Serre's Conjecture for Projective Modules

Omkar Javadekar



Department of Mathematics
Indian Institute of Technology, Bombay

October 26, 2020

What is Serre's Conjecture?

Theorem

Every finitely generated projective module over a polynomial ring in finitely many variables is free.

1. It is also known as Quillen–Suslin theorem.
2. Conjectured by J. P. Serre in 1955.
3. In 1958 C. S. Seshadri proved the conjecture for polynomial ring in two variables.
4. Daniel Quillen and Andrei Suslin indepenently proved it in 1976.
5. Leonid Vaserstein later gave a simpler proof of this result.

Strategy of the Proof

1. Finite projective modules over polynomial rings are stably free.
2. Unimodular extension property and Horrocks theorem.
3. Polynomial rings have unimodular column extension property.
4. Stably free modules over a ring with unimodular column extension property are free.

Definitions

Throughout this talk, all rings are assumed to be commutative with multiplicative identity.

Definition

An R-module F is said to be *free* if it has a basis, i.e. if $F \cong \bigoplus_{i \in \Lambda} R$.

Definition

An R-module P is said to be *projective* if there exists a free R-module F and an R-module Q such that $F = P \oplus Q$.

Definition

An R-module E is said to be *stably free* if there exists a finitely generated free module F such that $E \oplus F$ is free of finite rank.

Stably Free Modules

Theorem

Let M be a projective module. Then M is stably free if and only if M admits a finite free resolution .

Proof:

If M is stably free, then for some finite free module F, $M \oplus F$ is finite free.

Thus, M has a finite free resolution

$$0 \to F \to M \oplus F \to M \to 0$$

Proof (Continued)...

Conversely let

$$0 \to E_n \to \cdots \to E_1 \to E_0 \to M \to 0$$

be a finite free resolution of M. We induct on n.

For $n = 0$ the result is trivial.

Let M_1 denote the kernel of $E_0 \to M$. Since M is projective, $E_0 = M \oplus M_1$. Now M_1 is projective, and has a free resolution of length $< n$.

Thus, by induction hypothesis $M_1 \oplus F$ is finite free for some finite free module F.

Therefore, $M \oplus (M_1 \oplus F) = E_0 \oplus F$ is finite free. $\square$

Finite Projective $\Rightarrow$ Stably Free

Theorem

Let R be a commutative Noetherian ring. Let x be a variable . If every finite R-module has a finite free resolution, then every finite $R[x]$-module has a finite free resolution.

Theorem (Hilbert–Serre)

If k is a field and $x_1, \ldots, x_r$ independent variables, then every finite projective module over $k[x_1, \ldots, x_r]$ is stably free, or equivalently, admits a finite free resolution .

Strategy of the Proof

1. Finite projective modules over polynomial rings are stably free.
2. Unimodular extension property and Horrocks theorem.
3. Polynomial rings have unimodular column extension property.
4. Stably free modules over a ring with unimodular column extension property are free.

Unimodular Extension Property

Definition

Let R be a commutative ring. Let $f = (f_1, \ldots, f_n) \in R^n$ is called *unimodular* if $R = \langle f_1, \ldots, f_n \rangle$. We say that f has the *unimodular extension property* if there exists a matrix in $GL_n(R)$ with first column $(f_1, \ldots, f_n)^T$.

Definition

A ring R is said to have the *unimodular column extension property* if every unimodular vector $f \in R^n$ has the unimodular extension property, for all positive integers n.

Horrocks Theorem

Theorem (Horrocks)

Let $(A, \mathfrak{m})$ be a local ring and let $R = A[x]$ be the polynomial ring in one variable over A. Let $f \in R^n$ be unimodular such that some component has leading coefficient 1. Then f has the unimodular extension property.

Proof:

- If $n = 1$, then $f = f_1$ itself is a unit, and we are done.
- If $n = 2$, then using $R = \langle f_1(x), f_2(x) \rangle$ we see that there exist $g_1(x), g_2(x) \in A[x]$, such that

$$1 = f_1(x)g_1(x) + f_2(x)g_2(x)$$

and hence we get a 2×2 invertible matrix

$$\begin{bmatrix} f_1(x) & -g_2(x) \\ f_2(x) & g_1(x) \end{bmatrix}.$$

Proof (continued)...

So, we assume $n > 2$ and do an induction of the smallest degree d of a component of f with leading coefficient 1.

Note that if $d = 0$, then the result is obvious. So, assume $d > 0$.

Without loss of generality, we may assume that f_1 has leading coefficient 1, degree d, and that $\deg(f_i) < d$ for $i \neq 1$.

Since f is unimodular, a relation $\sum g_i f_i = 1$ shows that not all coefficients of $f_2, \ldots f_n$, lie in the maximal ideal $\mathfrak{m}$.

Without loss of generality, we may assume that some coefficient of f_2 does not lie in $\mathfrak{m}$ and so is a unit since A is local.

Proof (continued)...

We write

$$\begin{aligned} f_1(x) &= x^d + a_{d-1}x^{d-1} + \cdots + a_0 \\ f_2(x) &= \qquad\qquad b_s x^s + \cdots + b_0 \end{aligned}$$

with $a_i \in A$, $b_i \in A$, $s < d$, such that some b_i is a unit.

Let $\mathfrak{a}$ be the ideal generated by all leading coefficients of polynomials $h_1 f_1 + h_2 f_2$ of degree $< d$. We claim that $\mathfrak{a}$ contains all the coefficients $b_i, i = 0, ..., s$.

Note that $b_s \in \mathfrak{a}$ is obvious $(0 \cdot f_1(x) + 1 \cdot f_2(x))$. And by repeated use of a linear combination like

$$x^{d-s} f_2(s) - b_s f_1(x) = (b_{s-1} - b_s a_{d-1})x^{d-1} + \cdots$$

(and then by adding $b_s a_{d-1} x^{d-1} + \cdots$) it follows that all b_i's are in $\mathfrak{a}$.

Proof(continued)...

Therefore $\mathfrak{a}$ is the unit ideal, and there exists a polynomial $h_1 f_1 + h_2 f_2$ of degree $< d$ with leading coefficient 1.

By row operations, we now get a polynomial of degree $< d$ and leading coefficient 1 as some component in the i-th place, for some $i \neq 1, 2$.

Therefore, the proof is complete by induction. $\square$

Corollaries

Definition

The column vectors $f, g \in R^n$ are said to be *equivalent* over R if $f = Mg$ for some $M \in GL_n(R)$, and we write $f \sim g$ in such a case.

Corollary

Let A be a local ring, $R = A[x]$, and $f \in R^n$ be a unimodular vector with one component having leading coefficient 1. Then $f \sim (1, 0, \ldots, 0)$.

Proof:

By Horocks theorem, there exists $M \in GL_n(R)$ with first column equal to f. Then $M^{-1}f = (1, 0, \ldots, 0)^T$. □

Corollaries

Corollary

Let A be a local ring, $R = A[x]$. Let f be a unimodular vector in R^n such that some component has leading coefficient 1. Then $f \sim f(0)$ over R.

Proof:

By previous corollary, $f \sim (1, 0, \ldots, 0)$.

Since f is unimodular, and A is local, there is a component of f having constant term which is a unit in A.

Therefore there exists $M \in GL_n(A) \subseteq GL_n(R)$ such that $f(0)$ is its first column, and hence $f(0) \sim (1, 0, \ldots, 0)$. $\square$

Strategy of the Proof

1. Finite projective modules over polynomial rings are stably free.
2. Unimodular extension property and Horrocks theorem.
3. Polynomial rings have unimodular column extension property.
4. Stably free modules over a ring with unimodular column extension property are free.

A Localization Lemma

Lemma

Let R be an integral domain, and let S be a multiplicative subset. Let x, y be independent variables. If $f(x) \sim f(0)$ over $S^{-1}R[x]$, then there exists $c \in S$ such that $f(x + cy) \sim f(x)$ over $R[x, y]$.

Proof:

Let $M \in GL_n(S^{-1}R[x])$ be such that $f(x) = M(x)f(0)$.

Then $M(x)^{-1}f(x) = f(0)$ is constant, and thus invariant under translation $x \mapsto x + y$.

Let

$$G(x, y) = M(x)M(x + y)^{-1}.$$

Then $G(x, y)f(x + y) = f(x)$. We have $G(x, 0) = I$, and hence

$$G(x, y) = I + yH(x, y)$$

with $H(x, y) \in S^{-1}R[x, y]$.

Proof (Continued)...

There exists $c \in S$ such that cH has coefficients in $R[x, y]$.

Thus, we have $G(x, cy)f(x + cy) = f(x)$ and $G(x, cy)$ has all entries in $R[x, y]$.

We also have $G(x, cy) = M(x)M(x + cy)^{-1}$.

Since $M(x)$ is invertible, $\det M(x)$ is constant in $S^{-1}R$, and thus it follows that $\det M(x + cy)$ is equal to the same constant.

Therefore, $\det G(x, cy) = 1$. This proves the lemma. $\square$

Theorem

Let R be an integral domain, and let f be a unimodular vector in $R[x]^n$, such that one component has leading coefficient 1. Then $f(x) \sim f(0)$ over $R[x]$.

Proof:

Let J be the set of elements $c \in R$ such that $f(x + cy) \sim f(x)$ over $R[x, y]$.

Then J is an ideal. This is because $0 \in J$, and if $c \in J$ and $a \in R$ then replacing y by ay in the equivalence above shows that

$$f(x + cay) \sim f(x)$$

over $R[x, ay]$, so over $R[x, y]$. Similarly, we have that if $c, c' \in J$, then $c + c' \in J$.

Proof (Continued)...

Now let $\mathfrak{p}$ be a prime ideal of R. Since $R_{\mathfrak{p}}$ is local, by Horrocks theorem we get that

$$f(x) \sim f(0) \text{ over } R_{\mathfrak{p}}[x].$$

Now, by the previous lemma it follows that there exists $c \in R$ and $c \notin \mathfrak{p}$ such that $f(x + cy) \sim f(x)$ over $R[x, y]$.

Hence J is not contained in $\mathfrak{p}$, and so J is unit ideal in R. Thus, there exists an invertible matrix $M(x, y)$ over $R[x, y]$ such that

$$f(x + y) = M(x, y)f(x).$$

Putting 0 for x in above equation gives $f(y) \sim f(0)$. □

Theorem

Let k be a field and $R = k[x_1, \ldots, x_r]$. If f is a unimodular vector in R^n, then f has the unimodular extension property.

Proof: (By induction on r).
If $r = 1$ then $k[x_1]$, and the result is easy to prove.

Assume the theorem for $r - 1$ variables with $r > 1$, and put $A = k[x_1, \ldots, x_{r-1}]$.

If we let $y_r = x_r$ and $y_i = x_i - x_r^{m_i}$ (for suitable $m_i \in \mathbb{N}$), then the polynomial vector

$$f(x_1, \ldots, x_r) = g(y_1, \ldots, y_r)$$

has one component with y_r-leading coefficient equal to a nonzero element of k. Without loss of generality, we may assume that it is equal to 1.

Proof(continued)...

By previous theorem, there exists a matrix

$$N(y_1, \ldots, y_r) = M(x_1, \ldots, x_n)$$

invertible over $A[x_r] = A[y_r]$ such that

$$g(y_1, \ldots, y_r) = N(y_1, \ldots, y_r)g(y_1, \ldots, y_{r-1}, 0),$$

and $g(y_1, \ldots, y_{r-1}, 0)$ is unimodular in $k[y_1, \ldots, y_{r-1}]^n$.

Thus, the proof can be concluded by induction. □

Strategy of the Proof

1. Finite projective modules over polynomial rings are stably free.
2. Unimodular extension property and Horrocks theorem.
3. Polynomial rings have unimodular column extension property.
4. Stably free modules over a ring with unimodular column extension property are free.

Stably Free + UCEP $\Rightarrow$ Free

Theorem

If R has unimodular column extension property, then every stably free R-module is free.

Proof:

Let E be stably free. We induct on the rank of the free modules F such that $E \oplus F$ is free.

By induction, it suffices to prove that if $E \oplus R$ is free then E is free.

So, let $E \oplus R = R^n$ and let p: $R^n \to R$ denote the projection map. Suppose $\{u_1\}$ is a basis of R over itself.

Viewing R as a direct summand in $E \oplus R = R^n$ we write

$$u_1 = (a_{11}, \ldots, a_{n1})^T, \quad \text{with } a_{i1} \in R$$

Then u_1 is unimodular, and by assumption u_1 is the first column of a matrix $M = (a_{ij})$ whose determinant is a unit in R.

Proof(continued)...

Let

$$u_j = Me_j \quad \text{for } j = 1, \ldots, n\,,$$

where e_j is the j-th unit column vector of R^n.

Note that u_1 is the first column of M. By elementary column operations, we may change M so that $u_j \in E$ for $j = 2, \ldots, n$. Indeed, if $\mathrm{p}(e_j) = cu_1$ for $j > 1$ we replace e_j by $e_j - ce_1$.

So, without loss of generality we assume that $u_2, \ldots, u_n$ lie in E.

Since $M \in GL_n(R)$, M induces an automorphism of R^n as R-module with itself by $X \mapsto MX$.

From the construction and the fact that $R^n = E \oplus R$ we get that M maps the free module with basis $\{e_2, \ldots, e_n\}$ onto E. This concludes the proof. □

Strategy of the Proof

1. Finite projective modules over polynomial rings are stably free.
2. Unimodular extension property and Horrocks theorem.
3. Polynomial rings have unimodular column extension property.
4. Stably free modules over a ring with unimodular column extension property are free.

References

- S. S. Abhyankar, *Lectures on Algebra, Volume I*, World Scientific Publishing Co. Pte. Ltd. (2006).
- S. Lang, *Algebra*, Springer-Verlag New York, Graduate Texts in Mathematics, (2002).
- T.Y. Lam, *Serre's Problem on Projective Modules*, Springer-Verlag Berlin Heidelberg, Springer Monographs in Mathematics, (2006).
- N. Mohan Kumar, *On a theorem of Seshadri*, https://www.math.wustl.edu/ kumar/papers/seshadri.pdf
- Nil Garces de Marcilla Escubedo, *The Quillen-Suslin Theorem*, http://diposit.ub.edu/dspace/bitstream/2445/125803/2/memoria.pdf
- https://en.wikipedia.org/wiki/Quillen–Suslin_theorem.

Thank You!