

Discrete Math, 8th day, Friday 7/2/04
REU 2004. Info:
<http://people.cs.uchicago.edu/~laci/reu04>.

Instructor: László Babai
Scribe: Eric Patterson and Travis Schedler

1 Steiner Triple Systems

Exercise 8.1 (Puzzle). Let $A_1 \dots A_n$ be a regular n -gon inscribed in the unit circle. Prove that $\overline{A_1 A_2} \overline{A_1 A_3} \cdots \overline{A_1 A_n} = n$. Here \overline{XY} is the length of the segment from X to Y . Hint: \mathbb{C} .

Recall [Definition 5.11] that a Steiner Triple System (STS) is a 3-uniform hypergraph [Definition 5.7(a,b)] such that for any pair of points (vertices) there is exactly one line passing through them.

Recall **Exercise 5.12**: Prove that in a STS, the number of vertices n is odd.

Recall **Exercise 5.18**: If $n \equiv 1, 3 \pmod{6}$, then there exists a STS on n points. (note that **Exercise 5.13** is the converse of this statement). To get started on this, make sure to prove and use the

Lemma 8.2. *For any k , we get a STS on 3^k points from the k -dimensional SET game (i.e. with k characteristics).*

The above lemma is part of Exercise 5.15.

Definition 8.3. The finite field $\mathbb{F}_3 = \{0, 1, 2\}$ is defined by taking arithmetic modulo 3. For any k we can consider the k -dimensional \mathbb{F}_3 -vector space, $\mathbb{F}_3^k = \{(\alpha_1, \dots, \alpha_k) : \alpha_i \in \mathbb{F}_3\}$.

Definition 8.4. More generally, for any p we can define $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$, the **finite field of order p** , by taking arithmetic modulo p . We can also define the k -dimensional \mathbb{F}_p -vector space, denoted by \mathbb{F}_p^k .

Definition 8.5. For any vector space F^k (where F is any field such as $\mathbb{F}_p, \mathbb{C}, \mathbb{Q}, \mathbb{Q}[\sqrt{2}]$, etc.), we define a **linear subspace** to be a nonempty subset which is closed under addition and multiplication by scalars (elements of F). We define an **affine subspace** to be any translate of

a linear subspace (i.e. a linear subspace with origin moved to any given vector). (In particular, any linear subspace is also affine.) For any $v_1, \dots, v_j \in F^k$, we can consider the subspace

$$\text{Span}(v_1, \dots, v_s) = \left\{ \sum_{i=1}^s \alpha_i v_i : \alpha_i \in F \right\}. \quad (1)$$

We can also consider the **affine span**,

$$\text{Aff}(v_1, \dots, v_s) = \left\{ \sum_{i=1}^s \alpha_i v_i : \alpha_i \in F, \sum_{i=1}^s \alpha_i = 1 \right\}. \quad (2)$$

Note that the linear (resp. affine) span is the smallest linear (resp. affine) subspace containing the given vectors. Also note that the span of v_1, \dots, v_s is the same as the affine span of $v_1, \dots, v_s, 0$. Intuitively, the affine span is the smallest hyperplane of any dimension (not necessarily passing through the origin) containing the given vectors, and the linear span is the smallest hyperplane of any dimension which passes through 0 and contains the given vectors.

Observation 8.6. Note that if \mathcal{T} is an affine subspace, and $v \in \mathcal{T}$, then $\mathcal{T} = \mathcal{U} + v$ where \mathcal{U} is a linear subspace. Also, \mathcal{U} is independent of the choice of v .

Definition 8.7. If \mathcal{T} is an affine subspace $\mathcal{T} = v + \mathcal{U}$ where \mathcal{U} is a linear subspace, then we define $\dim(\mathcal{T}) = \dim(\mathcal{U}) =$ the maximum number of linearly independent vectors in \mathcal{U} .

Now we will consider some enumerative geometry over finite fields \mathbb{F}_p .

Exercise 8.8. First of all, show that $|\mathbb{F}_p^k| = p^k$.

Exercise 8.9. Prove that, for all $x \neq y \in \mathbb{F}_p^k$, there exists a unique line through x, y , namely $\text{Aff}(x, y)$. (A line is by definition a set $\{v + tw\}_{t \in \mathbb{F}_p}$, for a fixed choice of $v, w \in \mathbb{F}_p^k$.)

Exercise 8.10. Show that the total number of lines in \mathbb{F}_p^k is

$$\frac{\binom{p^k}{2}}{\binom{p}{2}} = \frac{p^k(p^k - 1)/2}{p(p - 1)/2} = \frac{p^k(p^k - 1)}{p(p - 1)}. \quad (3)$$

Exercise 8.11. Show that the total number of planes (i.e. two-dimensional affine subspaces) in \mathbb{F}_p^k is

$$\frac{p^k(p^k - 1)(p^k - p)}{p^2(p^2 - 1)(p^2 - p)}. \quad (4)$$

Definition 8.12. For any k and p , we define $AG(k, p)$ (“affine geometry”) to be the set \mathbb{F}_p^k with its affine lines, planes, etc.

Exercise 8.13. Verify that the “set” cards form the space $AG(4, 3)$, where the SETs are affine lines. (cf. Lecture 5, 6/25/04)

Exercise 8.14. Verify that the SET game $AG(k, 3)$ gives an STS for $n = 3^k$.

For the relevant definition of projective space and the Fundamental Theorem of Projective Geometry, see the *Linear Algebra Methods in Combinatorics* handout, pages 49 and 50.

Theorem 8.15 (Galois). *A finite field of order n exists iff $n = p^k$.*

Consequence 8.16. *If $n = p^k$, then there is a projective plane of order n .*

Puzzle 8.17 (Euler's 36 Officers Problem). Given n^2 officers with n ranks and n divisions such that no officers have the same rank and division, put the officers in a $n \times n$ grid so that neither rank nor division occurs twice in any row or column. It can be done for any prime power p but not for 6.

Exercise 8.18. Prove that the impossibility of Euler's 36 officers problem implies the nonexistence of a projective plane of order 6.