On the Complexity of Embedding Configurations in Finite Planes

G. Eric Moorhouse

Department of Mathematics
University of Wyoming

RMDMD 19 May 2012

Acknowledgement

Joint work with Jason Williford and John Hitchcock at the University of Wyoming.

Point-Line Incidence Structures

In a *projective plane*,

- any two points are on a unique line;
- any two lines meet in a unique point.

In a *linear space*,

- any two points are on a unique line;
- any two lines meet in *at most one* point.

In a *partial linear space*,

- any two points are on *at most one* line;
- any two lines meet in *at most one* point.

Point-Line Incidence Structures

In a *projective plane*,

- any two points are on a unique line;
- any two lines meet in a unique point.

In a *linear space*,

- any two points are on a unique line;
- any two lines meet in *at most one* point.

In a *partial linear space*,

- any two points are on *at most one* line;
- any two lines meet in *at most one* point.

Point-Line Incidence Structures

In a *projective plane*,

- any two points are on a unique line;
- any two lines meet in a unique point.

In a *linear space*,

- any two points are on a unique line;
- any two lines meet in *at most one* point.

In a *partial linear space*,

- any two points are on *at most one* line;
- any two lines meet in *at most one* point.

Embeddings

Let $(\mathfrak{P}, \mathfrak{L})$ and $(\mathfrak{P}', \mathfrak{L}')$ be partial linear spaces.

A *(weak) embedding* of $(\mathfrak{P}, \mathfrak{L})$ into $(\mathfrak{P}', \mathfrak{L}')$ is a pair of injections

$$\phi : \mathfrak{P} \to \mathfrak{P}', \quad \mathfrak{L} \to \mathfrak{L}'$$

such that

$$P \in \ell \;\Rightarrow\; \phi(P) \in \phi(\ell).$$

For a *strict embedding*,

$$P \in \ell \;\Leftrightarrow\; \phi(P) \in \phi(\ell).$$

Every embedding of a linear space is strict.

Embeddings

Let $(\mathfrak{P}, \mathfrak{L})$ and $(\mathfrak{P}', \mathfrak{L}')$ be partial linear spaces.

A *(weak) embedding* of $(\mathfrak{P}, \mathfrak{L})$ into $(\mathfrak{P}', \mathfrak{L}')$ is a pair of injections

$$\phi : \mathfrak{P} \to \mathfrak{P}', \quad \mathfrak{L} \to \mathfrak{L}'$$

such that

$$P \in \ell \;\Rightarrow\; \phi(P) \in \phi(\ell).$$

For a *strict embedding*,

$$P \in \ell \;\Leftrightarrow\; \phi(P) \in \phi(\ell).$$

Every embedding of a linear space is strict.

Embeddings

Let $(\mathfrak{P}, \mathfrak{L})$ and $(\mathfrak{P}', \mathfrak{L}')$ be partial linear spaces.

A *(weak) embedding* of $(\mathfrak{P}, \mathfrak{L})$ into $(\mathfrak{P}', \mathfrak{L}')$ is a pair of injections

$$\phi : \mathfrak{P} \to \mathfrak{P}', \quad \mathfrak{L} \to \mathfrak{L}'$$

such that

$$P \in \ell \;\Rightarrow\; \phi(P) \in \phi(\ell).$$

For a *strict embedding*,

$$P \in \ell \;\Leftrightarrow\; \phi(P) \in \phi(\ell).$$

Every embedding of a linear space is strict.

Examples of Embeddings

$AG(2,3)$ embeds in $PG(2,F)$ iff $\mathrm{char}(F) = 3$ or F has a primitive cube root of unity. (Note: $\mathbb{F}_q$ satisfies this condition iff $q \not\equiv 2 \mod 3$.)

The Desargues configuration embeds in every finite projective plane.

(Weak) embeddings of cycles in finite projective planes were the subject of Felix Lazebnik's talk.

Bryan Petrak spoke about embeddings of $PG(2,2)$ and $PG(2,3)$ in finite Figueroa planes.

Examples of Embeddings

$AG(2,3)$ embeds in $PG(2,F)$ iff $\mathrm{char}(F) = 3$ or F has a primitive cube root of unity. (Note: $\mathbb{F}_q$ satisfies this condition iff $q \not\equiv 2 \mod 3$.)

The Desargues configuration embeds in every finite projective plane.

(Weak) embeddings of cycles in finite projective planes were the subject of Felix Lazebnik's talk.

Bryan Petrak spoke about embeddings of $PG(2,2)$ and $PG(2,3)$ in finite Figueroa planes.

Examples of Embeddings

$AG(2,3)$ embeds in $PG(2,F)$ iff $\text{char}(F) = 3$ or F has a primitive cube root of unity. (Note: $\mathbb{F}_q$ satisfies this condition iff $q \not\equiv 2 \mod 3$.)

The Desargues configuration embeds in every finite projective plane.

(Weak) embeddings of cycles in finite projective planes were the subject of Felix Lazebnik's talk.

Bryan Petrak spoke about embeddings of $PG(2,2)$ and $PG(2,3)$ in finite Figueroa planes.

Examples of Embeddings

$AG(2,3)$ embeds in $PG(2,F)$ iff $\text{char}(F) = 3$ or F has a primitive cube root of unity. (Note: $\mathbb{F}_q$ satisfies this condition iff $q \not\equiv 2 \mod 3$.)

The Desargues configuration embeds in every finite projective plane.

(Weak) embeddings of cycles in finite projective planes were the subject of Felix Lazebnik's talk.

Bryan Petrak spoke about embeddings of $PG(2,2)$ and $PG(2,3)$ in finite Figueroa planes.

Embeddings

Open Question

Does every finite partial linear space embed in a finite projective plane?

Given a finite partial linear space $(\mathfrak{P}, \mathfrak{L})$, how does one look for a finite projective plane in which $(\mathfrak{P}, \mathfrak{L})$ embeds?

It is even notoriously difficult to decide: Does $(\mathfrak{P}, \mathfrak{L})$ embed in $PG(2, \mathbb{F}_q)$ for some q? Equivalently, does $(\mathfrak{P}, \mathfrak{L})$ embed in $PG(2, \overline{\mathbb{F}_p})$ for some p? where $\overline{F}$ is the algebraic closure of F.

Embeddings

Open Question

Does every finite partial linear space embed in a finite projective plane?

Given a finite partial linear space $(\mathfrak{P}, \mathfrak{L})$, how does one look for a finite projective plane in which $(\mathfrak{P}, \mathfrak{L})$ embeds?

It is even notoriously difficult to decide: Does $(\mathfrak{P}, \mathfrak{L})$ embed in $PG(2, \mathbb{F}_q)$ for some q? Equivalently, does $(\mathfrak{P}, \mathfrak{L})$ embed in $PG(2, \overline{\mathbb{F}_p})$ for some p? where $\overline{F}$ is the algebraic closure of F.

Embeddings

Open Question

Does every finite partial linear space embed in a finite projective plane?

Given a finite partial linear space $(\mathfrak{P}, \mathfrak{L})$, how does one look for a finite projective plane in which $(\mathfrak{P}, \mathfrak{L})$ embeds?

It is even notoriously difficult to decide: Does $(\mathfrak{P}, \mathfrak{L})$ embed in $PG(2, \mathbb{F}_q)$ for some q? Equivalently, does $(\mathfrak{P}, \mathfrak{L})$ embed in $PG(2, \overline{\mathbb{F}_p})$ for some p? where $\overline{F}$ is the algebraic closure of F.

Embeddings

Open Question

Does every finite partial linear space embed in a finite projective plane?

Given a finite partial linear space $(\mathfrak{P}, \mathfrak{L})$, how does one look for a finite projective plane in which $(\mathfrak{P}, \mathfrak{L})$ embeds?

It is even notoriously difficult to decide: Does $(\mathfrak{P}, \mathfrak{L})$ embed in $PG(2, \mathbb{F}_q)$ for some q? Equivalently, does $(\mathfrak{P}, \mathfrak{L})$ embed in $PG(2, \overline{\mathbb{F}_p})$ for some p? where $\overline{F}$ is the algebraic closure of F.

Lower Bound on the Complexity

We consider the *time complexity* of the problem of finding an embedding of $(\mathfrak{P}, \mathfrak{L})$ in some finite classical plane $PG(2, q)$.

We show that given a large integer N, there exists a partial linear space $(\mathfrak{P}, \mathfrak{L})$ with $O(n)$ points and lines where $n = \log N$, such that the problem of factoring N reduces in polynomial time to the problem of embedding $(\mathfrak{P}, \mathfrak{L})$ in a finite classical plane.

Theorem (M)

The problem of embedding a given finite partial linear space in a finite classical plane, is at least as hard as integer factorization.

The corresponding decision problem (*deciding* whether $(\mathfrak{P}, \mathfrak{L})$ embeds in some finite classical plane) *might* be easier than actually constructing an embedding, although I cannot see how.

Lower Bound on the Complexity

We consider the *time complexity* of the problem of finding an embedding of $(\mathfrak{P}, \mathfrak{L})$ in some finite classical plane $PG(2, q)$.

We show that given a large integer N, there exists a partial linear space $(\mathfrak{P}, \mathfrak{L})$ with $O(n)$ points and lines where $n = \log N$, such that the problem of factoring N reduces in polynomial time to the problem of embedding $(\mathfrak{P}, \mathfrak{L})$ in a finite classical plane.

Theorem (M)

The problem of embedding a given finite partial linear space in a finite classical plane, is at least as hard as integer factorization.

The corresponding decision problem (*deciding* whether $(\mathfrak{P}, \mathfrak{L})$ embeds in some finite classical plane) *might* be easier than actually constructing an embedding, although I cannot see how.

Lower Bound on the Complexity

We consider the *time complexity* of the problem of finding an embedding of $(\mathfrak{P}, \mathfrak{L})$ in some finite classical plane $PG(2, q)$.

We show that given a large integer N, there exists a partial linear space $(\mathfrak{P}, \mathfrak{L})$ with $O(n)$ points and lines where $n = \log N$, such that the problem of factoring N reduces in polynomial time to the problem of embedding $(\mathfrak{P}, \mathfrak{L})$ in a finite classical plane.

Theorem (M)

The problem of embedding a given finite partial linear space in a finite classical plane, is at least as hard as integer factorization.

The corresponding decision problem (*deciding* whether $(\mathfrak{P}, \mathfrak{L})$ embeds in some finite classical plane) *might* be easier than actually constructing an embedding, although I cannot see how.

Let $(\mathfrak{P}, \mathfrak{L})$ be a partial linear space with $O(n)$ points and $O(n)$ lines, and let p be prime. Consider the decision problem: Does $(\mathfrak{P}, \mathfrak{L})$ embed in $PG(2, \overline{\mathbb{F}_p})$?

Theorem (M)

There is a deterministic algorithm to answer this question in time $e^{O(n^4)}$. (Also a nondeterministic algorithm in time $e^{O(n^2)}$.)

Can one do better?

Let $(\mathfrak{P}, \mathfrak{L})$ be a partial linear space with $O(n)$ points and $O(n)$ lines, and let p be prime. Consider the decision problem: Does $(\mathfrak{P}, \mathfrak{L})$ embed in $PG(2, \overline{\mathbb{F}_p})$?

Theorem (M)

There is a deterministic algorithm to answer this question in time $e^{O(n^4)}$. (Also a nondeterministic algorithm in time $e^{O(n^2)}$.)

Can one do better?

Obstacle to Improving the Upper Bound

Theorem (M)

Let $n_0 > 1$. There exists $n > n_0$ a finite partial linear space $(\mathfrak{P}, \mathfrak{L})$ with $O(n)$ points and lines, which embeds in some finite classical plane $PG(2, q)$, yet for which the smallest such q satisfies $q \geq 2^{2^{\Omega(n)}}$ (and so coordinates in $\mathbb{F}_q$ are expressed as strings of length $2^{\Omega(n)}$).

Thank You!

Questions?