in S} \sum_{k \in S} M_{kj} = M_{pq}. \square \end{aligned}$$

If the reduction is admissible, then there is a close connection between the ranges of both matrices.

Lemma 2.3. *If $N = M[S \to i]$ and S is admissible for M then the range of N is obtained from the range of M as follows:*

$$\operatorname{range} N = \left\{ v + \left(\sum_{j \in S} v_j \right) e_i : v \in \operatorname{range} M \right\},$$

where e_i is the ith basis vector. In words, the range of N is obtained from the range of M by adding the columns in S to column i.

Proof. Let x be a vector. We calculate Nx:

$$\begin{aligned} (Nx)_p &= \sum_q N_{pq} x_q \\ &= \sum_q \left(M_{pq} + \delta(p,i) \sum_{j \in S} M_{jq} + \delta(q,i) \sum_{j \in S} M_{pj} \right) x_q \\ &= \sum_q M_{pq} x_q + \delta(p,i) \sum_{j \in S} M_{jq} x_q + \sum_{j \in S} M_{pj} x_i \\ &= (Mx)_p + \delta(p,i)(Mx)_j + x_i \left(M \sum_{j \in S} e_j \right)_p . \end{aligned}$$

This prompts us to defined

$$y = x + x_i \sum_{j \in S} e_j.$$

Since $i \notin S$, we similarly have

$$x = y + y_i \sum_{j \in S} e_j.$$

Rewriting our earlier result,

$$\begin{aligned}
(Nx)_p &= (Mx)_p + \delta(p,i)(Mx)_j + x_i \left(M \sum_{j \in S} e_j \right)_p \\
&= (My)_p + \delta(p,i)(My)_j + \delta(p,i) y_i \left(M \sum_{j \in S} e_j \right)_j \\
&= (My)_p + \delta(p,i)(My)_j + \delta(p,i) y_i \sum_{j \in S} M_{jj} \\
&= (My)_p + \delta(p,i)(My)_j.
\end{aligned}$$

Here we used the admissibility of S. The result follows since the function transforming x to y is a bijection on the domain of M. □

As a corollary, we obtain that an admissible reduction preserves realizability.

Corollary 2.4. *If $N = M[S \to i]$ and S is admissible then N is realizable if and only if M is realizable.*

Proof. Suppose M is realizable. Denote $v = \operatorname{diag} M = \operatorname{diag} N$. Thus $v \in \operatorname{range} M$. Since

$$\sum_{j \in S} v_j = \sum_{j \in S} M_{jj} = 0,$$

by the lemma also $v \in \operatorname{range} N$. □

We need several more trivial results.

Lemma 2.5. *If a column of a matrix M is equal to $\operatorname{diag} M$, then M is realizable.*

Lemma 2.6. *Suppose M is a block matrix. If all blocks of M are realizable, then so is M.*

Definition 2.4. *If $M_{ij} = M_{ji} = 0$ for $j \neq i$, the index i is called* lonely. *The matrix without row and column i is denoted M^{-i}.*

Corollary 2.7. *Let M be a matrix with a lonely index i. If M^{-i} is realizable then so is M.*

We now have enough tools at our disposal to prove the theorem.

Theorem 2.8. *All matrices are realizable.*

Proof. The proof is by induction on n. The base case $n = 1$ is trivial.

Let M be an $n \times n$ matrix. Define $S = \{i : M_{ii} = 1\}$. If $S = \varnothing$ then $\operatorname{diag} M = 0$ and so the theorem is trivial.

Suppose next that $S = \{s\}$. Assume first that $M_{ab} = 0$ for all $a, b \neq s$. If $M_{st} = 1$ for some $t \neq s$ then column t represents M. If $M_{st} = 0$ for all $t \neq s$ then column s represents M.

Thus we can assume that $M_{ab} = 1$ for some $a, b \neq s$. Since $M_{aa} = M_{bb} = 0$, we can add a to c for any other index c satisfying $M_{bc} = 1$, and b to d for any other index d satisfying $M_{ad} = 1$. In the resulting matrix N, $N_{ae} = N_{be} = 0$ for $e \neq a, b$. Thus N can be split into two blocks, $\{a, b\}$ and the rest. The block corresponding to $\{a, b\}$ is trivially realizable, and by induction so is the other block. Thus N is realizable, hence M is realizable.

From now on, we assume that $|S| > 1$. We consider several cases. Suppose first that there exist $i \neq j \in S$ such that $M_{ij} = 0$. Since $M_{ii} + M_{jj} = 0$, we can add i, j to all $k \neq i$ satisfying $M_{ik} = 1$. In the resulting matrix N, the index i is lonely. By induction, N^{-i} is realizable, hence so are N and M.

Suppose next that there are indices $i \neq j \in S$ and $k \notin S$ such that $M_{ij} = M_{ik} = 1$. Since $M_{kk} = 0$, we can add k to j. The resulting matrix N satisfies $N_{ij} = 0$, and so the previous case applies.

Finally, suppose that none of the other cases apply. Thus for all $i, j \in S$ we have $M_{ij} = 1$, and for all $i \in S$, $k \notin S$ we have $M_{ik} = 0$. Therefore M is a block matrix consisting of an all-ones block and a block whose diagonal is zero. Any column $i \in S$ realizes M. $\square$

3 Recursive Proof for Forests

Any matrix over $GF(2)$ corresponds to a graph. In this section we prove the theorem for matrices which correspond to forests (we allow arbitrary self-loops).

We first need a definition.

Definition 3.1. *Let M be the adjacency matrix of a rooted tree, and suppose r is the index of the root. A vector x is said to* (α, β)-realize *M if $Mx = \operatorname{diag} M + \alpha e_r$ and $x_r = \beta$.*

Furthermore, M is (α, β)-realizable if some vector (α, β)-realizes it.

A $(*, \beta)$-realization is either a $(0, \beta)$- or a $(1, \beta)$-realization. An $(\alpha, *)$-realization is defined similarly.

We can divide all trees into three classes, as the following theorem shows.

Theorem 3.1. *Let M be the adjacency matrix of a rooted tree. Then M belongs to one of the following classes:*

Class 0: *M is (α, β)-realizable iff $\alpha + \beta = 1$.*

Class 1: *M is (α, β)-realizable iff $\alpha = 0$.*

Class 2: *M is (α, β)-realizable iff $\beta = 0$.*

Note that the classes are mutually exclusive, and that in all classes, M is $(0, *)$-realizable, and so it is realizable (in the original sense).

Proof. The proof is by induction on the height of the tree. The base case is when M consists of a leaf. One can easily check that $M = (0)$ is class 1 and $M = (1)$ is class 0.

Next, let M represent a tree T, and consider the (non-empty) set of subtrees of the root. We denote the root of a subtree S by $r(S)$. There are two fundamental cases.

One of the subtrees S is class 1. We claim that in this case, T is class 2. First, we show that T is $(\alpha, 0)$-realizable for both choices of α. By induction, all subtrees of T other than S are $(0, *)$-realizable. The subtree S is by assumption $(0, \beta)$-realizable for both choices of β. By combining all these realizations along with $x_r = 0$, we get two vectors x^β that differ only on S. Since $x^\beta_{r(S)} = \beta$, we see that Mx^0, Mx^1 differ on r. Thus they $(\alpha, 0)$-realize T for both possibilities of α.

Second, we claim that T is not $(\alpha, 1)$-realizable for any α. For suppose x is an $(\alpha, 1)$-realization of T. Then x_S, the part consisting of the vertices of S, $(1, *)$-realizes S, which contradicts the definition of class 1.

None of the subtrees is class 1. In that case, each subtree S_i is (α, β)-realizable only for $\beta = f_i(\alpha)$, where either $f_i(\alpha) = 1+\alpha$ (class 0) or $f_i(\alpha) = 0$ (class 2). Notice that in both cases, $f_i(1) = 0$. In any $(*, 1)$-realization of T, all the subtrees must be $(1, 0)$-realized, and so this in fact a $(0, 1)$-realization of T. Similarly, in any $(*, 0)$-realization of T, subtree S_i must be $(0, f_i(0))$-realized. Setting $a = M_{rr} + \sum f_i(0)$, this is always an $(a, 0)$-realization of T. Notice that in both cases, such realizations are actually possible. Thus T is class 1 if $a = 0$ and class 0 if $a = 1$. □

Corollary 3.2. *All forests are realizable.*

The proof of the theorem shows that a vertical path of length k with self-loops in all vertices is class $(k \mod 3)$. If there are no self-loops at all, it is class $1 + (k \mod 2)$.

4 Noga Alon's Proof

Here is Noga's original proof. For every vector x and symmetric matrix M,

$$\begin{aligned} x^T M x &= \sum_{i,j} x_i M_{ij} x_j \\ &= \sum_i x_i M_{ii} x_i + \sum_{i<j} (x_i M_{ij} x_j + x_j M_{ij} x_i) \\ &= \sum_i M_{ii} x_i = x^T \operatorname{diag} M. \end{aligned}$$

Therefore $\operatorname{diag} M \perp \ker M$, i.e.

$$\operatorname{diag} M \in (\ker M)^\perp = \operatorname{range} M^T = \operatorname{range} M.$$

The proof is non-constructive since the connection between $\ker M$ and $\operatorname{range} M^T$ is proved by comparing dimensions.

5 Thanks

I thank Moti Levy for spotting out a mistake in the proof of Corollary 2.4, and Moron for letting me know Noga's proof.