1 Two similar problems

**Eventown Problem**: All clubs must have even cardinality, their pairwise intersection must be even as well, and no two clubs can have the same members: we want distinct subsets $S_1, \ldots, S_m \subseteq [n]$ such that

$$|S_i| \text{ is even for all } i$$

$$|S_i \cap S_j| \text{ is even for all } i \neq j$$

What is the maximum number $m = m(n)$ of such subsets?

**Exercise 1.** Show that in Eventown there can be $2^\lfloor n/2 \rfloor$ such subsets.

**Oddtown Problem**: All clubs must have even cardinality, their pairwise intersection must be odd, and no two clubs can have the same members: we want distinct subsets $S_1, \ldots, S_m \subseteq [n]$ such that

$$|S_i| \text{ is odd for all } i$$

$$|S_i \cap S_j| \text{ is even for all } i \neq j$$


What is the maximum number \( m = m(n) \) of such subsets?

**Exercise 2.** Show that in Oddtown there can be \( n \) such subsets.

The bound for Oddtown in Exercise 2 cannot be improved (next section). These problems are not so similar!

For \( n = 32 \) we can have \( 2^{16} = 65,536 \) clubs in Eventown, but only 32 in Oddtown.

### 1.1 Solution to Oddtown

We show that in Oddtown the **exact bound** is \(^1\)

\[ m(n) = n \]

We can break the proof into three steps:

| Step 1: Each subset is a 0/1 vector |
|---|---|
| Think of every \( S_i \) as a 0/1-vector \( v_i \) of length \( n \). Oddtown rules (13-14) can be expressed in terms of inner product of these vectors |
| \( v_i \cdot v_i = 1 \mod 2 \) for every \( i \) \hspace{1cm} (5) |
| \( v_i \cdot v_j = 0 \mod 2 \) for every \( i \neq j \). \hspace{1cm} (6) |

| Step 2: These vectors are linearly independent |
|---|---|
| These two conditions (5-6) imply that the vectors are linearly independent (proof below), meaning that |
| \( \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m = 0 \iff \lambda_1 = \cdots = \lambda_m = 0 \) \hspace{1cm} (7) |
| (Here \( \lambda_i \in \{0, 1\} \), \( \lambda_i v_i \) is the scalar multiplication, and the sum is \( \mod 2 \).) |

| Step 3: The linear algebra bound implies \( m \leq n \) |
|---|---|
| A “Magic Theorem” in linear algebra (Theorem 1 below) says that, if \( m \) vectors \( v_1, \ldots, v_m \) are linearly independent, then \( m \leq n \) (where \( n \) is the length of the vectors). |

\(^1\)Exercise 2 says that \( m(n) \geq n \). Here we show \( m(n) \leq n \).
1.1.1 Linear independence

The only missing part is the linear independence (7) of these vectors. Note that the “⇐” direction is trivial, so we only prove “⇒”:

\[(\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m) \cdot v_1 = \lambda_1 v_1 \cdot v_1 + \lambda_2 v_1 \cdot v_2 + \cdots + \lambda_m v_1 \cdot v_m \]

\[(6) \lambda_1 v_1 \cdot v_1 = \lambda_1 \]

Since \(0 \cdot v_1 = 0\) we conclude that \(\lambda_1 = 0\). If we start with some \(v_i\) in place of \(v_1\) we obtain \(\lambda_i = 0\). So, we get \(\lambda_1 = \cdots = \lambda_m = 0\) which proves “⇒”.

2 A geometric problem (next lecture)

Points with only one distance: Find points in \(\mathbb{R}^n\) whose pairwise distances are all the same. We want \(s_1, \ldots, s_m \in \mathbb{R}^n\) such that

\[d(s_i, s_i) = 0 \quad \text{for every } i \quad \text{(obvious)} \quad (8)\]

\[d(s_i, s_j) = 1 \quad \text{for every } i \neq j \quad (9)\]

What is the maximum number \(m = m(n)\) of such points?

\[
\begin{array}{cccc}
\text{n = 2} & \text{n = 3} & \cdots \\
\text{3 points} & \text{4 points} & \\
\end{array}
\]

An approach similar to oddtown (linear algebra bound)

Consider

\[F(x, y) \triangleq 1 - d(x, y)\]

and observe that for \(f_i(y) \triangleq F(s_i, y)\) we have

\[f_i(s_i) \neq 0 \quad \text{for every } i \quad (10)\]

\[f_i(s_j) = 0 \quad \text{for every } i \neq j \quad (11)\]
Can we use **functions** instead of vectors?

We want to write things like

\[ f + g \quad \text{addition} \]
\[ \lambda f \quad \text{scalar multiplication} \]
\[ \lambda_1 f_1 + \cdots + \lambda_m f_m \quad \text{linear combination, independence} \]

## 3 A bit of linear algebra

In the sequel \( \mathbb{F} \) is a **field**. Some examples first:

- \( \mathbb{Q} \) – rationals with standard addition \((a + b)\) and multiplication \((ab)\)
- \( \mathbb{R} \) – reals with same operations
- \( \mathbb{F}_2 = \mathbb{Z}_2 \) – set \( \{0, 1\} \) with addition \((a + b \mod 2)\) and multiplication \((ab \mod 2)\)
- \( \mathbb{F}_p = \mathbb{Z}_p \) – field with \( p \) elements, with \( p \) prime, that is the
  - set \( \{0, \ldots, p - 1\} \) with “mod \( p \)” addition and multiplication
- \( \mathbb{F}_q \) – field with \( q = p^k \) elements, with \( p \) prime and \( k \geq 0 \) integer

### Field (informal)

**addition** \((a + b)\)

- associative, commutative, identity “0”, inverse “\(-a\)”

**multiplication** \((ab)\)

- associative, commutative, identity “1”, inverse “\(a^{-1}\)”
  (except for \(a = 0\))

**distributive law:** the usual one...\(a(b + c) = ab + ac\)

The symbol \( \mathbb{F}^n \) indicates the **vector space** consisting of all vectors of length \( n \). For vectors \( u, v \) in \( \mathbb{F}^n \) and for \( \lambda \in \mathbb{F} \), we have the usual “component-wise”

**addition:** \( u + v \triangleq (u_1 + v_1, \ldots, u_n + v_n) \)

**scalar multiplication:** \( \lambda u \triangleq (\lambda u_1, \ldots, \lambda u_n) \)
In Oddtown $\mathbb{F} = \mathbb{F}_2$ the field of two elements (or the field $\mathbb{Z}_2$).
Define “addition” and “scalar multiplication” of functions:

For two functions $f, g : \Omega \to \mathbb{F}$ we define

- addition $f + g$ \( (f + g)(x) \overset{\Delta}{=} f(x) + g(x) \)
- scalar multiplication $\lambda f$: \( (\lambda f)(x) \overset{\Delta}{=} (\lambda)(f(x)) \)

The sum of functions and the scalar multiplication are again functions. If we start with “simple” functions, then we also get “simple” functions.

**Linear Space (informal)**

**addition** vector + vector = vector
- associative, commutative, identity “0”, inverse “−v”

**scalar multiplication** (scalar)(vector) = vector
- “associative”: \((\lambda \lambda')(v) = \lambda(\lambda'v)\), “identity”: \(1v = v\),

**distributive law:**
- \(\lambda(v + v') = \lambda v + \lambda v'\) and \((\lambda + \lambda')v = \lambda v + \lambda'v\)

**Vectors.** Any vector \(v = (v_1, \ldots, v_n) \in \mathbb{F}^n\) can be regarded as a function from \(\Omega = \{1, \ldots, n\}\).

**Polynomials (in one variable) of degree 2.** These are the functions $f : \mathbb{F} \to \mathbb{F}$ of the form

$$f(x) = a_0 + a_1x + a_2x^2$$

where $a_i \in \mathbb{F}$. (You can replace “degree 2” by “degree $d'$”.)

**Polynomials (in 2 variables) of degree 2.** These are the functions $f : \mathbb{F}^2 \to \mathbb{F}$ that can be written as

$$f(x_1, x_2) = a_0 + a_1x_1 + a_2x_2 + a_3x_1x_2 + a_4x_1^2 + a_5x_2^2$$

where $a_i \in \mathbb{F}$. (Generalize: $m$ variables of degree $d$.)
All of these (and others) fall into this definition:

<table>
<thead>
<tr>
<th>Linear Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>A linear space over ( F ) is a set ( V ) with addition “( u + v )” and scalar multiplication “( \lambda u )” satisfying</td>
</tr>
<tr>
<td>(A1) ( v + w \in V ) for all ( v, w \in V )</td>
</tr>
<tr>
<td>(A2) ( (v + w) + z = v + (w + z) ) for all ( v, w, z \in V )</td>
</tr>
<tr>
<td>(A3) ( v + w = w + v ) for all ( v, w \in V )</td>
</tr>
<tr>
<td>(A4) There exists ( 0 \in V ) such that ( 0 + v = v ) for all ( v \in V )</td>
</tr>
<tr>
<td>(A5) For every ( v \in V ) there exists ( (-v) \in V ) such that ( v + (-v) = 0 )</td>
</tr>
<tr>
<td>(M1) ( \lambda v \in V ) for all ( \lambda \in F ) and ( v \in V )</td>
</tr>
<tr>
<td>(M2) ( 1v = v ) for every ( v \in V )</td>
</tr>
<tr>
<td>(D1) ( \lambda(\mu)v = \lambda(\mu)v ) for all ( \lambda, \mu \in F ) and ( v \in V )</td>
</tr>
<tr>
<td>(D2) ( \lambda(v + w) = \lambda v + \lambda w ) for all ( \lambda \in F ) and ( v, w \in V )</td>
</tr>
<tr>
<td>(D3) ( \lambda(\mu)v = \lambda v + \mu v ) for all ( \lambda, \mu \in F ) and ( v \in V )</td>
</tr>
</tbody>
</table>

We say that \( v_1, \ldots, v_m \in V \) are linearly independent (over \( F \)) if

\[
\lambda_1 v_1 + \cdots + \lambda_m v_m = 0 \quad (\lambda_i \in F) \tag{12}
\]

implies \( \lambda_1 = \cdots = \lambda_m = 0 \), and they are linearly dependent otherwise.

**Remark 1.** When \( v_1, \ldots, v_m : \Omega \to F \) are functions, then \( 0 \) denotes the function that is identically equal to \( 0 \in F \) (the “constant 0”). The identity in (12) means that \( \lambda_1 v_1(x) + \cdots + \lambda_m v_m(x) = 0 \) for all \( x \in \Omega \).

This is the “Magic Theorem” mentioned during the lecture:

<table>
<thead>
<tr>
<th>Linear Algebra Bound (only for vectors)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Theorem 1.</strong> If ( v_1, \ldots, v_m \in \mathbb{F}^n ) are linearly independent then ( m \leq n ).</td>
</tr>
</tbody>
</table>
This is the analogue for polynomials (instead of vectors).

### Linear Algebra Bound (only for polynomials)

**Theorem 2.** If \( f_1, \ldots, f_m : \mathbb{R} \to \mathbb{R} \) are polynomials in one variable of degree at most \( d \) and they are linearly independent, then \( m \leq d + 1 \).

We prove Theorems 1 and 2 in the next lecture (actually a generalization of both that will be useful for all of our problems).

**Remark 2** (Solve the geometric problem). *The natural approach to solve the geometric problem in Section 2 is to show that (1) the functions \( f_i \) in (10)-(11) are polynomials of degree at most \( n \), (2) they are linearly independent, and (3) then apply this theorem to conclude \( m \leq n + 1 \). This is the right idea for the proof but unfortunately the first step is “wrong” (that functions use more than one variable...we see this in the next lecture).*

### 3.1 Two curious facts about...“the right field”

Look at these three vectors:

- **dependent over \( \mathbb{F}_2 \)**
  \[
  \begin{pmatrix}
  0 \\ 1 \\ 1 \\
  \end{pmatrix}
  \begin{pmatrix}
  1 \\ 0 \\ 1 \\
  \end{pmatrix}
  \begin{pmatrix}
  1 \\ 1 \\ 0 \\
  \end{pmatrix}
  \]

- **independent over \( \mathbb{F}_3 \)**

If we work over the field \( \mathbb{F}_2 \) (“ mod 2 operations”) then they are linearly dependent:

\[
\begin{pmatrix}
  0 \\
  1 \\
  1 \\
\end{pmatrix}
+ \begin{pmatrix}
  1 \\
  0 \\
  1 \\
\end{pmatrix}
+ \begin{pmatrix}
  1 \\
  1 \\
  0 \\
\end{pmatrix}
= \begin{pmatrix}
  0 \\
  0 \\
  0 \\
\end{pmatrix}
\]

If we work over the field \( \mathbb{F}_3 \) (“ mod 3 operations”) then they are linearly independent:

\[
\lambda_1 \begin{pmatrix}
  0 \\
  1 \\
  1 \\
\end{pmatrix}
+ \lambda_2 \begin{pmatrix}
  1 \\
  0 \\
  1 \\
\end{pmatrix}
+ \lambda_3 \begin{pmatrix}
  1 \\
  1 \\
  0 \\
\end{pmatrix}
= \begin{pmatrix}
  0 \\
  0 \\
  0 \\
\end{pmatrix}
\]
This system implies that $\lambda_1 = \lambda_2 = \lambda_3$ (look for instance at the first two coordinates of the vectors). But then the only possible value is $\lambda_i = 0$ (try with $\lambda_i = 1, 2$ and check that the equality does not hold).

The underlying field $\mathbb{F}$ is important for (in)dependence. The field $\mathbb{F}_3$ is useful to prove the “mod-3-town” variant of Oddtown (replace “mod 2” with “mod 3” in the definition – see Exercise 5), but when we go to the “mod-4-town”... strange things happen:

$$2 \cdot 2 = 0 \mod 4$$

**Exercise 3.** Try the following: replace “mod 2” by “mod 4” in (5)-(6) and try to “replicate” the proof of “linear independence”. Explain why we cannot conclude that $\lambda_1 = 0$ from “$\lambda_1 v_1 \cdot v_1 = 0$”.

$\mathbb{Z}_4$ is not a field.

### 4 What to remember and where to look

Keep in mind the “three-steps” used to solve Oddtown and that we may want to use the same three steps (with some adaptation) to solve other problems. There are two things that can be changed and still we can talk about linear independence:

- We can replace vectors by functions (e.g., polynomials);
- The underlying field (what are the “numbers” – our building blocks).

During the exercise class we have solved Exercise 5, “mod-4-town” (see Exercise 7), and an analogous “mod-6-town”. Finally

- The nice story about Eventown vs Oddtown and the proof are in [BF92, Section 1.1].
- The two-distance set problem is in [BF92, Section 1.2].
- The definitions of linear space, liner combination, span, etc. can be found in [BF92, Section 2.1.3].

We shall see a bit more about linear algebra in the following lectures. If you are curious/interested, you can have a look at [Cur90, Chapter 1.A].
References


A Exercises

The “Exercise Set 1” in the webpage contains exactly the exercises marked with “∗”.

Exercise (*) 4. Consider the “Reversed Oddtown” problem that is the variant of Oddtown in which we swap “odd” with “even”: we want $S_1, \ldots, S_m \subseteq [n]$ such that

\begin{align}
|S_i| & \text{ is even for all } i \\
|S_i \cap S_j| & \text{ is odd for all } i \neq j
\end{align}

(13) (14)

Show how the result of Oddtown implies $m \leq n + 1$ for this problem.

Exercise 5. Consider the following variant of Oddtown: we want $S_1, \ldots, S_m \subseteq [n]$ such that

\begin{align}
|S_i| & \neq 0 \mod 3 \quad \text{for every } i \\
|S_i \cap S_j| & = 0 \mod 3 \quad \text{for every } i \neq j.
\end{align}

(15) (16)

Prove that $m \leq n$. Prove the same result for the version in which “mod 3” is replaced by “mod $p$” with $p$ be any prime.

Exercise 6. Prove that the vectors of Oddtown are linearly independent over $\mathbb{Q}$. (Hint: Observe that if

$$\lambda_1 v_1 + \cdots + \lambda_m v_m = 0$$

then the same holds if we multiply the coefficients by any scalar $\mu$, that is

$$\mu \lambda_1 v_1 + \cdots + \mu \lambda_m v_m = 0.$$ 

Use this trick to show that you can always construct another linear combination where all coefficients $\lambda_i$ are integers and at least one of them is not divisible by 2. Finally, prove that in Oddtown the coefficients must be all even if they are integer – here you can use the idea of the proof seen in the exercise class to solve “mod-4-town”.

Exercise (*) 7. Call mod-$p^k$-town the variant of Oddtown in which “mod 2” is replaced by “mod $p^k$” for prime $p$ and positive integer $k$. Show that in this variant $m(n) \leq n$. (Hint: show linear independence over $\mathbb{Q}$ by adapting the solution of mod-4-town seen in the exercise class – you can also use the idea of Exercise 6.)
Exercise (*) 8. Construct a solution for the “mod-4-town” problem in Exercise 7 such that the corresponding incidence vectors are linearly dependent over $\mathbb{F}_2$.

Exercise (*) 9. Consider these two polynomials in one variable

\[ f_1(x) = x^2 \quad \text{and} \quad f_2(x) = 1 - 2x \]

over the field $\mathbb{R}$. Show that they are linearly independent. (Hint: look at these two “special” values $s_1 = 1/2$ and $s_2 = 0$ and write down the conditions for $f_i(s_j)$; then look at the linear combination.)

Exercise (*) 10. In this exercise we consider functions that are polynomials over the reals of degree at most $d$. In particular, we have $f_1, \ldots, f_m : \mathbb{R} \to \mathbb{R}$ and these polynomials satisfy the following additional condition: there are numbers $s_1, \ldots, s_m \in \mathbb{R}$ such that

\[ f_i(s_i) \neq 0 \quad \text{for every } i \tag{17} \]
\[ f_i(s_j) = 0 \quad \text{for every } i \neq j. \tag{18} \]

Prove that these polynomials are at most $d + 1$ using Theorem 2 in the lecture notes. (Hint: you may try first with $m = 2$ and look back at the solution of the previous exercise.)