Geometric Secret Sharing Schemes

Bill Cherowitzo
CU-Denver

The Great River Bank

The Great River Bank has a president, four vice presidents and five senior tellers. The president knows the combination to the vault, but he is rarely at the bank. It is necessary for the vault to be opened daily, so the combination needs to be known by other personnel in the bank. The president does not want the combination to be known by any individual other than himself. He would like a way to give out parts (***shares***) of the combination (the **secret**) so that any two of the vice presidents can combine their information and open the vault, or any one of the vice presidents and any three of the senior tellers can open the vault. Other combinations of personnel, such as one vice president and only two senior tellers, or all five senior tellers, should not be able to open the vault.

Secret Sharing Schemes

A solution to the president's problem would be called a ***Secret Sharing Scheme***. The various combinations of people who could combine their information to get the secret is known as an ***access structure***. If any group of people not in the access structure have no additional information about the secret than someone not involved in the scheme, then the secret sharing scheme is said to be ***perfect***.

We will first look at one of the simplest access structures, where there are n people involved and any k of them can obtain the secret. Schemes with this access structure are called ***k out of n schemes*** (also known as *(k,n)-threshold schemes*).

Shamir's (k,n)-threshold scheme

Let ***F*** be a field. The secret, K, is an element of this field. The dealer (the person who wants to share the secret), randomly selects k-1 elements of ***F***, say, $a_1, a_2, ..., a_{k-1}$ and forms the polynomial,

$$f(x) = K + a_1x + a_2x^2 + ... + a_{k-1}x^{k-1} .$$

For each of the participants, the dealer picks an element x_i from ***F*** (but not 0) and calculates $f(x_i)$. The share given to participant i is the pair $(x_i, f(x_i))$.

Shamir's (k,n)-threshold scheme

Now, if k participants pool their information, the polynomial f(x) can be reconstructed (for instance, by using the Lagrange interpolation formula) and the constant term (i.e., the secret) can be obtained by evaluating the polynomial at 0. If less than k participants combine their information, then the polynomial is not uniquely determined, and its constant term could be any element of the field. So having less than k shares is equivalent to having no shares at all.

This scheme is thus a perfect (k,n)-threshold scheme.

Lagrange Interpolation Polynomial

Over any field, there is a unique polynomial f(x) of degree t-1, so that $f(x_i) = y_i$ with $1 \le i \le t$, the x_i distinct and the y_i arbitrary elements of the field. This polynomial is constructed as follows:

$$f(x) = \sum_{k=1}^{t} y_k \prod_{j \neq k} \frac{x - x_j}{x_k - x_j}.$$

Note that $\prod_{j \neq k} \frac{x_j - x_j}{x_k - x_j} = \begin{cases} 1 \text{ when } k = j \\ 0 \text{ when } k \neq j \end{cases}$.

Lagrange Interpolation Polynomial

For example, over Z_5 the polynomial having the values f(0) = 3, f (1) = 4 and f(3) = 3 is:

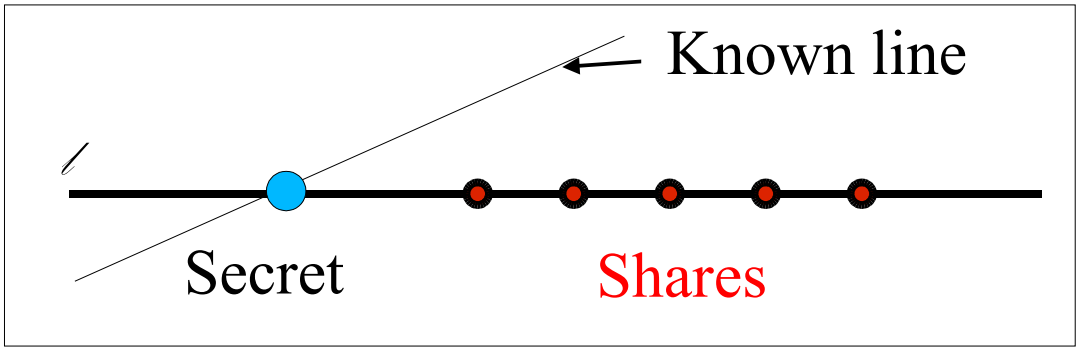
$$f(x)=3\left(\frac{x-1}{-1}\right)\left(\frac{x-3}{-3}\right)+4\left(\frac{x}{1}\right)\left(\frac{x-3}{1-3}\right)+3\left(\frac{x}{3}\right)\left(\frac{x-1}{3-1}\right)$$

$$f(x)=x^2-4x+3-2(x^2-3x)+\frac{1}{2}(x^2-x)$$

$$f(x)=2x^2-x+3.$$

Geometric Threshold Schemes

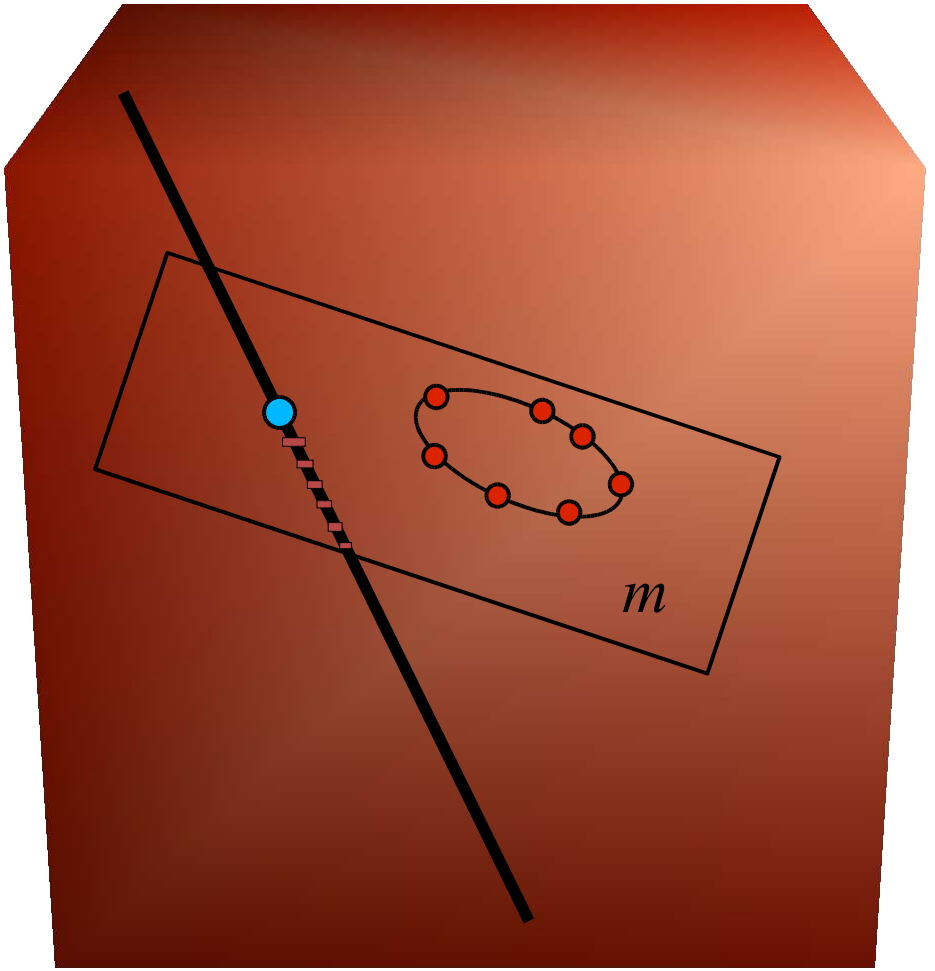
Let the secret be the coordinates of a fixed point on a given line in a plane (the line and the fact that the secret is a point on that line is public information). Let ⁄ be another line which intersects the given line at the secret point. As shares, the distinct points of ⁄ can be given out. If you know two of these points, then the line ⁄ is determined and its intersection with the given line will give the secret. This is a perfect (2,n)-threshold scheme for any n.



Another Example

Let the secret be the coordinates of a point on a line in 3-space. Let m be a plane which intersects the line only at the secret point. Let $\mathscr{C}$ be any arc in m. As shares, distinct points on $\mathscr{C}$ can be given out. Any three points of $\mathscr{C}$ can be used to determine m and therefore the secret, but two or fewer points do not, and knowing them would not eliminate any possibilities for the secret point. This is therefore a perfect (3,n)-threshold scheme (for any n). Using points on an arc ensures that any three shares will determine the plane m.

Another Example Cont.



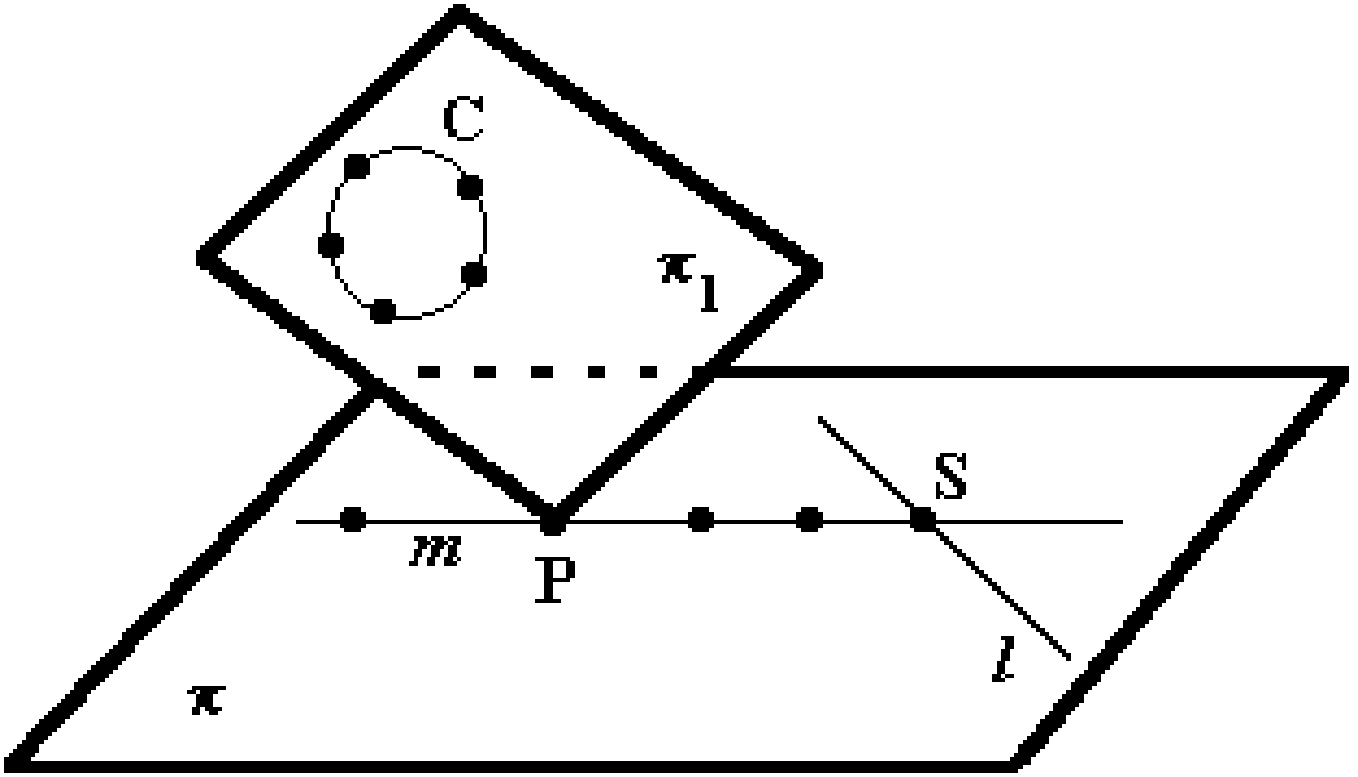
Multilevel Schemes

A multilevel scheme refers to an access structure like the bank example above, where different categories of participants are involved, each having their own criteria for obtaining the secret. For any access structure which is ***monotone***, that is, having the property that every set of participants which contains a subset of participants that can obtain the secret, can also obtain the secret (a rather obvious requirement), we can construct a secret sharing scheme that realizes this structure. One general method utilizes Boolean circuits to construct the scheme. We will not examine this general construction, but rather present a geometric construction for a multilevel access structure.

Bank Problem Revisited

Our geometric construction will use elements of a four-dimensional projective space. The secret S will be a point on a fixed line (ℓ) in a fixed plane π in a 4-dimensional space. Let π_1 be another plane which intersects π in a unique point P which does not lie on ℓ. Let m be the line in π determined by P and S. Finally, let $\mathscr{C}$ be an arc in π_1.

Bank Problem Cont.



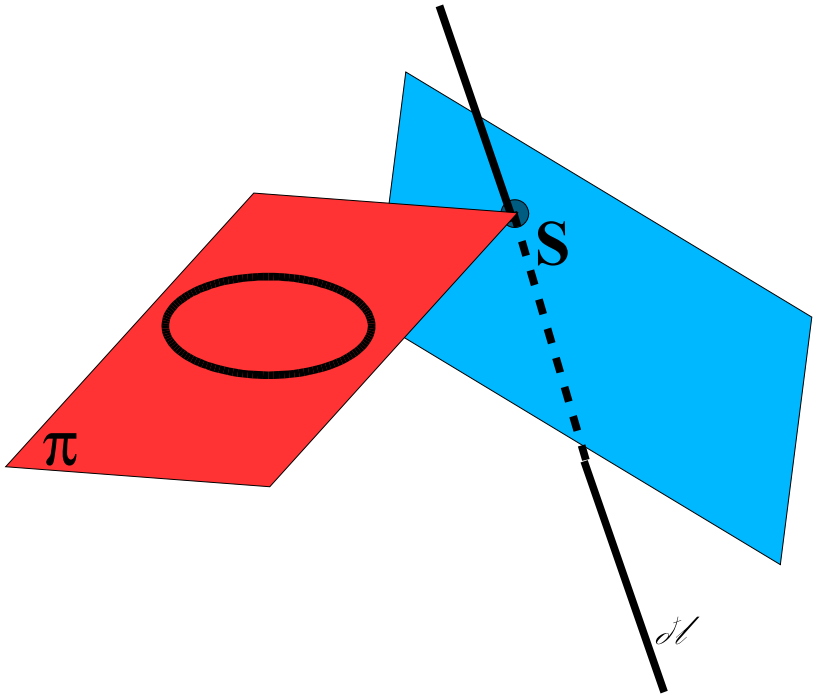
Bank Problem Cont.

Now, as shares, each vice-president gets the coordinates of a point on *m* other than P or S, and each senior teller gets the coordinates of a point on the circle $\mathscr{C}$. Two vice-presidents would have two points on *m*, so they could determine this line and calculate where it intersected $\mathscr{C}$, obtaining the secret. Any three senior tellers could combine their three points and determine the plane π_1, and then calculate where this plane intersects the plane π (giving the point P). Any vice-president could then use their point together with P to determine *m* and hence the secret.

A Variation

As a variant of this bank example consider the access structure which consists of any two vice-presidents or any three senior tellers.

A geometric solution in projective 4-space is given by:



Modifying the Variant

It would be reasonable in this variant to have 1 vice-president and 2 senior tellers also be able to find the secret, but this is not possible in our construction unless the line ℓ is contained in the plane π. This, however, creates other problems. To make the system work, no share given to a vice-president (point of ℓ) can be on a secant of the arc, else the three shares do not determine π.

Given a k-arc $\boldsymbol{K}$ and a line ℓ exterior to $\boldsymbol{K}$, it is not clear that there will be any points of ℓ not on secants of $\boldsymbol{K}$.

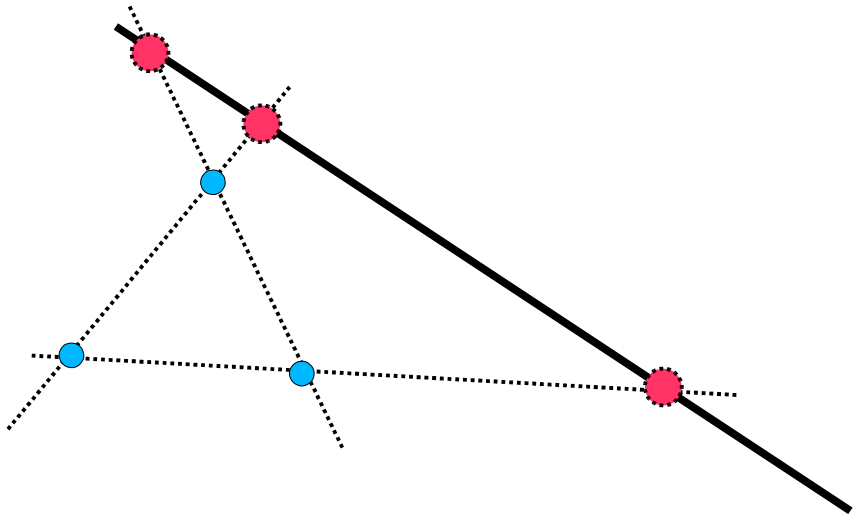
This leads us to consider ...

Sharply Focused Arcs

In a projective plane, a k-arc ***K*** is said to be ***sharply focused*** on a line ℓ (exterior to ***K***) if all the secants of ***K*** meet ℓ in a set of exactly k points.

Examples:

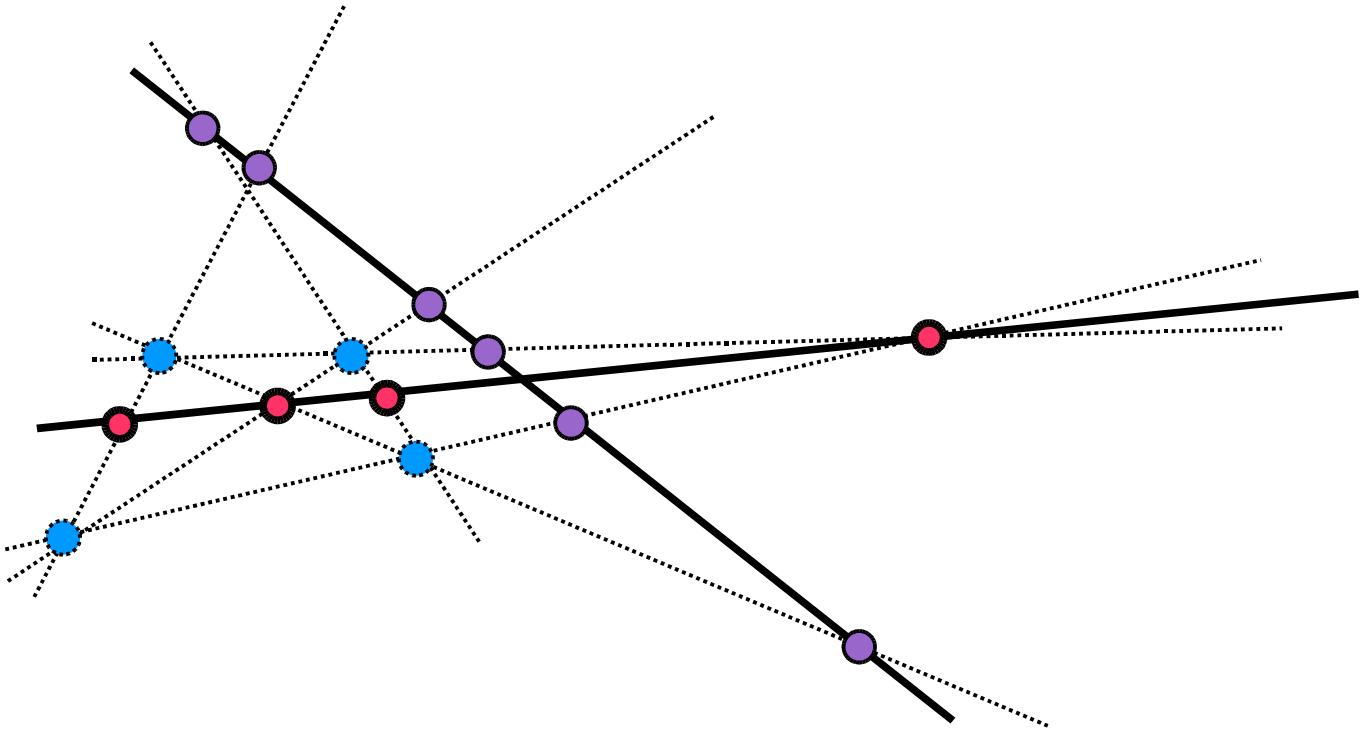
In any projective plane, any 3-arc is sharply focused on any line exterior to the arc.



Sharply Focused Arcs

Examples:

In PG(2,q), q odd, any 4-arc is sharply focused on any diagonal line, but not sharply focused on any other line.



Constructions of SFA's

Theorem (Holder, 200?): A set of points $\boldsymbol{K}$, with $3 < |\boldsymbol{K}|$, on a conic in PG(2,q) is sharply focused on :

a) a **tangent line** to that conic if and only if $\boldsymbol{K}$ is projectively equivalent to a set of points determined by a subgroup of (GF(q),+). In particular, $|\boldsymbol{K}| \mid q$.

b) a **secant line** to that conic if and only if $\boldsymbol{K}$ is projectively equivalent to a set of points determined by a subgroup of (GF(q)*,•). In particular, $|\boldsymbol{K}| \mid q-1$.

c) an **exterior line** to that conic if and only if $\boldsymbol{K}$ is projectively equivalent to a set of points determined by a subgroup of Z_{q+1}. In particular, $|\boldsymbol{K}| \mid q+1$.

Back to the Bank

In the secret sharing scheme application, the points of the k-arc are used as shares for the senior tellers and the points on the line which are not on any secant are the shares given to the vice-presidents. To have shares to give the vp's, the k-arc needs to be focused on the line, and the sharper the focus, the more shares that are available.

Thus, to maximize the vp shares we want the minimum focus. It is easy to see that the theoretical minimum focus for a k-arc is k-1 ...

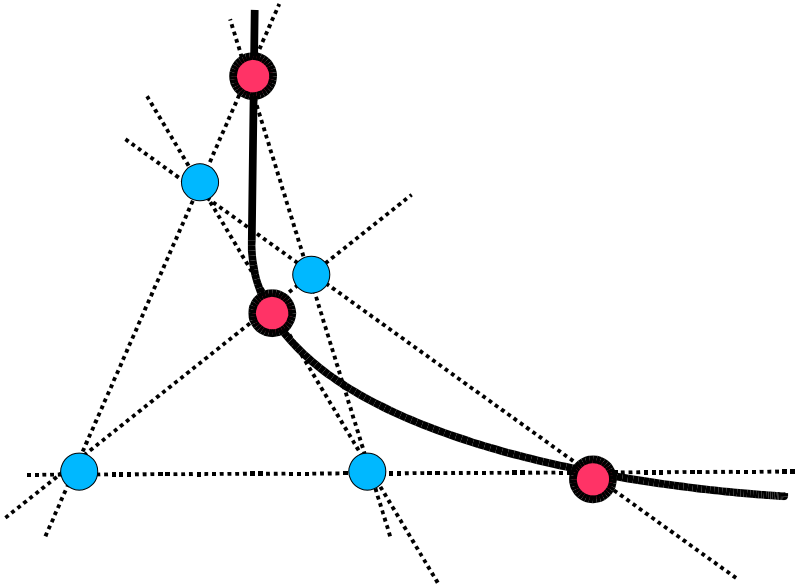
but this can not always be obtained.

Hyperfocused Arcs

In a projective plane, a k-arc ***K*** is said to be ***hyperfocused*** on a line ℓ (exterior to ***K***) if all the secants of ***K*** meet ℓ in a set of exactly k-1 points.

Example:

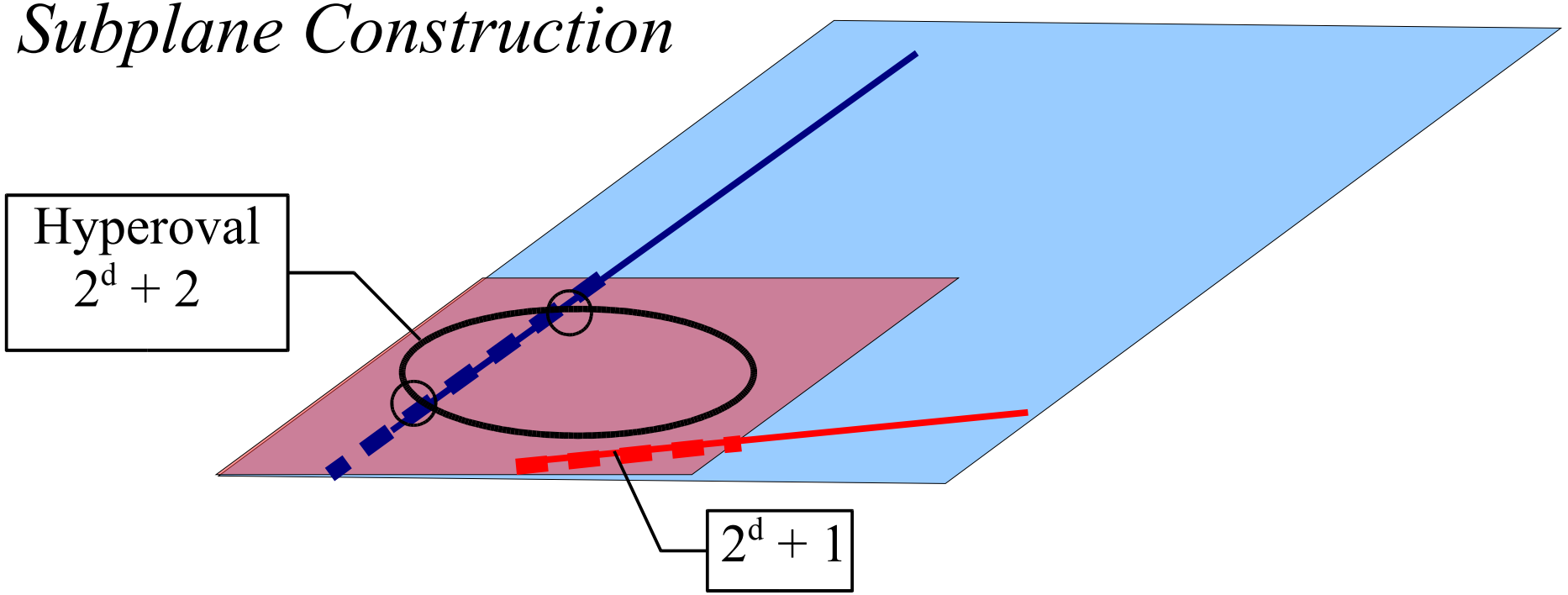
In PG(2,q), q even, any 4-arc is hyperfocused on the diagonal line of the 4-arc.



Construction of SSFA's

Theorem (Holder, 1997): For every divisor d of e, there are hyperfocused sets of sizes 2^d and $2^d + 2$ in PG(2,2^e).

Subplane Construction



The small sfa's and hfa's

k	q	type	on conic
3	3^e, or $\equiv \pm 1 \bmod 3$	sfa	yes
4	2^e, $e > 1$	ssfa	yes
	$\equiv \pm 1 \bmod 4$	sfa	yes
5	5^e, or $\equiv \pm 1 \bmod 5$	sfa	yes
6	2^{2e}	ssfa	yes
	$\equiv \pm 1 \bmod 6$	sfa	yes
7	7^e, or $\equiv \pm 1 \bmod 7$	sfa	yes
8	$\equiv \pm 1 \bmod 8$	sfa	yes
	2^e, $e \geq 3$	ssfa	yes
	8^e	ssfa	no *

*but on a pointed conic.

Open Problems

1. Do there exist sharply focused arcs which are not arcs contained in a conic in PG(2,q), q odd?
- NO!

2. Do there exist hyperfocused arcs in PG(2,q) with q odd?
- NO!

3. Do there exist hyperfocused arcs which are not obtained by the subplane construction?
- YES!

4. What is the situation in non-Desarguesian planes? - ???