# Generation of algebras and versality of torsors

Uriya A. First

University of Haifa

MIT number theory seminar, April 2020

Joint work with Zinovy Reichstein (UBC)

# Our starting point

**Theorem (Primitive Element Theorem)**

Every finite separable field extension $K/k$ is generated by a single element.

**Theorem (Folklore)**

Every central simple algebra over a field is generated by 2 elements.

- An algebra $A$ over a field $k$ is *central simple* if $A$ is simple, $Z(A) = k$ and $\dim_k A < \infty$. Equivalently, $A \otimes_k \overline{k} \cong \mathrm{M}_{n\times n}(\overline{k})$.
- Examples: $\mathrm{M}_n(k)$, $k\langle i, j \mid i^2 = j^2 = -1,\ ij = -ji\rangle$ (quaternions).

**Trivial Theorem**

Every $n$-dimensional vector space over a field is generated by $n$ elements.

# Globalization I

## Trivial Theorem

Every $n$-dimensional vector space over a field is generated by $n$ elements.

Vector spaces globalize to locally free modules:

- A module $M$ over a ring $R$ is *locally free* of rank $n$ if there exists a faithfully flat $R$-ring $S$ with $M \otimes_R S \cong S^n$.

## Theorem (Forster, 1964)

Assume $R$ is a noetherian ring, and let $d = \dim R$.
Every locally free $R$-module of rank $n$ is generated by $n + d$ elements.

- Swan, 1962: Forester's bound is tight in general.
- Swan, 1967: Can take $d = \dim \operatorname{Max} R$.
- Improvements by Eizenbud–Evans (1973), Warfried (1980), Upadhyay–Kumar (2013), . . .

# Globalization II

**Theorem (Primitive Element Theorem)**

Every finite separable field extension $K/k$ is generated by a single element.

Separable field extensions globalize to finite étale algebras:

- An algebra $E$ over a ring $R$ is *finite étale* (of rank $n$) if there exists a faithfully flat $R$-ring $S$ with $E \otimes_R S \cong S^n$ as $S$-algebras.

**Theorem (F–Reichstein, 2017)**

Let $R$ be a noetherian ring with no finite images, and let $d = \dim \operatorname{Max} R$. Every finite étale $R$-algebra can be generated by $1 + d$ elements.

- $d = 0$: Every étale algebra over an *infinite* field is generated by a single element.
- The case of finite fields and $\mathbb{Z}$ was analyzed by Kravchenko–Mazur–Petrenko (2012). See also F–Salazar–Reichstein (2018).

# Globalization III

**Theorem (Folklore)**

Every central simple algebra over a field is generated by 2 elements.

Central simple algebras globalize to Azumaya algebras:

- An algebra $A$ over a ring $R$ is *Azumaya of degree $n$* if there exists a faithfully flat $R$-ring $S$ with $A \otimes_R S \cong \mathrm{M}_{n\times n}(S)$.

**Theorem (F–Reichstein, 2017)**

Let $R$ be a noetherian ring, and let $d = \dim \operatorname{Max} R$.
Every Azumaya $R$-algebra can be generated by $2 + d$ elements.

# The general case

**Theorem A (F–Reichstein, 2017)**

Let $R$ be a noetherian ring, and let $d = \dim \operatorname{Max} R$.
Let $A$ be a finite $R$-algebra.
Assume that for every $\mathfrak{m} \in \operatorname{Max} R$, the $k(\mathfrak{m})$-algebra $A \otimes_R k(\mathfrak{m})$ can be generated by $n$ elements.
Then $A$ can be generated by $n + d$ elements.

- $A$ does not have to be associative or unital.
- Forster's theorem is recovered by taking an $R$-module $M$ and regarding it as an $R$-algebra with zero multiplication.
- $A$ can even be a *multialgebra*, i.e., an $R$-module with a collection of $R$-multilinear maps $\{m_i : A^{r_i} \to A\}_{i \in I}$. For example,
  1. a binary product is a bilinear map $m : A^2 \to A$,
  2. a unity is a (0-multilinear) map $u : A^0 \to A$,
  3. an involution is a linear map $i : A \to A$, ...

# Forms of algebras

## Definition

Let $A$ be $R$-algebra, and let $S$ be an $R$-ring.
A **form** of $A$ over $S$ is an $S$-algebra $B$ for which there is a faithfully flat $S$-ring $S'$ such that $A \otimes_R S' \cong B \otimes_S S'$.

- Azumaya algebras of degree $n$ are $R$-forms of the $\mathbb{Z}$-algebra $\mathrm{M}_n(\mathbb{Z})$.
- Finite étale algebras of degree $n$ are $R$-forms of the $\mathbb{Z}$-algebra $\mathbb{Z}^n$.
- Octonion $R$-algebras are $R$-forms of the split octonion $\mathbb{Z}$-algebra $\mathbb{O}_{\mathbb{Z}}$.

## Corollary (F–Reichstein, 2017)

Let $k$ be an infinite field, and let $A$ be a finite-dimensional $k$-algebra which is $n$-generated. Let $R$ be a noetherian $k$-ring, and let $d = \dim \operatorname{Max} R$. Then every $R$-form of $A$ can be generated by $n + d$ elements.

**Is this tight?**

# Lower bounds: The finite étale case

**Theorem (Shukla–Williams, 2019 / Ojanguren, 2017)**

Let $d \geq 0$ and $n \geq 2$. There exist a smooth finite type $\mathbb{R}$-ring $R$ with $\dim R = d$ and a finite étale $R$-algebra $E$ of rank $n$ such that $E$ cannot be generated by fewer than $1 + d$ elements.

There is some sensitivity to the base field.

**Proposition (Shukla–Williams, 2019)**

Let $R$ be a *smooth* finite type ring over an algebraically closed field. Assume that $d := \dim R \geq 2$. Then every finite étale algebra of rank 2 can be generated by $d$ elements.

# Lower bounds: The Azumaya case

**Theorem (Williams, 2018)**

Let $d, n \in \mathbb{N}$. There exist a smooth finite type $\mathbb{C}$-ring $R$ with $\dim R = d$ and a degree-$n$ Azumaya $R$-algebra $A$ such that $A$ cannot be generated by fewer than $2 + \lfloor \frac{d}{2n-2} \rfloor$ elements.

$$2 + \lfloor \tfrac{d}{2n-2} \rfloor \ll 2 + d$$

**Theorem (Williams, 2018)**

Every *topological Azumaya algebra* of degree $n$ over a $D$-dimensional CW-complex can be generated by $2 + \lfloor \frac{D}{2n-2} \rfloor$ global sections.

- A topological Azumaya algebra over a topological space $X$ is a $\mathbb{C}$-algebra bundle over $X$ with fibers isomorphic to $\mathrm{Mat}_{n\times n}(\mathbb{C})$.
- Write $d = \frac{D}{2}$ for the complex dimension of $X$. Then William's upper bound becomes $2 + \lfloor \frac{d}{n-1} \rfloor$.

# What is new? A better upper bound

Henceforth:

- $k$ is an infinite field.
- $A$ is a finite-dimensional $k$-algebra, e.g., $k^n$ or $\mathrm{M}_{n\times n}(k)$.
- $Z_r$ is the $k$-variety of tuples $(a_1,\dots,a_r)\in A^r$ not generating $A$.

**Theorem B (F–Reichstein, 2020)**

Let $R$ be a finite type $k$-ring, and let $d=\dim R$.
Assume that $r\dim A-\dim Z_r>d$.
Then every $R$-form of $A$ can be generated by $r$ elements.

- For $A=k^n$, we have $\dim Z_r=(n-1)r$, so every finite étale $R$-algebra is generated by $d+1$ elements (same as Theorem A).
- For $A=\mathrm{M}_{n\times n}(k)$, we have $\dim Z_r=(n^2-n+1)r+(n-1)$, hence:

**Corollary**

Azumaya $R$-algebras of degree $n$ can be generated by $2+\lfloor\frac{d}{n-1}\rfloor$ elements.

# Bounds on number of generators for various algebras

Let $R$ denote a finite type $k$-algebra of dimension $d$.

| $A$ | $\dim Z_r$ | $R$-forms of $A$ are | no. of generators $\leq$ |
|---|---|---|---|
| $\mathrm{M}_{n\times n}(k)$ | $(n^2-n+1)r+(n-1)$ | Azumaya of deg. $n$ | $2+\lfloor\frac{d}{n-1}\rfloor$ |
| $k^n$ | $(n-1)r$ | étale of rank $n$ | $1+d$ |
| $(\mathrm{M}_{n\times n}(k),\mathrm{t})$ | $n\neq 4$: $(n^2-2n+3)r+(r-2)$<br>$n=4$: $12r+1$ | Azumaya of deg. $n$ with orth. invol. | $n\neq 4$: $1+\lfloor\frac{d+(n-2)}{2n-3}\rfloor$<br>$n=4$: $1+\lfloor\frac{d+1}{4}\rfloor$ |
| $(\mathrm{M}_{n\times n}(k),\mathrm{s})$<br>$n$ even | $n\geq 8$: $(n^2-2n+3)r+(r-1)$<br>$n=6$: $27r+6$<br>$n=4$: $12r+3$<br>$n=2$: $3r+1$ | Azumaya of deg. $n$ with symp. invol. | $n\geq 8$: $1+\lfloor\frac{d+(n-2)}{2n-3}\rfloor$<br>$n=6$: $1+\lfloor\frac{d+6}{9}\rfloor$<br>$n=4$: $1+\lfloor\frac{d+3}{4}\rfloor$<br>$n=2$: $2+d$ |
| octonion | $6r+5$ | octonion $R$-alg's | $3+\lfloor\frac{d+1}{2}\rfloor$ |
| Albert | $21r+O(1)$ | Albert $R$-alg's | $\frac{d}{6}+O(1)$ |

- Theorem A gives bounds of the form $d+O(1)$.
- The calculation of $\dim Z_r$ for $(\mathrm{M}_{n\times n}(k),\mathrm{t})$ and $(\mathrm{M}_{n\times n}(k),\mathrm{s})$ is due to Taeuk Nam, Cindy Tan and Ben Williams, 2019.
- Let $b$ denote the maximal dimension of a proper $\overline{k}$-subalgebra of $A\otimes_k\overline{k}$. Then, *under a mild assumption*, $\dim Z_r = br+O(1)$, and every $R$-form of $A$ is generated by $\frac{d}{\dim A-b}+O(1)$ elements.

# The dimension of $Z_r$ for $A = \mathrm{M}_n(k)$

## Lemma

Assume $A = \mathrm{M}_{n\times n}(k)$. Then $\dim Z_r = (n^2 - n + 1)r + (n-1)$.

**Proof.** By Theorem B, we reduce to proving $\dim Z_r = (n^2 - n + 1)r + (n-1)$. We may assume that $k = \overline{k}$. By Burnside's Theorem, $Z_r = X_1 \cup \cdots \cup X_{n-1}$ for

$$X_i = \{(a_1, \dots, a_r) \in A^r \mid a_1, \dots, a_r \text{ stabilize a common } i\text{-dimensional space}\}.$$

Consider $Y_i = \{(a_1, \dots, a_r, W) \mid a_i(W) \subseteq W\} \subseteq \mathrm{M}_n^r \times \mathrm{Gr}(n, i)$.
Let $p_1 : Y_i \to X_i$ and $p_2 : Y_i \to \mathrm{Gr}(n, i)$ denote the evident projections.
By the fiber dimension theorem:

$$\dim Y_i = \dim X_i + \dim p_1^{-1}(\text{general } x \in X_i) = \dim X_i$$

$$\begin{aligned}\dim Y_i &= \dim \mathrm{Gr}(n,i) + \dim p_2^{-1}(\text{general } W \in \mathrm{Gr}(n,i)) \\ &= i(n-i) + r(n^2 - i(n-i)) = rn^2 - (r-1)i(n-i).\end{aligned}$$

The maximum of $\dim X_i = rn^2 - (r-1)i(n-i)$ is attained for $i = 1$ and $i = n-1$, yielding $\dim Z_r = (n^2 - n + 1)r + (n-1)$.

# Forms of algebras and torsors

Let $G = \underline{\mathrm{Aut}}_k(A)$, an affine group scheme over $k$.

**Recall:** Let $X$ be a $k$-scheme. A *$G$-torsor* over $X$ consists of an $X$-scheme $T$ with $G_X$-action $T \times_X G_X \to T$, such that there exists a faithfully flat morphism $X' \to X$ for which $T_{X'} \cong G_{X'}$ as right $G_{X'}$-spaces. (Informally, $G$ acts freely on $T$, and $X = T/G$.)

**Example:** The trivial torsor, $G_X = X \times_k G$ over $X$.

**Example:** Let $R$ be $k$-ring and let $B$ be an $R$-form of $A$. Put $X = \mathrm{Spec}\, R$ and $T = \underline{\mathrm{Iso}}_R(A \otimes_k R, B)$. Then $T$ is a $G$-torsor over $X$.

**Theorem (Serre)**

There is an equivalence of categories

$$\{R\text{-forms of } A\} \sim \{G\text{-torsors over } Spec R\}$$

given by $B \mapsto \underline{\mathrm{Iso}}_R(A \otimes_k R, B)$ and $T \mapsto T \times^G A$.

# The variety of $r$-tuples which generate $A$

Let $U_r = A^r - Z_r$ denote the variety of $r$-tuples $(a_1, \dots, a_r) \in A^r$ generating $A$. Formally,

$$U_r(S) = \{(a_1, \dots, a_r) \in A_S^r \,:\, a_1, \dots, a_r \text{ generate } A_S \text{ as an } S\text{-algebra}\}.$$

Then $G = \underline{\mathrm{Aut}}_k(A)$ acts on $U_r$, and $U_r$ is a $G$-torsor over $U_r/G$ (a priori $U_r/G$ is not a scheme but an algebraic space).

## Proposition

Let $R$ be a $k$-ring, let $B$ be an $R$-form of $A$ and let $T$ be its associated $G$-torsor. Then the following are in canonical bijection:

1. $G$-equivariant morphisms $T \to U_r$,
2. $r$-tuples $(b_1, \dots, b_r) \in B^r$ generating $B$ as an $R$-algebra.

In order to prove the Theorem B, we need so show that if $\mathrm{codim}_{A^r} Z_r > d$, then every $G$-torsor over a $d$-dimensional finite type $k$-ring is a specialization of $U_r \to U_r/G$.

# Some remarks

1. Morphisms $Y \to U_r/G$ classify tuples $(B, b_1, \dots, b_r)$ where $B$ is a $Y$-form of $A$ and $b_1, \dots, b_r$ are global sections generating $B$ (this is a categorical equivalence).
2. The identity morphism $U_r/G \to U_r/G$ corresponds to a $U_r/G$-form of $A$ which is the universal for being generated by $r$ elements.
3. $U_r$ embeds $G$-equivariantly in $U_{r+1}$ by appending a 0. These embeddings induce a tower of "approximations"

$$\begin{array}{ccccccc} U_1/G & \longrightarrow & U_2/G & \longrightarrow & U_3/G & \longrightarrow & \cdots \\ \downarrow & \swarrow & & \swarrow & & & \\ BG & & & & & & \end{array}$$

Constructing forms of $A$ which can be generated by $r$ elements and no fewer amounts to obstructing the existence of maps $U_r/G \to U_{r-1}/G$ over $BG$. Obstructing such maps using low-dimensional invariants results in examples over a low-dimensional base ring/scheme.

# $d$-versal torsors

## Definition

Let $G$ be a group scheme over $k$, and let $\mathscr{C}$ be a class of $k$-schemes. We say that a $G$-torsor $T \to X$ is *versal* for $\mathscr{C}$ if every $G$-torsor $T_1 \to X_1$ with $X_1 \in \mathscr{C}$ is a specialization of $T \to X$.
When $\mathscr{C}$ is the class of $d$-dimensional finite type affine $k$-schemes, we simply say that $T \to X$ is *$d$-versal*.

**Remark:** When $\mathscr{C}$ is the class of $k$-fields, we recover *weakly versal* torsors.

**Question:** Are there $d$-versal torsors?

## Theorem C (F–Reichstein, 2020)

Let $\rho : G \to \mathrm{GL}(V)$ be a representation and let $Z$ denote a $G$-subvariety of $V$ with $\operatorname{codim}_V Z > d$. Then $(V - Z) \to (V - Z)/G$ is $d$-versal, provided that $G$ acts freely on $V - Z$.

Totaro, 1999: There exist appropriate $V$ and $Z$ for every $d$.

# Recap: Proof of Theorem B

**Theorem B (F–R)**

Let $R$ be a finite type $k$-ring, and let $d = \dim R$.
Assume that $r \dim A - \dim Z_r > d$.
Then every $R$-form of $A$ can be generated by $r$ elements.

**Proof.** Let $B$ be an $R$-form of $A$.

Let $T = \underline{\mathrm{Iso}}_R(A \otimes_k R, B)$ be its associated $G$-torsor.

We assume that $r \dim A > \dim Z_r + d$, or rather, $\dim_{A^r} Z_r > d$.

By Theorem C, $U_r \to U_r/G$ is $d$-versal, so there exists a $G$-equivariant morphism $f : T \to U_r$.

By the proposition, $f : T \to U_r$ corresponds to an $r$-tuple $(b_1, \ldots, b_r) \in B^r$ generating $B$.

# Questions

**Question 1.** Are the upper bounds on number of generators implied by Theorem B the best possible?

Theorem B applies only to finite type $k$-rings $R$ where $k$ is an infinite field, whereas Theorem A applies to all rings.

**Question 2.** What can be said about the number of generators of forms $A$ when $k$ and $R$ are general noetherian rings?
Specifically, can any Azumaya algebra of degree $n$ over a $d$-dimensional ring be generated by $2 + \lfloor \frac{d}{n-1} \rfloor$ elements?

Thank you!