On secret sharing with nonlinear product reconstruction

Ignacio Cascudo* Ronald Cramer† Diego Mirandola‡ Carles Padró §
Chaoping Xing¶

Abstract

Multiplicative linear secret sharing is a fundamental notion in the area of secure multi-party computation (MPC) and, since recently, in the area of two-party cryptography as well. In a nutshell, this notion guarantees that "the product of two secrets is obtained as a linear function of the vector consisting of the coordinate-wise product of two respective share-vectors". This paper 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 this product is obtained by *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*. Concretely, fix a finite field $\mathbb{F}_q$ as the base field over which linear secret sharing is considered. Then we show there exists an (exotic) linear secret sharing scheme with an unbounded number of players n such that it has t-privacy with $t = \Omega(n)$ and such that it does admit a product reconstruction function, yet this function is *necessarily* nonlinear. In addition, we determine the minimum number of players for which those exotic schemes exist. Our proof is based on combinatorial arguments involving quadratic forms. It extends to similar separation results for important variations, such as strongly multiplicative secret sharing.
Keywords: (arithmetic) secret sharing.

1 Introduction

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 [12].

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

*Aarhus University, Denmark. Email: ignacio@cs.au.dk. Ignacio Cascudo acknowledges support from the Danish National Research Foundation and The National Science Foundation of China (under the grant 61361136003) for the Sino-Danish Center for the Theory of Interactive Computation and from the Center for Research in Foundations of Electronic Markets (CFEM), supported by the Danish Strategic Research Council. Part of this research was done while he was at CWI Amsterdam, supported by Cramer's NWO VICI Grant.

†CWI Amsterdam & Mathematical Institute, Leiden University, The Netherlands. Email: cramer@cwi.nl, cramer@math.leidenuniv.nl.

‡CWI Amsterdam, The Netherlands, and Institut de Mathématiques de Bordeaux, UMR 5251, Université de Bordeaux, France. Email: diego@cwi.nl.

§Universitat Politècnica de Catalunya, Barcelona, Spain. Email: cpadro@ma4.upc.edu. This research work was done while this author was with Division of Mathematical Sciences, Nanyang Technological University, Singapore

¶Division of Mathematical Sciences, Nanyang Technological University, Singapore. Email: xingcp@ntu.edu.sg. This author's work was supported by the Singapore Ministry of Education through the Tier 1 Program under Grant RG20/13

property that "the product of two secrets is obtained as a linear function of the vector consisting of the coordinate-wise 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 [8] 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 [2, 5, 11]) in the context of application of Shamir's secret sharing scheme [16] to (information-theoretically) secure multi-party computation. The *asymptotical* (constant-rate) theory of strongly multiplicative schemes has been initiated in [6], using algebraic geometry. [2] It has found several notable applications, starting with [12]. For a full discussion and references, please refer to [4].

This paper 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*. Concretely, fix a finite field $\mathbb{F}_q$ as the base field $\mathbb{F}_q$ over which linear secret sharing is considered. Then we show there exists an (exotic) linear secret sharing scheme with an unbounded number of players n such that it has t-privacy with $t = \Omega(n)$ and such that it does admit a product reconstruction function, yet this function is *necessarily* nonlinear.

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 nonlinear product reconstruction on a small number of players. Our main result is then obtained by composing those small examples with multiplicative linear secret sharing schemes on an arbitrary number of players n that have t-privacy with $t = \Omega(n)$. The existence of such schemes over any fixed base field $\mathbb{F}_q$ was proved in [3, 7]. As an additional result, we determine the minimum number of players for which such exotic schemes exist. Our results extend to similar separation results for important variations, such as strongly multiplicative secret sharing.

It is an interesting question whether there are applications of this "exotic", novel class of secret sharing schemes with nonlinear product reconstruction [3] to cryptographic protocols, but we will not offer any speculations here.

We remark that, while the notion of multiplicativity defined in [8] applies to linear secret sharing schemes where each share may consist of an arbitrary number of elements of the field $\mathbb{F}_q$, in this work our definitions and results concern only *ideal* linear secret sharing schemes, i.e., those where each share is a *single* element of the field $\mathbb{F}_q$. This is the notion considered in e.g. [3, 6, 7]. 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

[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.

[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.

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

(maybe except for fields of characteristic 2). [4]

This paper is organized as follows. In Section 2, we recall some elementary theory of bilinear and quadratic forms over finite fields. In Section 3, we review the standard definition of multiplicative linear secret sharing in Definition 3.1. In Section 4, we formally define our relaxation of multiplicative linear secret sharing in Definition 4.1 and state in Main Theorem 4.3 our main separation result, i.e., the existence of "exotic schemes" with an unbounded number of players n and t-privacy with $t = \Omega(n)$.

In Section 5 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 5.1 and 5.2). This leads us to defining the "separating quadratic forms", which are characterized in Propositions 5.3 and 5.4 by using the classification of quadratic forms over finite fields.

By using those results, several examples of linear secret sharing schemes that prove the separation between the two notions are presented in Section 6. Specifically, for every finite field $\mathbb{F}_q$, we present examples of $\mathbb{F}_q$-linear secret sharing schemes with nonlinear product reconstruction on n players, where $n = 9$ if $q \geq 3$ and $n = 14$ if $q = 2$.

In Section 7, we review a well known method of combining secret sharing schemes and we analyze the behavior of product reconstruction under this composition in Propositions 7.2 and 7.3. At this point, Main Theorem 4.3 is proved by composing the examples on a small number of players presented in Section 6 with multiplicative linear secret sharing schemes whose privacy is linear on the number of players. Moreover, this composition technique makes it possible to extend our results to strongly multiplicative secret sharing.

Finally, in Section 8, we prove that it is not possible to find examples separating the two notions on less than 9 players. Therefore, the examples presented in Section 6 are among the smallest ones.

2 Preliminaries

We fix notations for linear algebra and we recall some basic facts about bilinear and quadratic forms. Most of the material covered in this section (tensor products, bilinear and quadratic forms) can be found in algebra handbooks as [14]. More specific references concerning classification of quadratic forms will be given later.

Let $\mathbb{F}_q$ denote a finite field of cardinality $q = p^m$. The prime number p is the *characteristic* of $\mathbb{F}_q$ and is denoted by $\operatorname{char} \mathbb{F}_q$. Let V be an $\mathbb{F}_q$-vector space with $\dim V = k$. If $S \subset V$ is a non-empty set, then $\langle S \rangle$ denotes the *span* of S, that is, the $\mathbb{F}_q$-linear subspace of V generated by the elements of S. The $\mathbb{F}_q$-vector space V^* of the linear forms $V \to \mathbb{F}_q$ is called the *dual space* of V. If $\{e_1, \ldots, e_k\}$ is a basis of V, its *dual basis* is the basis $\{e^1, \ldots, e^k\}$ of V^* whose elements are determined by $e^i(e_j) = 1$ if $i = j$ and $e^i(e_j) = 0$ otherwise. For reference later on, we include the following trivial lemma.

LEMMA 2.1. *Let V be an $\mathbb{F}_q$-vector space, $W \subset V$ a vector subspace, and $x \in V$. Then $x \notin W$ if and only if there is a linear form $\alpha \in V^*$ such that $\alpha(x) \neq 0$ and $\alpha(y) = 0$ for every $y \in W$.*

A *bilinear form* on V is a map $B : V \times V \to \mathbb{F}_q$ such that, for all $x, y, z \in V$, $\lambda \in \mathbb{F}_q$, the following holds.

- $B(x + y, z) = B(x, z) + B(y, z)$.

[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.

- $B(x, y+z) = B(x,y) + B(x,z)$.
- $B(\lambda x, y) = B(x, \lambda y) = \lambda B(x,y)$.

The vector space formed by all bilinear forms on V is denoted by $\mathrm{Bil}(V)$. By the universal property of the tensor product, there exists an isomorphism $V^* \otimes V^* \cong \mathrm{Bil}(V)$ mapping $\alpha \otimes \beta \in V^* \otimes V^*$ into the bilinear form on V defined by $\alpha \otimes \beta(x,y) = \alpha(x)\beta(y)$ for all $x, y \in V$. By duality, there is an isomorphism $V \otimes V \cong \mathrm{Bil}(V^*)$ which maps $x \otimes y \in V \otimes V$ into $x \otimes y(\alpha, \beta) := \alpha(x)\beta(y)$. The bilinear forms $\alpha \otimes \beta$ span $\mathrm{Bil}(V)$. Moreover, if $\{e^i\}_{1 \le i \le k}$ is a basis of V^*, then $\{e^i \otimes e^j\}_{1 \le i,j \le k}$ is a basis of $\mathrm{Bil}(V)$, which has dimension k^2.

Moreover, there is an isomorphism $V \otimes V \cong \mathrm{Bil}(V)^*$ that maps $x \otimes y \in V \otimes V$ into the linear form on $\mathrm{Bil}(V)$ determined by $\alpha \otimes \beta \mapsto \alpha(x)\beta(y)$. Composition with the isomorphism $\mathrm{Bil}(V^*) \cong V \otimes V$ described above yields an isomorphism $\mathrm{Bil}(V^*) \cong \mathrm{Bil}(V)^*$ which maps $B \in \mathrm{Bil}(V^*)$ into the linear form determined by $\alpha \otimes \beta \mapsto B(\alpha, \beta)$.

The matrix M of a bilinear form B on V with respect to a basis $\{e_i\}_{1 \le i \le k}$ of V is $M = (B(e_i, e_j))_{1 \le i,j \le k}$. For a bilinear form B on V, consider the linear maps $B_1 : V \to V^*$ and $B_2 : V \to V^*$, where, for every $x \in V$, the linear forms $B_1(x)$ and $B_2(x)$ are defined by $B_1(x)(y) = B(x,y)$ and $B_2(x)(y) = B(y,x)$, respectively. The linear maps B_1 and B_2 have the same rank, which is equal to the rank of any matrix associated to B. This value is called the *rank* of the bilinear form B and is denoted by $\operatorname{rk} B$. A proof for the following lemma can be found in [1, II, §7, no. 8].

LEMMA 2.2. *The rank of a bilinear form $B \in \mathrm{Bil}(V)$ equals the minimum integer $\ell_0 \ge 0$ such that there exist linear forms $\alpha^1, \ldots, \alpha^{\ell_0}, \beta^1, \ldots, \beta^{\ell_0} \in V^*$ with $B = \sum_{i=1}^{\ell_0} \alpha^i \otimes \beta^i$.*

The *transpose* of a bilinear form $B \in \mathrm{Bil}(V)$ is the bilinear form $B^t \in \mathrm{Bil}(V)$ defined by $B^t(x,y) = B(y,x)$ for all $x, y \in V$. A bilinear form $B \in \mathrm{Bil}(V)$ is *symmetric* if $B = B^t$, and it is *alternating* if $B(x,x) = 0$, for all $x \in V$. The $\mathbb{F}_q$-vector space consisting of all symmetric (respectively, alternating) bilinear forms on V is denoted by $\mathrm{Sym}(V)$ (respectively, $\mathrm{Alt}(V)$).

LEMMA 2.3. *For all $B \in \mathrm{Alt}(V)$, it holds that $B = -B^t$. If the characteristic is different from 2, the converse also holds.*

PROOF. For all $x, y \in V$, it holds that $B(x+y, x+y) = B(x,x) + B(x,y) + B(y,x) + B(y,y)$. Since $B(x,x) = B(y,y) = B(x+y, x+y) = 0$, it follows that $B(x,y) = -B(y,x)$. On the other hand, if $B = -B^t$, then $B(x,x) = -B(x,x)$ for all $x \in V$. This implies $B(x,x) = 0$ for all $x \in V$ if the characteristic is different from 2. △

LEMMA 2.4. *If the characteristic is different from 2, then $\mathrm{Bil}(V)$ is the direct sum of $\mathrm{Sym}(V)$ and $\mathrm{Alt}(V)$.*

PROOF. If the characteristic is different from 2, then $\mathrm{Sym}(V) \cap \mathrm{Alt}(V) = \{0\}$ by Lemma 2.3. In addition, for every $B \in \mathrm{Bil}(V)$,

$$B = \frac{B + B^t}{2} + \frac{B - B^t}{2}.$$

The first and the second terms on the right-hand side are, respectively, in $\mathrm{Sym}(V)$ and $\mathrm{Alt}(V)$. △

In some of our proofs in Section 5 we will consider elements in $\mathrm{Bil}(V)$ of the form $\pi \otimes \pi$ for some $\pi \in V^*$. These elements span the vector space $\mathrm{Sym}(V)$ of the symmetric bilinear forms on V. Indeed, if $\{e^1, \ldots, e^k\}$ is a basis of V^*, then the terms $e^i \otimes e^i$ with $1 \le i \le k$ and $(e^i + e^j) \otimes (e^i + e^j)$ with $1 \le i < j \le k$ constitute a basis of $\mathrm{Sym}(V)$. In particular, the dimension of $\mathrm{Sym}(V)$ is $k(k+1)/2$.

A *quadratic* form on V is a map $Q \colon V \to \mathbb{F}_q$ such that

- $Q(\lambda x) = \lambda^2 Q(x)$ for all $x \in V, \lambda \in \mathbb{F}_q$,
- the map $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form on V.

The $\mathbb{F}_q$-vector space of all quadratic forms on V is denoted by $\mathrm{Quad}(V)$.

Every bilinear form $B \in \mathrm{Bil}(V)$ defines a quadratic form $Q_B : V \to \mathbb{F}_q$ on V by taking $Q_B(x) = B(x, x)$ for every $x \in V$. This induces an isomorphism $\mathrm{Bil}(V)/\mathrm{Alt}(V) \cong \mathrm{Quad}(V)$. By Lemma 2.4, if $\mathrm{char}\,\mathbb{F}_q \neq 2$ this induces an isomorphism $\mathrm{Sym}(V) \cong \mathrm{Quad}(V)$ as well.

LEMMA 2.5. *There exists an isomorphism* $\phi\colon \mathrm{Quad}(V^*) \to \mathrm{Sym}(V)^*$ *such that* $\phi(Q)(\alpha \otimes \alpha) = Q(\alpha)$ *for all* $Q \in \mathrm{Quad}(V^*)$ *and all* $\alpha \in V^*$.

PROOF. Recall that we have an isomorphism $\mathrm{Bil}(V^*) \cong \mathrm{Bil}(V)^*$ that maps $B \in \mathrm{Bil}(V^*)$ into the linear form determined by $\alpha \otimes \beta \mapsto B(\alpha, \beta)$. Composing it with the restriction map $\mathrm{Bil}(V)^* \to \mathrm{Sym}(V)^*$, we obtain a surjective linear map $\mathrm{Bil}(V^*) \to \mathrm{Sym}(V)^*$ whose kernel is $\mathrm{Alt}(V^*)$. Indeed, $B \in \mathrm{Bil}(V^*)$ is in the kernel if and only if $B(\alpha, \alpha) = 0$ for every $\alpha \in V^*$. This gives an isomorphism $\mathrm{Bil}(V^*)/\mathrm{Alt}(V^*) \cong \mathrm{Sym}(V)^*$, and the lemma follows composing it with the isomorphism $\mathrm{Quad}(V^*) \cong \mathrm{Bil}(V^*)/\mathrm{Alt}(V^*)$ considered above. △

We need to introduce some results about the classification of quadratic forms. Proofs for these results can be found in [13, 15] for fields of odd characteristic and in [9, 10] for the characteristic 2 case. Let Q_1, Q_2 be two quadratic forms on V. They are said to be *equivalent* if there exists an automorphism ψ of V such that $Q_1 = Q_2 \circ \psi$.

We associate to a quadratic form $Q \in \mathrm{Quad}(V)$ the symmetric bilinear form $\widetilde{B}_Q \in \mathrm{Sym}(V)$ defined by $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$. We define the *radical* $\mathrm{Rad}_Q V$ of V with respect to Q as the kernel of the linear map $(\widetilde{B}_Q)_1 : V \to V^*$, that is,

$$\mathrm{Rad}_Q V := \{x \in V : \widetilde{B}_Q(x, y) = 0 \text{ for all } y \in V\}.$$

First consider the case $\mathrm{char}\,\mathbb{F}_q \neq 2$. Then the map

$$Q \mapsto B_Q := \frac{1}{2}\widetilde{B}_Q$$

is an isomorphism between the vector spaces $\mathrm{Quad}(V)$ and $\mathrm{Sym}(V)$. Let Q_1, Q_2 be quadratic forms. Fix a basis of V and, for $i = 1, 2$, take the matrix M_i associated to B_{Q_i}. Then Q_1 and Q_2 are equivalent if and only if there exists an invertible matrix P such that $M_1 = PM_2P^t$. The *rank* of a quadratic form Q is defined as the rank of B_Q. If Q has full rank k, then the *discriminant* of Q is defined as the class in the group $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2 \cong \{1, -1\}$ of the determinant of any matrix associated to B_Q. If Q has rank $r < k$, then it induces a decomposition $V = \mathrm{Rad}_Q V \oplus V'$ such that V' has dimension r and the restriction Q' of Q to V' has full rank. In this case the discriminant of Q is defined to be the discriminant of Q'. It holds that two quadratic forms are equivalent if and only if they have the same rank and the same discriminant [13].

Consider now the case $\mathrm{char}\,\mathbb{F}_q = 2$. In this case, quadratic forms are classified by the rank and the *Arf invariant*. Let Q be a quadratic form on V. In the characteristic 2 case, the rank is defined as follows. Let r' be the codimension of $\mathrm{Rad}_Q V$, which is always even. If there exists $x \in \mathrm{Rad}_Q V$ such that $Q(x) \neq 0$ then we define the rank of Q to be $r' + 1$. In this case the Arf invariant is not defined, as the rank suffices to classify the forms: two quadratic forms having the same, odd rank are equivalent. Otherwise, i.e. if Q identically vanishes on $\mathrm{Rad}_Q V$, the rank of Q is defined to be r'. If Q has rank $r = k = 2$ and $\{v_1, v_2\}$ is any $\mathbb{F}_q$-basis of V then the Arf invariant of Q is defined to be the class of $Q(v_1)Q(v_2)/(\tilde{B}_Q(v_1, v_2))^2$ in $\mathbb{F}_q/L$, where $L = \{\lambda^2 + \lambda : \lambda \in \mathbb{F}_q\}$, the kernel of the trace

map $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_2$. Note that $\mathbb{F}_q/L \cong \mathbb{F}_2$. In general, if Q has even rank r then it induces a decomposition $V = \mathrm{Rad}_Q\, V \oplus \bigoplus_{i=1}^{r/2} V_i$. If, for $i = 1, \ldots, r/2$, we denote by Q_i the restriction of Q to V_i, then the Arf invariant of Q is defined to be the sum of the Arf invariants of the Q_i's. It holds that two quadratic forms having the same, even rank are equivalent if and only if they have the same Arf invariant.

3 Multiplicative Linear Secret Sharing

For the purposes of this paper, a *linear secret sharing scheme* Σ over $\mathbb{F}_q$ is a tuple $(n, V, (\pi_i)_{i=0}^n)$ in the following conditions.

- V is an $\mathbb{F}_q$-vector space of finite dimension.
- $\pi_0 \in V^* \setminus \{0\}$ and $\pi_1, \ldots, \pi_n \in V^*$.
- π_0 is in the span of $\{\pi_i\}_{i=1}^n$.

The set $\{1, \ldots, n\}$ is the *player set*. Let $A \subset \{1, \ldots, n\}$ be a non-empty set. If $\pi_0 \in \langle\{\pi_i\}_{i\in A}\rangle$, then A is *accepting*. Otherwise, A is *rejecting*.

Let $s \in \mathbb{F}_q$, the *secret*. Select $x \in V$ uniformly at random such that $\pi_0(x) = s$. This is possible since $\pi_0 \neq 0$. The elements $\pi_1(x), \ldots, \pi_n(x)$ are the *shares*. The *joint shares of A* corresponds to the vector $(\pi_i(x))_{i\in A} \in \mathbb{F}_q^{|A|}$.

If A is accepting, then there is an $\mathbb{F}_q$-linear form $\rho^A : \mathbb{F}_q^{|A|} \longrightarrow \mathbb{F}_q$, the *(linear) reconstruction function for A*, such that $\rho^A((\pi_i(x))_{i\in A}) = \pi_0(x) = s$, for all $x \in \mathbb{F}_q^k$. In other words, if A is accepting, the secret can be reconstructed (linearly) from the joint shares of A.

On the other hand, if A is non-empty and rejecting, then the random variable $(\pi_i(x))_{i\in A}$ does not depend on the choice of the secret s. To prove this claim, the key observation is that, by Lemma 2.1, $\pi_0 \notin \langle\{\pi_i\}_{i\in A}\rangle$ if and only if there exists $z \in V$ (where z may depend on A) such that $\pi_0(z) = 1$ and $\pi_i(z) = 0$ for all $i \in A$. Indeed, let $s' \in \mathbb{F}_q$ be an arbitrary secret and write $\lambda = s' - s$. Then choosing $x' \in V$ uniformly at random with $\pi_0(x') = s'$ is equivalent to choosing uniformly at random a vector of the form $x + \lambda z \in V$ with $\pi_0(x) = s$. It holds that $(\pi_i(x + \lambda z))_{i\in A} = (\pi_i(x) + \lambda\pi_i(z))_{i\in A} = (\pi_i(x))_{i\in A}$.

The *access structure* $\Gamma(\Sigma)$ of the scheme collects the accepting sets, whereas the *adversary structure* $\mathcal{A}(\Sigma)$ collects the rejecting sets. Let t, r be integers with $0 \leq t < r \leq n$. The scheme has *r-reconstruction* if $\Gamma(\Sigma)$ contains all subsets of $\{1, \ldots, n\}$ of cardinality at least r and it has *t-privacy* if $\mathcal{A}(\Sigma)$ contains all subsets of $\{1, \ldots, n\}$ of cardinality at most t. By definition, the scheme is n-reconstructing. Of course, it could be r-reconstructing as well, for some $r < n$. Note that the definition of linear secret sharing does not guarantee any privacy. Although any interesting schemes do in fact offer privacy, it is convenient not to include this as a requirement in the definition here.

Note that we will not consider any of the more general definitions of linear secret sharing from the literature in this paper, such as those allowing the secrets (and/or the shares) to be vectors rather than single field elements.

Definition 3.1 (Multiplicative linear secret sharing [8]). *Let $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ be an LSSS over $\mathbb{F}_q$. It is* multiplicative (M1) *if there is an $\mathbb{F}_q$-linear form $\rho : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ such that, for all $x, y \in V$,*

$$\rho(z_1, \ldots, z_n) = \pi_0(x) \cdot \pi_0(y),$$

where

$$(z_1, \ldots, z_n) = (\pi_1(x) \cdot \pi_1(y),\ \ldots\ , \pi_n(x) \cdot \pi_n(y)).$$

In other words, "the product of two secrets is obtained as a *linear* function of the vector consisting of the coordinate-wise product of two respective share-vectors". This is a special property that is not generally satisfied by linear secret sharing schemes. Please refer to [8, 7] for more information about constructions and bounds. The multiplicative property can be characterized in terms of the properties of the symmetric bilinear forms $\pi_i \otimes \pi_i$.

PROPOSITION 3.2. *A linear secret sharing scheme* $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ *is M1 if and only if* $\pi_0 \otimes \pi_0$ *is in the span of* $\{\pi_i \otimes \pi_i\}_{i=1}^n$.

PROOF. By Definition 3.1, Σ is M1 if and only if there exist $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q$ such that $\pi_0(x) \cdot \pi_0(y) = \sum_{i=1}^n \lambda_i \pi_i(x) \cdot \pi_i(y)$, for all $x, y \in V$. △

Given $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ and a set A of players and a set A of players, we notate Σ_A for the linear secret sharing scheme $\Sigma_A = (|A|, k, (\pi_i)_{i \in \{0\} \cup A})$, that is, the restriction of Σ to the players in A.

DEFINITION 3.3. *A linear secret sharing scheme* $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ *is said to be* t-strongly multiplicative *if* Σ *has* t*-privacy and, for every set* A *consisting of* $n - t$ *players,* Σ_A *is a multiplicative linear secret sharing scheme.*

4 Our Contributions

The focus in this paper is on the following theoretical question, which is novel to the best of our knowledge. Consider multiplicative linear secret sharing, where "the product of two secrets is obtained as a *linear* function of the vector consisting of the coordinate-wise product of two respective share-vectors". Suppose we abandon the linearity condition and instead make the relaxed requirement that this product is obtained by *some*, not-necessarily-linear 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*.

DEFINITION 4.1 (Relaxation of Multiplicative Secret Sharing). *Let* $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ *be an LSSS over* $\mathbb{F}_q$. *The scheme has* product reconstruction (M2) *if, for all* $x, x', y, y' \in V$ *with*

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

it holds that

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

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

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

for all $x, y \in V$. In particular, a multiplicative linear secret sharing scheme (see Definition 3.1) is one for which a *linear* product reconstruction function exists. Thus, the M1 condition implies the M2 condition. As a consequence of our results the converse does not hold.

REMARK 4.2. *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 coordinate-wise product of two corresponding share-vectors, it suffices to solve a system of quadratic equations.*

MAIN THEOREM 4.3. *Let $\mathbb{F}_q$ be the finite field of q elements. There exists a function $t_q(n) \in \Omega(n)$ such that for infinitely many values of $n \in \mathbb{N}$, there exists a linear secret sharing scheme $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ over $\mathbb{F}_q$ such that it has $t_q(n)$-privacy and such that it admits a product reconstruction function (M2). However, such function is necessarily not $\mathbb{F}_q$-linear. Therefore, it is not a multiplicative linear secret sharing scheme (i.e., not M1).*

We state next other results that are proved in this work. The following two theorems prove that, for every finite field $\mathbb{F}_q$ with $q \geq 3$, $n = 9$ 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 4.4. *For every finite field $\mathbb{F}_q$ with $q \geq 3$, 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.*

THEOREM 4.5. *Every M2 linear secret sharing scheme on at most 8 players is also M1.*

In addition, we extend our separation result to the notion of strong multiplication.

THEOREM 4.6. *Let $\mathbb{F}_q$ be the finite field of q elements. There exists a function $\hat{t}_q(n) \in \Omega(n)$ such that for an unbounded number $n \in \mathbb{N}$, there exists a linear secret sharing scheme $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ over $\mathbb{F}_q$ such that Σ has $\hat{t}_q(n)$-privacy and for each set A consisting of $n - \hat{t}_q(n)$ players, Σ_A admits a product reconstruction function (M2). However there exists a set A with $n - \hat{t}_q(n)$ players such that Σ_A is not M1. Therefore, Σ is not a $\hat{t}_q(n)$-strongly multiplicative linear secret sharing scheme.*

5 Separating Quadrating 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*. We provide a characterization for this class.

PROPOSITION 5.1 (Not-M1 Characterization). *Let $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ be an $\mathbb{F}_q$-linear secret sharing scheme. Then Σ 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 3.2, Lemma 2.1, and the isomorphism between $\mathrm{Sym}(V)^*$ and $\mathrm{Quad}(V^*)$ in Lemma 2.5. △

Given $x, y, x', y' \in V$, consider the bilinear form $T_{x,y,x',y'} = x \otimes y - x' \otimes y' \in \mathrm{Bil}(V^*)$ and its associated quadratic form $Q_{x,y,x',y'} \in \mathrm{Quad}(V^*)$. A quadratic form $Q \in \mathrm{Quad}(V^*)$ is called *separating* if $Q \neq Q_{x,y,x',y'}$ for every $x, y, x', y' \in V$.

PROPOSITION 5.2 (Not-M2 Characterization). *Let $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ be an $\mathbb{F}_q$-linear secret sharing scheme. Then Σ 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 4.1. △

As a consequence of the last two theorems, $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ is M2 but not M1 if and only 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 5.3. *No quadratic form of rank $r \leq 3$ is separating. All quadratic forms of rank $r \geq 5$ are separating.*

PROOF. If Q is not separating, then $Q = Q_{x,y,x',y'}$ for some $x, y, x', y' \in V$. Then the associated bilinear form $\tilde{B}_Q$ defined at the end of Section 2 is given by $\tilde{B}_Q = x \otimes y + y \otimes x - x' \otimes y' - y' \otimes x'$. By Lemma 2.2, this bilinear form has rank at most 4. This directly implies that non-separating forms have rank at most 4, since in the case $\operatorname{char} \mathbb{F}_q = 2$, when the rank of $\tilde{B}_Q$ is exactly 4 it is easy to see that Q is identically zero in $\operatorname{Rad}_Q V$. 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 $\operatorname{char} \mathbb{F}_q \neq 2$. By the classification of quadratic forms, there exists a basis $\{e_1, e_2, e_3\}$ of V such that, for some $\alpha \in \mathbb{F}_q^*$, 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 $\operatorname{char} \mathbb{F}_q = 2$. 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 5.4. *If* $\operatorname{char} \mathbb{F}_q \neq 2$, *a quadratic form of rank* $r = 4$ *is separating if and only if its discriminant is* -1. *If* $\operatorname{char} \mathbb{F}_q = 2$, *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 $\operatorname{char} \mathbb{F}_q \neq 2$. 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 $\operatorname{rk} B_Q \leq 3$ by Lemma 2.2. 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 $\operatorname{char} \mathbb{F}_q = 2$, then $\tilde{B}_Q = x \otimes y + y \otimes x + x' \otimes y' + y' \otimes x'$. Again, $\{x, y, x', y'\} = \{e_1, e_2, e_3, e_4\}$ is a basis of V. Let $\{e^1, e^2, e^3, e^4\}$ be the dual basis of V^*. The Arf invariant of Q is equal to 0 because $Q(e^i) = 0$ for $i = 1, \ldots, 4$ and hence $Q(e^1)Q(e^2) + Q(e^3)Q(e^4) = 0$. △

6 Finding "Exotic Schemes"

We apply here the results in Section 5 to find examples of linear secret sharing schemes that are M2 but not M1. Specifically, we prove Theorem 4.4 and we present some additional examples of interest.

Associated to an $\mathbb{F}_q$-linear secret sharing scheme $\Sigma = (n, V, (\pi_i)_{i=0}^n)$, consider the subspace

$$W(\Sigma) = \langle \{\pi_i \otimes \pi_i\}_{i=1,\dots,n} \rangle \subset \mathrm{Sym}(V)$$

and its annihilator

$$I(\Sigma) = \{\phi \in \mathrm{Sym}(V)^* \,:\, \phi(B) = 0 \text{ for every } B \in W(\Sigma)\} \subset \mathrm{Sym}(V)^* \cong \mathrm{Quad}(V^*).$$

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

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

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

Proposition 6.1 (Sufficient Separation Conditions). *Suppose Σ satisfies the following conditions.*

1. $\dim W(\Sigma) = \dim \mathrm{Sym}(V) - 1$.
2. *There is a separating quadratic form $Q \in \mathrm{Quad}(V^*)$ such that $Q(\pi_i) = 0$ for $i = 1, \dots, n$ while $Q(\pi_0) \neq 0$.*

Then Σ has product reconstruction (is M2) but Σ does not have linear product reconstruction (is not M1).

Proof. Condition 2 implies that Σ is not M1. The subspace $I(\Sigma) \subset \mathrm{Sym}(V)^*$ has dimension 1, so $I(\Sigma) = \langle Q \rangle$, where Q is the separating form in Condition 2. Therefore, all non-zero elements in $I(\Sigma)$ are separating, which implies that Σ is M2 by Proposition 5.2. $\triangle$

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, $\mathrm{rk}\, Q = 5$, and hence Q is separating by Proposition 5.3. Our example is a linear secret sharing scheme $\Sigma = (14, V, (\pi_i)_{i=0}^{14})$ such that $\dim W(\Sigma) = \dim \mathrm{Sym}(V) - 1 = 14$ and $I(\Sigma) = \langle Q \rangle$. That is, we have to find $\pi_0, \dots, \pi_{14} \in V^*$ such that $\{\pi_i \otimes \pi_i\}_{i=1}^{14}$ is linearly independent, $Q(\pi_i) = 0$ for $i = 1, \dots, 14$, and $Q(\pi_0) \neq 0$. Then Σ is M2 but not M1 by Proposition 6.1. A suitable choice for $(\pi_i)_{i=0}^{14}$ 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 6.1 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 $\Sigma = (13, \mathbb{F}_5^5, (\pi_i)_{i=0}^{13})$ 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 5.4. Therefore, we can apply Proposition 6.1 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 $\Sigma = (9, \mathbb{F}_3^4, (\pi_i)_{i=0}^{9})$ 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 $\Sigma = (9, \mathbb{F}_q^4, (\pi_i)_{i=0}^9)$ 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.

7 Composition and Proof of the Main Result

We discuss here how to obtain larger examples from small ones by using composition of LSSS. This is a known operation in secret sharing that consists in substituting a player by several players by distributing its share using another LSSS. By using this tool and the examples in Section 6, we present proofs for Main Theorem 4.3 and Theorem 4.6.

Let $\Sigma' = (n, V', (\pi'_i)_{i=0}^n)$ and $\Sigma'' = (m, V'', (\pi''_i)_{i=0}^m)$ be LSSS over $\mathbb{F}_q$. Consider the vector space

$$V = \{(x', x'') \in V' \times V'' : \pi'_n(x') = \pi''_0(x'')\} \subset V' \times V''.$$

Then $V^* = ((V')^* \times (V'')^*)/\langle(\pi'_n, -\pi''_0)\rangle$. Let $\overline{(\alpha, \beta)} \in V^*$ denote the class of the vector $(\alpha, \beta) \in (V')^* \times (V'')^*$. Consider the LSSS $\Sigma = (n + m - 1, V, (\pi_i)_{i=0}^{n+m-1})$, where

- $\pi_i = \overline{(\pi'_i, 0)}$ if $i = 0, \ldots, n-1$,

- $\pi_{n+j-1} = \overline{(0, \pi''_j)}$ if $j = 1, \ldots, m$.

The LSSS Σ is called the *composition* of Σ' with Σ'' and is denoted by $\Sigma = \Sigma'[\Sigma'']$. In this composition, the player n of the scheme Σ' has been substituted by the set of players of the scheme Σ''.

The player sets of Σ' and Σ'' can be identified, respectively, with $\{1, \ldots, n-1, p_0\}$ and $\{n, \ldots, n+m-1\}$. Here p_0 denotes the player of the scheme Σ' corresponding to the linear form π'_n. For a set $A \subset \{1, \ldots, n+m-1\}$, take $A' = A \cap \{1, \ldots, n-1\}$ and $A'' = A \cap \{n, \ldots, n+m-1\}$. Then A is accepting for $\Sigma = \Sigma'[\Sigma'']$ if and only if A' is accepting for Σ', or $A' \cup \{p_0\}$ is accepting for Σ' and A'' is accepting for Σ''. In particular, Σ has t-privacy if Σ' has t-privacy. Take $\beta_0 = \overline{(\pi'_n, 0)} = \overline{(0, \pi''_0)} \in V^*$.

LEMMA 7.1. *The following properties hold.*

1. $\langle \{\pi_i\}_{i=0}^{n-1} \rangle \cap \langle \{\pi_i\}_{i=n}^{n+m-1} \rangle \subset \langle \{\beta_0\} \rangle$.
2. $\langle \{\pi_i \otimes \pi_i\}_{i=0}^{n-1} \rangle \cap \langle \{\pi_i \otimes \pi_i\}_{i=n}^{n+m-1} \rangle \subset \langle \{\beta_0 \otimes \beta_0\} \rangle$.

PROOF. The first property is obvious, while the second one is a straightforward consequence of the first one. △

Consider the LSSS $\Sigma' \setminus \{p_0\} = (n-1, V, (\pi'_i)_{i=0}^{n-1})$, that is, the LSSS that is obtained by removing player p_0 from Σ'.

PROPOSITION 7.2. *Suppose that $\Sigma' \setminus \{p_0\}$ is not a multiplicative linear secret sharing scheme (M1). Then the composition $\Sigma = \Sigma'[\Sigma'']$ is a multiplicative linear secret sharing scheme if and only if Σ' and Σ'' are so.*

PROOF. Sufficiency is clear. To prove necessity, observe that

$$\langle \{\pi_i \otimes \pi_i\}_{i=0}^{n-1} \rangle \cap \langle \{\pi_i \otimes \pi_i\}_{i=n}^{n+m-1} \rangle = \langle \{\beta_0 \otimes \beta_0\} \rangle$$

if the composition $\Sigma = \Sigma'[\Sigma'']$ is a multiplicative linear secret sharing scheme △

PROPOSITION 7.3. *If both Σ' and Σ'' have product reconstruction (M2), then the composition $\Sigma = \Sigma'[\Sigma'']$ has product reconstruction too.*

PROOF. Suppose that Σ is not M2 and Σ'' is M2. Then there exists $T \in \mathrm{Bil}(V^*)$ with $\operatorname{rk} T \leq 2$ such that $T(\pi_i, \pi_i) = 0$ for $i = 1, \ldots, m+n-1$ and $T(\pi_0, \pi_0) = 1$. Consider the bilinear forms $T' \in \mathrm{Bil}((V')^*)$ and $T'' \in \mathrm{Bil}((V'')^*)$ defined by

$$T'(\alpha_1, \alpha_2) = T\left(\overline{(\alpha_1, 0)}, \overline{(\alpha_2, 0)}\right) \quad \text{and} \quad T''(\beta_1, \beta_2) = T\left(\overline{(0, \beta_1)}, \overline{(0, \beta_2)}\right).$$

Observe that $\operatorname{rk} T', \operatorname{rk} T'' \leq 2$. Since Σ'' is M2 and $T''(\pi''_j, \pi''_j) = 0$ for every $j = 1, \ldots, m$, we have that

$$0 = T''(\pi''_0, \pi''_0) = T(\beta_0, \beta_0) = T'(\pi'_n, \pi'_n).$$

Therefore, Σ' is not M2 because $T'(\pi'_0, \pi'_0) = T(\pi_0, \pi_0) = 1$ and $T'(\pi'_i, \pi'_i) = 0$ for every $i = 1, \ldots, n$. △

By composing Shamir's threshold secret sharing scheme [16] with the small examples in Section 6, linear secret sharing schemes that are M2 but not M1 are obtained for an arbitrarily large number of players. Indeed, for every $t \geq 1$ and for every prime power $q \geq 2t+1$, Shamir's $(t+1, 2t+1)$-threshold secret sharing scheme (or a variant of it if $q = 2t+1$), which has t-privacy and $(t+1)$-reconstruction, provides a multiplicative (M1) $\mathbb{F}_q$-linear secret sharing scheme Σ' on $n' = 2t+1$ players. Moreover, $\Sigma' \setminus \{p_0\}$ is not M1

for every player p_0. If Σ'' is one of the examples over $\mathbb{F}_q$ on 9 players in Section 6, then by Propositions 7.2 and 7.3 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 $t \geq 1$ and for 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 $(t + 1, 3t + 1)$-threshold scheme. Consider, as before, a scheme Σ'' conveniently chosen among the examples in Section 6 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_A is M2 for every set A of $n - t$ players, but Σ_A is not $M1$ for some set A with $n - t$ players.

The previous constructions prove neither Main Theorem 4.3 nor Theorem 4.6, but the proofs for those results are derived in a very similar way.

The algebraic geometric constructions from [3, 4, 6] 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 $\Sigma' \setminus \{p_0\}$ 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 6. 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 7.2 and 7.3, The scheme Σ is M2 but not M1. This concludes the proof of Main Theorem 4.3.

The constructions from [3, 4, 6] 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 4.6 can be proved similarly to Main Theorem 4.3.

8 The Smallest Examples

We presented in Section 6 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 4.5, 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 $\mathbf{P} = \{1, \ldots, n\}$ for the set of players and $\mathbf{Q} = \{0, 1, \ldots, n\}$. 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 8.1. *If a linear secret sharing scheme is M2, then its access structure is $\mathcal{Q}_2$.*

Proof. Suppose that A and B with $A \cup B = \mathbf{P}$ are rejecting sets for $\Sigma = (n, V, (\pi_i)_{i=0}^n)$. Then there exist $x, y \in V$ such that $\pi_0(x) = \pi_0(y) = 1$, while $\pi_i(x) = 0$ for every $i \in A$ and $\pi_j(y) = 0$ for every $j \in B$. By applying Theorem 5.2 to $x, y, x' = 0, y' = 0$, this implies that Σ is not M2. △

The accepting sets of the $(2, 3)$-*threshold access structure* are precisely those with at least two players.

Lemma 8.2. *Every linear secret sharing scheme for the $(2, 3)$-threshold access structure is M1.*

Proof. Let $\Sigma = (3, V, (\pi_i)_{i=0}^3)$ be an $\mathbb{F}_q$-linear secret sharing scheme with $(2, 3)$-threshold access structure. Then we can assume that $\dim V = 2$. Moreover, $\{\pi_i, \pi_j\}$ is linearly independent for every two different $i, j \in \mathbf{Q}$. Therefore, there exists a basis of V such that, for

some $a, b \in \mathbb{F}_q^*$ with $a \neq b$, the linear forms $(\pi_i)_{i=0}^3$ 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 $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ and $X \subset \mathbf{P}$, the linear secret sharing scheme $\Sigma \setminus X$ is obtained from Σ by removing the players in X. This operation is called *puncturing*. For example, $\Sigma \setminus \{n\} = (n-1, V, (\pi_i)_{i=0}^{n-1})$

LEMMA 8.3. *Suppose that $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ is M2. If there exists a partition $\mathbf{Q} = X_0 \cup X_1$ with $0 \in X_0$ and $X_1 \neq \emptyset$ such that the span of $\{\pi_i\}_{i \in X_0}$ has trivial intersection with the span of $\{\pi_j\}_{j \in X_1}$, then the scheme $\Sigma \setminus X_1$ is also M2.*

PROOF. Suppose that $\Sigma \setminus X_1$ is not M2. Then there exist $x, y, x', y' \in V$ such that $Q_{x,y,x',y'}(\pi_i) = 0$ for every $i \in X_0 \setminus \{0\}$ 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 $j \in X_1$. This implies that Σ is not M2. △

Given a tuple of vectors $(\pi_i)_{i \in \mathbf{Q}}$ with $\pi_i \in V^*$, a set $B \subset \mathbf{Q}$ 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 8.4. *Let $B, B' \subset \mathbf{Q}$ 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 4.5. Let $\Sigma = (n, V, (\pi_i)_{i=0}^n)$ be a linear secret sharing scheme over $\mathbb{F}_q$ 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 $V^* = \langle \pi_i \rangle_{i=1}^n$. 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 8.5. $k < n$.

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

We prove in Claim 8.7 that Σ is M1 if $k \leq 4$. We need the following lemma.

LEMMA 8.6. *Assume $\dim V = 4$ and let $\{\pi_1, \ldots, \pi_4\}$ be an $\mathbb{F}_q$-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 $\lambda \in \mathbb{F}_q$ such that $Q_1 + \lambda Q_2$ is not separating.*

PROOF. Let $U_1, U_2 \in \mathbb{F}_q^{4 \times 4}$ 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

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

for some $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}_q, A_1, A_2 \in \mathbb{F}_q^{2\times 2}$. 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. This implies, by Lemma 2.2, that the bilinear form whose associated matrix is U_3 is of the form $x \otimes y - x' \otimes y'$ for some $x, y, x', y' \in \mathbb{F}_q^4$ and therefore $Q_1 + \lambda Q_2$ is not separating. △

Claim 8.7. *If $k \leq 4$, then Σ is M1.*

Proof. By Proposition 5.3, 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 8.6, we can replace all separating forms in a basis of $I(\Sigma)$ with non-separating forms, obtaining a basis $(Q_j)_{j=1}^r$ 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 $B \subset \mathbf{Q}$ such that $0 \in B$ and B is a basis (such a set always exists). Then $X = B \setminus \{0\} \notin \Gamma$, and hence $Y = \mathbf{P} \setminus X \in \Gamma$ because Γ is $\mathcal{Q}_2$. In addition, $|Y| = n - k + 1$.

Claim 8.8. *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 $X_1 \subset X$ such that $B' = X_1 \cup Y$ is a basis. By Lemma 8.4, for every $i \in X \setminus X_1 \subset B \setminus B'$, 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 $i \in \mathbf{Q} \setminus X_1$ is in the span of $\{\pi_\ell\}_{\ell\in Y}$. Take $X_0 = \mathbf{Q} \setminus X_1$. 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 8.3. The dimension of Σ' is $k - |X_1| = n - k + 1 \leq 4$. Then Σ' is M1 by Claim 8.7, and hence so is Σ. △

Claim 8.9. *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 8.8. △

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 8.10. *If every pair $\{i, j\} \subset \mathbf{Q}$ 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 8.8. Otherwise, we can assume that $\{1, 2\} \in \min \Gamma$. If π_3 is in the span of $\{\pi_1, \pi_2\}$, then $\Sigma' = \Sigma \setminus (\mathbf{P} \setminus Y)$ is a $(2, 3)$-threshold scheme and Σ' is M1 by Lemma 8.2. 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 8.8. 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 $\Sigma \setminus (\mathbf{P} \setminus \{1, 2, n\})$ is a $(2, 3)$-threshold scheme, and hence Σ is M1. △

Claim 8.11. *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 8.10. The proof is analogous for the case $n = 8$ and $k = 6$. $\triangle$

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 $\{i, j\} \subset \mathbf{Q}$ with $i \neq j$ is independent.

CLAIM 8.12. *Consider $Z \subset \mathbf{Q}$ with $3 \leq |Z| \leq 4$ and $0 \in Z$. Let W be the span of $\{\pi_j\}_{j\in Z}$ and take $C = \{i \in \mathbf{Q} : \pi_i \in W\}$. If $|C| \geq |Z| + 3$, then Σ is M1.*

PROOF. Take $Z' \subset Z$ such that $\{\pi_j\}_{j\in Z'}$ is a basis of W. Take $A = \mathbf{Q} \setminus C \subset P$. By a simple case analysis, it is not difficult to check that there exist disjoint sets $A_1, A_2 \subset A$ 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 $Q = Q_{x,y,x',y'} \in \mathrm{Quad}(V^*)$ 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. $\triangle$

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 8.8. 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 8.8. Observe that $\{7, 8\} \notin \Gamma$ because $\{7, 8\} \subset B$. 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 8.12 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 8.12. 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 8.12 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 8.2, 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 $\{7, 8\} \subset B$, 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 8.12. 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.

References

[1] N. Bourbaki. *Algebra I.* Springer, 1989.

[2] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proc. of STOC 1988*, pp. 1–10. ACM Press, 1988.

[3] I. Cascudo, H. Chen, R. Cramer, C. Xing. Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over *Any* Fixed Finite Field. *Proc. of 29th Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 5677, pp. 466–486, August 2009.

[4] I. Cascudo, R. Cramer, C. Xing. The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing. *Proc. of 31st Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 6842, pp. 685–705, August 2011.

[5] D. Chaum, C. Crépeau, and I. Damgaard. Multi-party unconditionally secure protocols. *Proc. of STOC 1988*, pp. 11–19. ACM Press, 1988.

[6] H. Chen and R. Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computation over Small Fields. *Proc. of 26th Annual IACR CRYPTO*, Springer Verlag LNCS, vol. 4117, pp. 516-531, Santa Barbara, Ca., USA, August 2006.

[7] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, V. Vaikuntanathan. Secure Computation from Random Error Correcting Codes. *Proc. of 27th Annual IACR EUROCRYPT*, Barcelona, Spain, Springer Verlag LNCS, vol. 4515, pp. 291-310, 2007.

[8] R. Cramer, I. Damgaard, and U. Maurer. General secure multi-party computation from any linear secret sharing scheme. *Proceedings of 19th Annual IACR EUROCRYPT*, Brugge, Belgium, Springer Verlag LNCS, vol. 1807, pp. 316-334, May 2000.

[9] J. Dieudonné. *La Géométrie des Groupes Classiques*, 2nd edition. Springer-Verlag, 1963.

[10] R. H. Dye. On the Arf Invariant. *Journal of Algebra*, pp. 36-39, 1978.

[11] M. K. Franklin, M. Yung. Communication Complexity of Secure Computation (Extended Abstract). *Proc. of STOC 1992*, pp. 699-710

[12] Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai. Zero-knowledge from secure multiparty computation. *Proc. of 39th STOC*, San Diego, Ca., USA, pp. 21-30, 2007.

[13] T. Y. Lam. *Introduction to Quadratic Forms over Fields.* Graduate Studies in Mathematics 67, American Mathematical Society, 2005.

[14] S. Roman. *Advanced linear algebra*, 3rd edition. Springer, 2008.

[15] J. -P. Serre. *A Course in Arithmetic.* Graduate Texts in Mathematics 7, Springer, 1973.

[16] A. Shamir. How to share a secret. *Comm. of the ACM*, 22(11):612-613, 1979.