On products of linear error correcting codes

Mirandola, D.

Chapter 5

On Secret Sharing with Non-linear Product Reconstruction

5.1 Overview

Multiplicative linear secret sharing is a fundamental notion in the area of secure multi-party computation (MPC). By extension, this holds in the area of two-party cryptography as well, by virtue of recently discovered deep applications of MPC to two-party cryptography as initiated in [39].

While linear secret sharing is additive in the sense that "the sum of share vectors corresponds to the sum of the secrets", multiplicative linear secret sharing enjoys the further property that "the product of two secrets is obtained as a linear function of the vector consisting of the coordinatewise product of two respective share vectors". There are several important (more demanding) variations on this notion, such as strongly multiplicative secret sharing. First framed and studied in [27] in the late 1990s as an abstract property of a linear secret sharing scheme[1], it had been implicit in several results since the mid 1980s (notably [7, 18, 35]) in the context of the application of Shamir's secret sharing scheme [67] to (information-theoretically) secure multi-party computation. The *asymptotical* (constant-rate) theory of strongly multiplica-

[1] It was shown, in particular, when and how a multiplicative scheme can be obtained from just a linear secret sharing scheme. However, this does not work for strong multiplicativity.

tive schemes has been initiated in [19], using algebraic geometry[2]. It has found several notable applications, starting with [39]. For a full discussion and references, please refer to [15].

This chapter focuses on the following foundational question, which is novel to the best of our knowledge. Suppose we *abandon the latter linearity condition* and instead require that the product of the two secrets is obtained by application of *some*, *not-necessarily-linear* "product reconstruction function". *Is the resulting notion equivalent to multiplicative linear secret sharing?* We show the (perhaps somewhat counter-intuitive) result that this relaxed notion is strictly *more general*.

Throughout this chapter, let $\mathbb{F}$ be a finite field of size q, n a positive integer, and let V be a finite-dimensional $\mathbb{F}$-vector space. When the field size needs to be put in evidence, we will use the notation $\mathbb{F}_q$ for the base field.

Definition 5.1.1. Let $(\pi_0, \ldots, \pi_n) \subseteq V^*$ be a secret sharing scheme. The scheme has *product reconstruction* if, for all $x, x', y, y' \in V$ with

$$\pi_1(x)\pi_1(y) = \pi_1(x')\pi_1(y'), \ldots, \pi_n(x)\pi_n(y) = \pi_n(x')\pi_n(y'),$$

it holds that

$$\pi_0(x)\pi_0(y) = \pi_0(x')\pi_0(y').$$

Note that the product reconstruction condition is equivalent to the existence of a *product reconstruction function* $\rho' : \mathbb{F}^n \longrightarrow \mathbb{F}$ such that

$$\rho'(\pi_1(x)\pi_1(y), \ldots, \pi_n(x)\pi_n(y)) = \pi_0(x)\pi_0(y),$$

for all $x, y \in V$. In particular, a multiplicative secret sharing scheme (see Definition 2.6.5) is one for which a *linear* product reconstruction function exists. To separate and compare the two multiplicativity notions, we say that a scheme is *M1* if it is multiplicative in the sense of Definition 2.6.5, *M2* if it admits a non-necessarily-linear product reconstruction function as required by Definition 5.1.1. Thus, an M1 scheme is also M2. As a consequence of our results the converse does not hold.

Remark 5.1.2. There does not appear to be much that one can say, a priori, about the complexity of such not-necessarily-linear product reconstruction functions. At best, one can say that in order to determine the product of two secrets from the coordinatewise product of two corresponding share vectors, it suffices to solve a system of quadratic equations.

The main result of this chapter is the following.

[2]Later, this asymptotical theory has also been developed in the case of *multiplicative* schemes using classical coding theory in [5]. The results there do not seem to carry over easily to strong multiplicative schemes.

MAIN THEOREM 5.1.3. *For any prime power q, there exists a function $t_q(n) \in \Omega(n)$ such that, for infinitely many $n \in \mathbb{N}$, there exists an $\mathbb{F}_q$-vector space V and a secret sharing scheme $(\pi_0, \ldots, \pi_n) \subseteq V^*$ which has $t_q(n)$-privacy and admits a product reconstruction function. However, such function is necessarily not $\mathbb{F}_q$-linear. Therefore, the scheme is M2 but not M1.*

The existence of such counterexamples can be explained from the difference between linear and algebraic independence of certain multivariate polynomials. For instance, the polynomials X, Y, XY are linearly independent but algebraically dependent. Nevertheless, since the involved polynomials are homogeneous with degree 2, quadratic forms are a powerful tool to solve our problem. Indeed, by means of combinatorial arguments involving bilinear and quadratic forms, we find examples of linear secret sharing schemes with non-linear product reconstruction on a small number of players.

THEOREM 5.1.4. *For every finite field $\mathbb{F}_q$ of size $q \geq 3$, there exists an $\mathbb{F}_q$-linear secret sharing scheme on 9 players that is M2 but not M1. In addition, there exists an $\mathbb{F}_2$-linear secret sharing scheme on 14 players that is M2 but not M1.*

Our main result is then obtained by composing those small examples with multiplicative linear secret sharing schemes on n players that have t-privacy with $t = \Omega(n)$. The existence of such schemes over any fixed base field was proved in [11, 20]. As an additional result, we prove that, for every finite field $\mathbb{F}_q$ of size $q \geq 3$, $n = 9$ is the minimum value for which there exists an $\mathbb{F}_q$-linear secret sharing scheme on n players that is M2 but not M1. This value remains undetermined for $q = 2$, but it is at least 9.

THEOREM 5.1.5. *Every M2 secret sharing scheme on less than 9 players is also M1.*

Our results extend to similar separation results for important variations, such as strongly multiplicative secret sharing.

THEOREM 5.1.6. *For any prime power q, there exists a function $\hat{t}_q(n) \in \Omega(n)$ such that, for infinitely many $n \in \mathbb{N}$, there exists an $\mathbb{F}_q$-vector space V and a secret sharing scheme $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$ which has $\hat{t}_q(n)$-privacy and such that, for each set $I \subseteq \mathcal{P}$ consisting of $n - \hat{t}_q(n)$ players, the scheme Σ_I admits a product reconstruction function (M2). However there exists a set $J \subseteq \mathcal{P}$ with $n - \hat{t}_q(n)$ players such that Σ_J is not M1. Therefore, Σ is not $\hat{t}_q(n)$-strongly multiplicative.*

It is an interesting question whether there are applications of this "exotic",

novel class of secret sharing schemes with non-linear product reconstruction[3] to cryptographic protocols, but we will not offer any speculations here.

We remark that, while the notion of multiplicativity defined in [27] applies to linear secret sharing schemes where each share may consist of an arbitrary number of elements of the base field, in this work our definitions and results concern only *ideal* linear secret sharing schemes, i.e., those where each share is a *single* field element. This is the notion considered in e.g. [11, 19, 20]. If the local function is the component-wise product of the share-vectors, then the analysis is the same for both cases. If any bilinear function can be used in the local computations, then the general case can be reduced to the case of ideal schemes (maybe except for fields of characteristic 2) [4].

This chapter is organized as follows. In Section 5.2 we show that both the multiplicativity notion and its relaxed notion of product reconstruction can be captured in terms of the existence of quadratic forms with certain algebraic conditions imposed on them (see Propositions 5.2.1 and 5.2.2). This leads us to defining the "separating quadratic forms", which are characterized in Propositions 5.2.4 and 5.2.5 by using the classification of quadratic forms over finite fields. For any necessary theoretical background, the reader is referred to the introductory Sections 2.3 and 2.4.

By using those results, several examples of linear secret sharing schemes that prove the separation between the two notions are presented in Section 5.3. Specifically, for every finite field $\mathbb{F}_q$, we present examples of $\mathbb{F}_q$-linear secret sharing schemes with non-linear product reconstruction on n players, where $n = 9$ if $q \geq 3$ and $n = 14$ if $q = 2$. This constitute the proof of Theorem 5.1.4.

In Section 5.4, we analyze the behavior of the relaxed notion of product reconstruction under the composition of secret sharing schemes defined in Section 2.6.1 and we prove Main Theorem 5.1.3 by composing the examples on a small number of players presented in Section 5.3 with multiplicative linear secret sharing schemes whose privacy is linear in the number of players. Moreover, we show how to extend our results to strongly multiplicative secret sharing using the same composition technique, proving Theorem 5.1.6.

Finally, in Section 5.5 we prove Theorem 5.1.5, which states that it is not possible to find examples separating the two notions on less than 9 players. Therefore, the examples presented in Section 5.3 are among the smallest ones.

[3] All applications of multiplicative linear secret sharing we are aware of make essential use of linearity of product reconstruction.

[4] Of course our results do not rule out that separating examples with a smaller number of players exist in the non-ideal case, but we do not elaborate further on this matter.

5.2 Separating Quadratic Forms

In this section we characterize properties M1 and M2, or rather, their negations, separately. The characterization of the M2 property is given in terms of a class of quadratic forms, which we call separating as they allow us to distinguish the two multiplicativity notions. Finally, we provide a characterization for this class.

PROPOSITION 5.2.1. *A secret sharing scheme $(\pi_0, \ldots, \pi_n) \subseteq V^*$ is not M1 if and only if there exists a quadratic form $Q \in \mathrm{Quad}(V^*)$ such that $Q(\pi_1) = \cdots = Q(\pi_n) = 0$ and $Q(\pi_0) \neq 0$.*

PROOF. Straightforward from Proposition 2.6.6 and the isomorphism between $\mathrm{Sym}(V)^*$ and $\mathrm{Quad}(V^*)$ in Lemma 2.4.2. Here we use the following trivial fact from linear algebra: if V is an $\mathbb{F}$-vector space, $W \subseteq V$ is a subspace and $x \in V$ is a vector, then $x \notin W$ if and only if there exists a linear form $\pi \in V^*$ such that $\pi(x) \neq 0$ and $\pi(y) = 0$ for all $y \in W$. □

Given $x, y, x', y' \in V$, define the bilinear form $T_{x,y,x',y'} := x \otimes y - x' \otimes y' \in \mathrm{Bil}(V^*)$ and its associated quadratic form $Q_{x,y,x',y'} \in \mathrm{Quad}(V^*)$.

PROPOSITION 5.2.2. *A secret sharing scheme $(\pi_0, \ldots, \pi_n) \subseteq V^*$ is not M2 if and only if there exist vectors $x, y, x', y' \in V$ such that $Q_{x,y,x',y'}(\pi_1) = \cdots = Q_{x,y,x',y'}(\pi_n) = 0$ and $Q_{x,y,x',y'}(\pi_0) \neq 0$.*

PROOF. Obvious from Definition 5.1.1. □

DEFINITION 5.2.3. A quadratic form $Q \in \mathrm{Quad}(V^*)$ is called *separating* if $Q \neq Q_{x,y,x',y'}$ for every $x, y, x', y' \in V$, *non-separating* otherwise.

Using this notion, Proposition 5.2.2 claims that $(\pi_0, \ldots, \pi_n)$ is not M2 if and only if there exists a non-separating quadratic form $Q \in \mathrm{Quad}(V^*)$ such that $Q(\pi_1) = \cdots = Q(\pi_n) = 0$ and $Q(\pi_0) \neq 0$.

As a consequence of the two propositions above, a secret sharing scheme $(\pi_0, \ldots, \pi_n) \subseteq V^*$ is M2 but not M1 if and only if there exists a quadratic form $Q \in \mathrm{Quad}(V^*)$ such that $Q(\pi_1) = \cdots = Q(\pi_n) = 0$ and $Q(\pi_0) \neq 0$, and all such quadratic forms are separating.

Next two propositions provide a characterization of the separating forms.

PROPOSITION 5.2.4. *No quadratic form of rank $r \leq 3$ is separating. All quadratic forms of rank $r \geq 5$ are separating.*

PROOF. Let Q be not separating, i.e. $Q = Q_{x,y,x',y'}$ for some $x, y, x', y' \in V$. Then the associated bilinear form $\tilde{B}_Q$ is given by $\tilde{B}_Q = x \otimes y + y \otimes x - x' \otimes y' - y' \otimes x'$ and its rank is at most 4. This directly implies that non-separating forms have rank at most 4, since in the case of characteristic 2, when the rank of $\tilde{B}_Q$ is exactly 4 it is easy to see that Q is identically zero on $\operatorname{Rad} V$. This proves the second claim of the theorem.

We prove the first statement for forms of rank $r = 3$, being the cases with $r \leq 2$ similar. Let $Q \in \operatorname{Quad}(V^*)$ be a quadratic form of rank 3. Clearly, we can assume that $k := \dim V = 3$.

Suppose first that $\operatorname{char} \mathbb{F} \neq 2$. By the classification of quadratic forms, there exists a basis $\{e_1, e_2, e_3\}$ of V such that, for some $\alpha \in \mathbb{F}^*$, the matrix associated to the symmetric bilinear form B_Q is

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

Therefore, Q is not separating because $B_Q = e_1 \otimes e_2 + e_2 \otimes e_1 + \alpha e_3 \otimes e_3$, and this implies that $Q = Q_{x,y,x',y'}$ with $x = 2e_1$, $y = e_2$, $x' = \alpha e_3$ and $y' = -e_3$.

Assume now that $\operatorname{char} \mathbb{F} = 2$. By the classification of quadratic forms, Q is determined by a bilinear form $T \in \operatorname{Bil}(V^*)$ such that its matrix in some suitable basis $\{e_1, e_2, e_3\}$ of V is

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

Then $T = T_{e_1,e_2,e_3,e_3}$, and hence Q is not separating. □

It remains to study what happens for quadratic forms of rank $r = 4$. Briefly, up to equivalence, there are two quadratic forms of rank 4, and only one of them is separating.

PROPOSITION 5.2.5. *If* $\operatorname{char} \mathbb{F} \neq 2$*, a quadratic form of rank* $r = 4$ *is separating if and only if its discriminant is* -1*. If* $\operatorname{char} \mathbb{F} = 2$*, a quadratic form of rank* $r = 4$ *is separating if and only if its Arf invariant is* 1*.*

PROOF. Let $Q \in \operatorname{Quad}(V^*)$ be a quadratic form of rank $r = 4$. As before, we can assume that $k = \dim V = 4$. Suppose that Q is not separating, that is, $Q = Q_{x,y,x',y'}$ for some x, y, x', y'.

Suppose that $\operatorname{char} \mathbb{F} \neq 2$. Then the symmetric bilinear form associated to Q is

$$B_Q = \frac{1}{2}(x \otimes y + y \otimes x) - \frac{1}{2}(x' \otimes y' + y' \otimes x').$$

If $\{x, y, x', y'\}$ is a linearly dependent set, then $\operatorname{rk} B_Q \leq 3$. Therefore, $\{x, y, x', y'\}$ is a basis of V. The determinant of the matrix of B_Q in this basis is equal to $(1/4)^2$, and hence the discriminant of Q is equal to 1.

If $\operatorname{char} \mathbb{F} = 2$, then $\widetilde{B}_Q = x \otimes y + y \otimes x + x' \otimes y' + y' \otimes x'$. Again, $\{x, y, x', y'\} = \{e_1, e_2, e_3, e_4\}$ is a basis of V. Let $\{\pi_1, \pi_2, \pi_3, \pi_4\}$ be the dual basis of V^*. The Arf invariant of Q is equal to 0 because $Q(\pi_i) = 0$ for $i = 1, \ldots, 4$ and hence $Q(\pi_1)Q(\pi_2) + Q(\pi_3)Q(\pi_4) = 0$. □

5.3 Finding "Exotic Schemes"

We apply here the results in Section 5.2 to find examples of linear secret sharing schemes that are M2 but not M1. Specifically, we prove Theorem 5.1.4 and we present some additional examples of interest.

Associated to a secret sharing scheme $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$, consider the subspace

$$W(\Sigma) = \langle \pi_i \otimes \pi_i : i = 1, \ldots, n \rangle \subseteq \operatorname{Sym}(V)$$

and its annihilator

$$I(\Sigma) = \{\phi \in \operatorname{Sym}(V)^* : \phi(B) = 0 \text{ for every } B \in W(\Sigma)\} \subseteq \operatorname{Sym}(V)^*.$$

Recall that Σ is M1 if and only if $\pi_0 \otimes \pi_0 \in W(\Sigma)$. By linear algebra, these subspaces satisfy

$$\dim W(\Sigma) + \dim I(\Sigma) = \dim \operatorname{Sym}(V) = \frac{k(k+1)}{2}.$$

If $W(\Sigma) = \operatorname{Sym}(V)$, then $\pi_0 \otimes \pi_0 \in W(\Sigma)$, and hence Σ is M1. In the case $\dim W(\Sigma) = \dim \operatorname{Sym}(V) - 1$, we obtain the following sufficient condition for a linear secret sharing scheme to be M2 but not M1.

PROPOSITION 5.3.1. *Suppose Σ satisfies the following conditions.*

(i) $\dim W(\Sigma) = \dim \operatorname{Sym}(V) - 1$.

(ii) There exists a separating quadratic form $Q \in \operatorname{Quad}(V^*)$ such that $Q(\pi_i) = 0$ for all $i = 1, \ldots, n$ while $Q(\pi_0) \neq 0$.

Then Σ has product reconstruction (is M2) but is not multiplicative (is not M1).

PROOF. Condition *(ii)* implies that Σ is not M1. The subspace $I(\Sigma) \subseteq \operatorname{Sym}(V)^*$ has dimension 1, so $I(\Sigma) = \langle Q \rangle$, where Q is the separating form in

Condition *(ii)*. Therefore, all non-zero elements in $I(\Sigma)$ are separating, which implies that Σ is M2 by Proposition 5.2.2. □

At this point, we can apply this sufficient condition to present the first example of a linear secret sharing scheme that is M2 but not M1. Take $q = 5$ and $V = \mathbb{F}_5^5$, and fix a basis of V. Consider the symmetric bilinear form $T \in \mathrm{Sym}(V^*)$ that is represented by the 5×5 identity matrix and the quadratic form Q that is determined by T. Obviously, $\operatorname{rk} Q = 5$, and hence Q is separating by Proposition 5.2.4. Our example is a linear secret sharing scheme Σ among $n = 14$ players such that $\dim W(\Sigma) = \dim \mathrm{Sym}(V) - 1 = 14$ and $I(\Sigma) = \langle Q \rangle$. That is, we have to find $\pi_0, \ldots, \pi_{14} \in V^*$ such that $\{\pi_i \otimes \pi_i : i = 1, \ldots, 14\}$ is linearly independent, $Q(\pi_i) = 0$ for all $i = 1, \ldots, 14$, and $Q(\pi_0) \neq 0$. Then Σ is M2 but not M1 by Proposition 5.3.1. A suitable choice for $(\pi_0, \ldots, \pi_{14})$ is given by the column vectors of the following matrix.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 1 & 1 & 0 & 0 & 3 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 1 & 0 & 0 & 3 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

It is easy to see that Σ achieves 2-privacy.

We use again Proposition 5.3.1 to present a similar example over $\mathbb{F}_2$. Take $V = \mathbb{F}_2^5$ and fix a basis for V. Consider the quadratic form $Q \in \mathrm{Quad}(V^*)$ defined by the bilinear form T with matrix

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

Observe that Q is separating because it has rank 5. Reasoning as in the previous example we obtain that the linear secret sharing scheme determined by the matrix

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

is M2 but not M1.

Similarly to the first one, the following example is again linear secret sharing scheme Σ with dimension $k = 5$ over $\mathbb{F}_5$, but in this case the number of players

is reduced to $n = 13$. This is achieved by taking $\dim I(\Sigma) = 2$. Consider the quadratic forms $Q_1, Q_2 \in \mathrm{Quad}(V^*)$ determined by the symmetric bilinear forms with matrices

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

respectively. One can check that all nonzero linear combinations of these two matrices have rank 5. As a consequence, all nonzero forms in $\langle Q_1, Q_2 \rangle$ have rank 5, and hence they are separating. Next, we present a linear secret sharing scheme Σ among 13 players such that it is not M1 and $I(\Sigma) = \langle Q_1, Q_2 \rangle$. Clearly, Σ is M2. A possible choice is given by the columns of the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 3 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 4 & 1 & 1 & 4 \\ 0 & 0 & 0 & 2 & 3 & 0 & 0 & 1 & 3 & 3 & 1 & 4 & 1 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 3 & 1 & 1 & 1 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 3 & 2 & 0 & 0 & 4 & 4 \end{pmatrix}.$$

There exist separating quadratic forms of rank 4, and they have been characterized in Proposition 5.2.5. Therefore, we can apply Proposition 5.3.1 to find examples with dimension $k = 4$ on $9 = k(k+1)/2 - 1$ players. In each of the three following examples, we consider $V = \mathbb{F}_q^4$, where the characteristic of the field is different from 2, and a quadratic form $Q \in \mathrm{Quad}(V^*)$ that is determined by a symmetric matrix

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix}.$$

Take $q = 3$ and $\alpha = -1$. As the determinant of D is not a square in $\mathbb{F}_3$, Q is separating. In addition, Q has at least 9 different zeros in $\mathbb{F}_3^4$, so we can construct a linear secret sharing scheme Σ among 9 players which is M2 but not M1. An example is

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 2 & 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

The previous example generalizes as follows. Take $\alpha = -1$ and a prime power q such that -1 is not a square in $\mathbb{F}_q$. As before, Q is separating. Observe that

$a^2 + b^2 \neq 0$ for every $a, b \in \mathbb{F}_q^*$ because -1 is not a square in $\mathbb{F}_q$. Therefore, there exist $a, b, c \in \mathbb{F}_q^*$ with $a^2 + b^2 + c^2 = 0$. The previous discussion implies that the matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & -1 & 0 & 0 & -a & a & a \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & b & -b & b \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & c & c & -c \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

defines a linear secret sharing scheme Σ among 9 players that is M2 but not M1.

We now consider the case of a field $\mathbb{F}_q$ with $\operatorname{char} \mathbb{F}_q \neq 2$ containing a square root i of -1. Let α be a non-square in $\mathbb{F}_q$, and assume further that $\alpha \neq i$. Note that this choice is always possible, replacing i with $-i$ if necessary. Again, Q is separating and we find another linear secret sharing scheme that is M2 but not M1.

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & \frac{\alpha+1}{2} & \frac{\alpha+1}{2} & 0 & \frac{\alpha+1}{2} \\ 0 & i & 0 & 1 & -i & 0 & \frac{i(\alpha-1)}{2} & 0 & \frac{\alpha+1}{2} & \frac{i(\alpha-1)}{2} \\ 0 & 0 & i & i & 0 & -i & 0 & \frac{i(\alpha-1)}{2} & \frac{i(\alpha-1)}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & i & i & i & -i \end{pmatrix}.$$

Finally, we present another example on 9 players, this time over fields of characteristic 2. Let $\mathbb{F}_q = \mathbb{F}_2[\alpha]$, with $\alpha \notin \mathbb{F}_2$, be an arbitrary field extension of $\mathbb{F}_2$, and assume $\operatorname{Tr}(\alpha) = 1$. Note that it is always possible to choose such an α. So the form

$$Q = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & \alpha \end{pmatrix}$$

is separating and yields the separating scheme

$$\Sigma = \begin{pmatrix} 1 & 1 & 0 & 1 & \alpha^{1/2} & \alpha^{1/2} & \alpha^{1/2} & 1 & \alpha^2 & 1 \\ 1 & 0 & 1 & 1 & \alpha^{1/2} & \alpha^{1/2} & 1 & \alpha^{1/2} & 1 & \alpha^2 \\ 1 & 0 & 0 & 1 & 0 & 1 & \alpha^{1/2} & \alpha^{1/2} & \alpha & \alpha \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Note that in the case of $\mathbb{F}_q = \mathbb{F}_2$ we have $\alpha = \alpha^2 = \alpha^{1/2} = 1$ and this construction gives a scheme that is M1.

5.4 Composition and Proof of the Main Result

We discuss here how to obtain larger examples from small ones by using the composition of secret sharing schemes defined in Section 2.6.1. Recall that this

operation consists in substituting a player by several players by distributing its share using another secret sharing scheme. By using this tool and the examples in Section 5.3, we present proofs for Main Theorem 5.1.3 and Theorem 5.1.6.

Let V' and V'' be $\mathbb{F}$-vector spaces. Let $\Sigma' = (\pi'_0, \ldots, \pi'_{n'}) \subseteq (V')^*$ and $\Sigma'' = (\pi''_0, \ldots, \pi''_{n''}) \subseteq (V'')^*$ be secret sharing schemes. Let $\Sigma = \Sigma'[\Sigma''] = (\pi_0, \ldots, \pi_n) \subseteq V^*$ be the composition of Σ' with Σ'', where the vector space V as well as the linear forms π_i are defined as in Section 2.6.1.

We investigate how the multiplicativity properties of Σ' and Σ'' are inherited by their composition. As to the M1 property, recall that we have proved in Proposition 2.6.10 that if $\Sigma = \Sigma'[\Sigma'']$ is multiplicative in the sense of Definition 2.6.5 and $\Sigma'_{\{1,\ldots,n'-1\}}$ is not, then both Σ' and Σ'' are multiplicative. As to the M2 property, the following holds.

PROPOSITION 5.4.1. *If both Σ' and Σ'' have product reconstruction, then the composition $\Sigma = \Sigma'[\Sigma'']$ has product reconstruction too.*

PROOF. Suppose that Σ is not M2 and Σ'' is M2, and let us prove that Σ' is not M2. By Proposition 5.2.2 there exists a non-separating quadratic form $Q \in \mathrm{Quad}(V^*)$ such that $Q(\pi_i) = 0$ for all $i = 1, \ldots, n$ and $Q(\pi_0) \neq 0$. Consider the quadratic forms $Q' \in \mathrm{Quad}((V')^*)$ and $Q'' \in \mathrm{Quad}((V'')^*)$ defined by

$$Q'(\pi') = Q\left(\overline{(\pi', 0)}\right) \quad \text{and} \quad Q''(\pi'') = Q\left(\overline{(0, \pi'')}\right).$$

Observe that both Q' and Q'' are non-separating. Since Σ'' is M2 and $Q''(\pi''_j) = 0$ for every $j = 1, \ldots, n''$, we have that $Q''(\pi''_0) = 0$, hence

$$Q'(\pi'_{n'}) = Q(\tau_0) = Q''(\pi''_0) = 0,$$

where $\tau_0 := \overline{(\pi'_{n'}, 0)} = \overline{(0, \pi''_0)} \in V^*$. Therefore, Σ' is not M2 because $Q' \in \mathrm{Quad}((V')^*)$ is a non-separating quadratic form such that $Q'(\pi'_i) = 0$ for all $i = 1, \ldots, n'$ and $Q'(\pi'_0) = Q(\pi_0) \neq 0$. □

By composing Shamir's threshold secret sharing scheme with the small examples in Section 5.3, linear secret sharing schemes that are M2 but not M1 are obtained for an arbitrarily large number of players. Indeed, for every integer $t \geq 1$ and every prime power $q \geq 2t + 1$, Shamir's scheme among $2t + 1$ players, with t-privacy and $(t + 1)$-reconstruction, provides a multiplicative (M1) $\mathbb{F}_q$-linear secret sharing scheme Σ' with the additional property that, for every proper subset $I \subsetneqq \{1, \ldots, 2t + 1\}$, Σ'_I is not multiplicative. If Σ'' is one of the examples over $\mathbb{F}_q$ on 9 players in Section 5.3, then by Propositions 2.6.10 and 5.4.1 the composition $\Sigma = \Sigma'[\Sigma'']$ is an $\mathbb{F}_q$-linear secret sharing scheme on $n = 2t + 9$ players with t-privacy that is M2 but not M1.

The same idea can be used to construct examples for the notion of strong multiplication. For every integer $t \geq 1$ and every prime power $q \geq 3t + 1$,

a t-strongly multiplicative $\mathbb{F}_q$-linear secret sharing scheme Σ' on $n' = 3t+1$ players is obtained from Shamir's threshold scheme. Consider, as before, a scheme Σ'' conveniently chosen among the examples in Section 5.3 and the composition $\Sigma = \Sigma'[\Sigma'']$. Then, Σ is an $\mathbb{F}_q$-linear secret sharing scheme on $n = 3t+9$ players with t-privacy such that the scheme Σ_I is M2 for every set $I \subseteq \{1,\ldots,n\}$ of $n-t$ players, but Σ_J is not M1 for some set $J \subseteq \{1,\ldots,n\}$ with $n-t$ players.

The previous constructions prove neither Theorem 5.1.3 nor Theorem 5.1.6, but the proofs for those results are derived in a very similar way.

The algebraic geometric constructions from [11, 15, 19] provide, for every finite field $\mathbb{F}_q$ and for infinitely many values of $n' \in \mathbb{N}$, multiplicative (M1) linear secret sharing schemes Σ' over $\mathbb{F}_q$ on n' players that have t-privacy with $t = \Omega(n')$. By removing some players, we can assume that there is a player p_0 such that $\Sigma'_{\{1,\ldots,n'-1\}}$ is not M1. Let Σ'' be one of the schemes over $\mathbb{F}_q$ on 9 (or 14 if $q=2$) players presented in Section 5.3. Then the composition $\Sigma = \Sigma'[\Sigma'']$ is an $\mathbb{F}_q$-linear secret sharing scheme on $n = n'+8$ (or $n = n'+13$ if $q=2$) players that has t-privacy with $t = \Omega(n)$. By Propositions 2.6.10 and 5.4.1, The scheme Σ is M2 but not M1. This concludes the proof of Main Theorem 5.1.3.

The constructions from [11, 15, 19] provide as well, for every finite field $\mathbb{F}_q$ and for infinitely many values of $n' \in \mathbb{N}$, t-strongly multiplicative linear secret sharing schemes over $\mathbb{F}_q$ with $t = \Omega(n')$. Therefore, Theorem 5.1.6 can be proved similarly to Main Theorem 5.1.3.

5.5 The Smallest Examples

We presented in Section 5.3 examples of linear secret sharing schemes of dimension $k=4$ on 9 players that are M2 but not M1. The aim of this section is to prove Theorem 5.1.5, which implies that $n=9$ is the minimum required number of players in order to have a separation between the two multiplicativity notions.

We begin with some technical lemmas. We notate $\mathcal{P} = \{1,\ldots,n\}$ for the set of players and $\mathcal{P}_0 = \{0,1,\ldots,n\}$. An access structure Γ is $\mathcal{Q}_2$ if the set of players is not covered by any two rejecting sets. It is well-known that the access structure of every multiplicative (M1) linear secret sharing scheme is $\mathcal{Q}_2$, and it is easy to prove that the same applies to the M2 property.

LEMMA 5.5.1. *If a linear secret sharing scheme is M2, then its access structure is $\mathcal{Q}_2$.*

PROOF. Suppose that I and J with $I \cup J = \mathcal{P}$ are rejecting sets for $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$. Then there exist $x, y \in V$ such that $\pi_0(x) = \pi_0(y) = 1$, while $\pi_i(x) = 0$ for every $i \in I$ and $\pi_j(y) = 0$ for every $j \in J$. By applying Proposition 5.2.2 to $x, y, x' = 0, y' = 0$, this implies that Σ is not M2. □

LEMMA 5.5.2. *Every 2-threshold linear secret sharing scheme among 3 players is M1.*

PROOF. Let $\Sigma = (\pi_0, \pi_1, \pi_2, \pi_3) \subseteq V^*$ be a 2-threshold linear secret sharing scheme. Then we can assume that $\dim V = 2$. Moreover, $\{\pi_i, \pi_j\}$ is linearly independent for every two different $i, j \in \mathcal{P}_0$. Therefore, there exists a basis of V such that, for some $a, b \in \mathbb{F}^*$ with $a \neq b$, the linear forms $(\pi_0, \pi_1, \pi_2, \pi_3)$ are given by the columns of the matrix

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

It is easy to check that Σ is M1. □

Given $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$ and $I \subseteq \mathcal{P}$, the linear secret sharing scheme $\Sigma \setminus I$ is obtained from Σ by removing the players in I. This operation is called *puncturing*. For example, $\Sigma \setminus \{n\} = (\pi_0, \ldots, \pi_{n-1})$.

LEMMA 5.5.3. *Suppose that $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$ is M2. If there exists a partition $\mathcal{P}_0 = I_0 \cup I_1$ with $0 \in I_0$ and $I_1 \neq \emptyset$ such that the span of $\{\pi_i : i \in I_0\}$ has trivial intersection with the span of $\{\pi_j : j \in I_1\}$, then the scheme $\Sigma \setminus I_1$ is also M2.*

PROOF. Suppose that $\Sigma \setminus I_1$ is not M2. Then there exist $x, y, x', y' \in V$ such that $Q_{x,y,x',y'}(\pi_i) = 0$ for every $i \in I_0 \setminus \{0\}$ and $Q_{x,y,x',y'}(\pi_0) \neq 0$. It is not difficult to check that we can select $x, y, x', y' \in V$ in such a way that $Q_{x,y,x',y'}(\pi_j) = 0$ for every $j \in I_1$. This implies that Σ is not M2. □

Given a tuple of vectors $(\pi_0, \ldots, \pi_n) \subseteq V^*$, a set $B \subseteq \mathcal{P}_0$ is said to be a *basis* (or an *independent set*) if $\{\pi_i : i \in B\}$ is a basis of V^* (or, respectively, it is linearly independent). The following is a well-known result from linear algebra and also matroid theory.

LEMMA 5.5.4. *Let $B, B' \subseteq \mathcal{P}_0$ be two different bases. Then the following properties are satisfied.*

1. *If $i \in B' \setminus B$, then $(B' \setminus \{i\}) \cup \{j\}$ is a basis for some $j \in B \setminus B'$.*
2. *If $i \in B' \setminus B$, then $(B \setminus \{j\}) \cup \{i\}$ is a basis for some $j \in B \setminus B'$.*

We proceed now with the proof of Theorem 5.1.5. Let $\Sigma = (\pi_0, \ldots, \pi_n) \subseteq V^*$ be a linear secret sharing scheme over $\mathbb{F}$ on $n \leq 8$ players. Suppose that Σ is M2. We want to prove that Σ is also M1.

The access structure of Σ is denoted by Γ and $\min\Gamma$ denotes the family of the minimal accepting sets. Take $k = \dim V$. We can suppose that $V^* = \langle \pi_i : i = 1, \ldots, n \rangle$. If there exists an accepting set formed by a single player, then Σ is M1. From now on, we assume that all accepting sets have at least two players.

Claim 5.5.5. *$k < n$.*

Proof. Obviously, $k \leq n$. If $k = n$, there exists a basis $B \subseteq \mathcal{P}_0$ with $0 \in B$. Then $\mathcal{P} = (B \setminus \{0\}) \cup \{j\}$ because $|B| = n - 1$. Therefore, $\mathcal{P}$ is the union of two rejecting sets and Γ is not $\mathcal{Q}_2$, a contradiction. □

We prove in Claim 5.5.7 that Σ is M1 if $k \leq 4$. We need the following lemma.

Lemma 5.5.6. *Assume $\dim V = 4$ and let $\{\pi_1, \ldots, \pi_4\}$ be an $\mathbb{F}$-basis of V^*. Let $Q_1, Q_2 \in \mathrm{Quad}(V^*)$ be linearly independent and such that $Q_j(\pi_i) = 0$ for all $i = 1, \ldots, 4$ and $j = 1, 2$. Then there exists $\lambda \in \mathbb{F}$ such that $Q_1 + \lambda Q_2$ is not separating.*

Proof. Let $U_1, U_2 \in \mathbb{F}^{4\times 4}$ be the unique upper-triangular matrices associated to Q_1 and Q_2, respectively, in the basis $\{\pi_1, \ldots, \pi_4\}$ of V^*. Then

$$U_1 = \left(\begin{array}{cc|cc} 0 & \alpha_1 & \multicolumn{2}{c}{\multirow{2}{*}{A_1}} \\ 0 & 0 & & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{0}} & 0 & \beta_1 \\ \multicolumn{2}{c|}{} & 0 & 0 \end{array}\right), \qquad U_2 = \left(\begin{array}{cc|cc} 0 & \alpha_2 & \multicolumn{2}{c}{\multirow{2}{*}{A_2}} \\ 0 & 0 & & \\ \hline \multicolumn{2}{c|}{\multirow{2}{*}{0}} & 0 & \beta_2 \\ \multicolumn{2}{c|}{} & 0 & 0 \end{array}\right)$$

for some $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}, A_1, A_2 \in \mathbb{F}^{2\times 2}$. Reordering the basis, we may assume that $\alpha_2 \neq 0$. Take $\lambda = -\alpha_1/\alpha_2$. Then the matrix $U_3 = U_1 + \lambda U_2$ has rank at most 2, hence the bilinear form whose associated matrix is U_3 is of the form $x \otimes y - x' \otimes y'$ for some $x, y, x', y' \in \mathbb{F}^4$ and therefore $Q_1 + \lambda Q_2$ is not separating. □

Claim 5.5.7. *If $k \leq 4$, then Σ is M1.*

Proof. By Proposition 5.2.4, Σ is M1 if $k \leq 3$. Suppose that $k = 4$. Since $\dim \mathrm{Sym}(V) = 10$, we have that $\dim I(\Sigma) \geq 2$. By iterated application of Lemma 5.5.6, we can replace all separating forms in a basis of $I(\Sigma)$ with non-separating forms, obtaining a basis $\{Q_1, \ldots, Q_r\}$ of $I(\Sigma)$ consisting entirely of non-separating forms. Since Σ is M2, $Q_j(\pi_0) = 0$ for all $j = 1, \ldots, r$, and hence $\pi_0 \in W(\Sigma)$. Therefore, Σ is M1. □

From now on, we suppose that $5 \leq k \leq n-1$, and hence $6 \leq n \leq 8$. Take a set $B \subseteq \mathcal{P}_0$ such that $0 \in B$ and B is a basis (such a set always exists). Then $X = B \setminus \{0\} \notin \Gamma$, and hence $Y = \mathcal{P} \setminus X \in \Gamma$ because Γ is $\mathcal{Q}_2$. In addition, $|Y| = n - k + 1$.

CLAIM 5.5.8. *If Y is a minimal accepting set, then Σ is M1.*

PROOF. If Y is a minimal accepting subset, then Y is independent. Since π_0 is in the span of $\{\pi_j\}_{j \in Y}$, there exists $X_1 \subseteq X$ such that $B' = X_1 \cup Y$ is a basis. By Lemma 5.5.4, for every $i \in X \setminus X_1 \subseteq B \setminus B'$, there exists $j \in B' \setminus B = Y$ such that $B_i'' = (B \setminus \{i\}) \cup \{j\}$ is a basis. This implies that $B_i'' \setminus \{0\} = (X \setminus \{i\}) \cup \{j\}$ is not in Γ, and hence its complement $(Y \setminus \{j\}) \cup \{i\}$ is accepting. Then π_i is in the span of $\{\pi_\ell : \ell \in (Y \setminus \{j\}) \cup \{0\}\}$ because $Y \setminus \{j\} \notin \Gamma$, and hence π_i is in the span of $\{\pi_\ell\}_{\ell \in Y}$. Therefore, every vector π_i with $i \in \mathcal{P}_0 \setminus X_1$ is in the span of $\{\pi_\ell\}_{\ell \in Y}$. Take $X_0 = \mathcal{P}_0 \setminus X_1$. Since $X_1 \cup Y$ is a basis, the span of $\{\pi_i\}_{i \in X_0}$ has trivial intersection with the span of $\{\pi_j\}_{j \in X_1}$. Therefore, $\Sigma' = \Sigma \setminus \{X_1\}$ is M2 by Lemma 5.5.3. The dimension of Σ' is $k - |X_1| = n - k + 1 \leq 4$. Then Σ' is M1 by Claim 5.5.7, and hence so is Σ. □

CLAIM 5.5.9. *If $k = n - 1$, then Σ is M1.*

PROOF. Since $|Y| = n - k + 1 = 2$, we have that Y is a minimal accepting set. Apply Claim 5.5.8. □

As a consequence, Σ is M1 if $n = 6$. From now on, we assume that $7 \leq n \leq 8$ and $5 \leq k \leq n - 2$.

CLAIM 5.5.10. *If every pair $\{i, j\} \subseteq \mathcal{P}_0$ with $i \neq j$ is independent and $k = n-2$, then Σ is M1.*

PROOF. Without loss of generality, we can suppose that $B = \{0, 4, \ldots, n\}$ and $Y = \{1, 2, 3\}$. If Y is a minimal accepting set, then Σ is M1 by Claim 5.5.8. Otherwise, we can assume that $\{1, 2\} \in \min \Gamma$. If π_3 is in the span of $\{\pi_1, \pi_2\}$, then $\Sigma' = \Sigma \setminus (\mathcal{P} \setminus Y)$ is a $(2, 3)$-threshold scheme and Σ' is M1 by Lemma 5.5.2. This implies that Σ is M1. Otherwise, we can assume that $\{1, 2, 3, \ldots, n-2\}$ is a basis. Since π_0 is a linear combination of $\{\pi_1, \pi_2\}$, then $\{0, 2, 3, \ldots, n-2\}$ is a basis, and hence $\{1, n-1, n\} \in \Gamma$. If this is a minimal accepting set, then Σ is M1 by Claim 5.5.8. Since $B = \{0, 4, \ldots, n\}$ is a basis, $\{n-1, n\} \notin \Gamma$. Without loss of generality, we can assume that $\{1, n\} \in \Gamma$. Then $\Sigma \setminus (\mathcal{P} \setminus \{1, 2, n\})$ is a $(2, 3)$-threshold scheme, and hence Σ is M1. □

CLAIM 5.5.11. *If $k = n - 2$, then Σ is M1.*

PROOF. Suppose $n = 7$ and $k = 5$. If the pair $\{\pi_i, \pi_j\}$ is linearly dependent, then by removing (puncturing) one of these players an M2 LSSS on 6 players is obtained, which is also M1. Otherwise, Σ is M1 by Claim 5.5.10. The proof is analogous for the case $n = 8$ and $k = 6$. □

At this point, only the case $n = 8$, $k = 5$ remains unproven. Since every M2 linear secret sharing scheme on 7 players is M1, we can suppose that every pair $\{i, j\} \subseteq \mathcal{P}_0$ with $i \neq j$ is independent.

CLAIM 5.5.12. *Consider $Z \subseteq \mathcal{P}_0$ with $3 \leq |Z| \leq 4$ and $0 \in Z$. Let W be the span of $\{\pi_j\}_{j \in Z}$ and take $C = \{i \in \mathcal{P}_0 : \pi_i \in W\}$. If $|C| \geq |Z| + 3$, then Σ is M1.*

PROOF. Take $Z' \subseteq Z$ such that $\{\pi_j\}_{j \in Z'}$ is a basis of W. Take $A = \mathcal{P}_0 \backslash C \subseteq P$. By a simple case analysis, it is not difficult to check that there exist disjoint sets $A_1, A_2 \subseteq A$ such that $A_1 \cup A_2 = A$ and $\{\pi_j\}_{j \in Z' \cup A_i}$ is linearly independent for $i = 1, 2$.

Suppose that Σ is not M1. Then $\Sigma' = \Sigma \setminus A$ is not M1 and, since its dimension is $|Z'| \leq 4$, it is not M2. Then there exists a quadratic form $Q = Q_{x,y,x',y'} \in \text{Quad}(V^*)$ such that $Q(\pi_0) \neq 0$ while $Q(\pi_i) = 0$ for every $i \in C \setminus \{p_0\}$. Moreover, by basic linear algebra there exist vectors $u, v, u', v' \in V$ such that

- $\pi(u) = \pi(x)$, $\pi(v) = \pi(y)$, $\pi(u') = \pi(x')$, and $\pi(v') = \pi(y')$ for all $\pi \in W$, and
- $\pi_i(u) = \pi_i(u') = 0$ for every $i \in A_1$, and
- $\pi_j(v) = \pi_j(v') = 0$. for every $j \in A_2$.

Consider the quadratic form $Q' = Q_{u,v,u',v'}$. Observe that $Q'(\pi_i) = Q(\pi_i)$ if $i \in C$ and $Q'(\pi_j) = 0$ if $j \notin C$. This implies that Σ is not M2, a contradiction. □

Without loss of generality $B = \{0, 5, 6, 7, 8\}$ is a basis. Let $Y = \{1, 2, 3, 4\}$. Remember that Y is an accepting set. If Y is a minimal accepting set, then Σ is M1 by Claim 5.5.8. Otherwise, we distinguish two cases

Case 1 $\{1, 2, 3\}$ *is a minimal accepting set.* We consider two subcases, depending on whether π_4 is in the span of $\{\pi_1, \pi_2, \pi_3\}$ or not. If yes, we can assume that $\{1, 2, 3, 5, 6\}$ is a basis. Then every set of the form $\{0, x, y, 5, 6\}$ with $x, y \in \{1, 2, 3\}$ and $x \neq y$ is a basis, and hence every set of the form $\{i, 4, 7, 8\}$ with $i \in \{1, 2, 3\}$ is accepting. If one of them is a minimal accepting set, then Σ is M1 by Claim 5.5.8. Observe that $\{7, 8\} \notin \Gamma$ because $\{7, 8\} \subseteq B$.

If $\{i, 4, j\} \in \Gamma$ for some $i \in \{1, 2, 3\}$ and $j \in \{7, 8\}$ such that $\{i, 4\} \notin \Gamma$, then π_j is in the span of $\{\pi_0, \pi_i, \pi_4\}$ and Σ is M1 by Claim 5.5.12 with $Z = \{0, 1, 2\}$ (since π_3,π_4,π_j are in the span of $\{\pi_0, \pi_1, \pi_2\}$). If a set of the form $\{i, 7, 8\}$ with $i \in \{1, 2, 3, 4\}$ is accepting, then π_8 is in the span of $\{\pi_0, \pi_i, \pi_7\}$, and hence the dimension of the span of $\{\pi_0, \pi_1, \pi_2, \pi_3, \pi_4, \pi_7, \pi_8\}$ is at most 4. Again, Σ is M1 by Claim 5.5.12. Suppose now that π_4 is not in the span of $\{\pi_1, \pi_2, \pi_3\}$. Then we can assume that $\{1, 2, 3, 4, 5\}$ is a basis. By using a similar argument as before, every set of the form $\{i, 6, 7, 8\}$ with $i = 1, 2, 3$ is accepting. Since $\{6, 7, 8\}$ is not accepting, the vector π_i is in the span of $\{\pi_0, \pi_6, \pi_7, \pi_8\}$ for every $i = 1, 2, 3$. Apply Claim 5.5.12 with $Z = \{0, 6, 7, 8\}$.

Case 2 *All minimal accepting subsets of Y have exactly 2 players.* We can assume that $\{1, 2\} \in \Gamma$. By Lemma 5.5.2, we can assume that $\{\pi_1, \pi_2, \pi_3\}$ is linearly independent. Suppose that π_4 is in the span of $\{\pi_1, \pi_2, \pi_3\}$ and that $\{1, 2, 3, 5, 6\}$ is a basis. Then $B' = \{p_0, 2, 3, 5, 6\}$ is a basis and $Y' = \{1, 4, 7, 8\} \in \Gamma$. If Y' is a minimal accepting set or $\{1, 4\} \in \Gamma$, then Σ is M1. If there is a minimal accepting subset of Y' with cardinality 3, then we can reduce to Case 1. Since $\{7, 8\} \subseteq B$, this set is not accepting. The only remaining case is that there exists an accepting set $\{i, j\}$ with $i \in \{1, 4\}$ and $j \in \{7, 8\}$. Then π_j is in the span of $\{\pi_1, \pi_2, \pi_3\}$ and Σ is M1 by Claim 5.5.12. Suppose now that π_4 is not in the span of $\{\pi_1, \pi_2, \pi_3\}$. Then we can assume that $\{1, 2, 3, 4, 5\}$ is a basis. Then $B' = \{p_0, 2, 3, 4, 5\}$ is a basis and $Y' = \{1, 6, 7, 8\} \in \Gamma$. The proof is concluded by using a similar argument as before.