Linear Algebra and Finite Sets

October 1, 2011

A curious example

Question (Even teams)

How many different teams can be formed from students in a class with $2n$ students subject to the following two conditions:

1. *Each team must have an even number of students.*
2. *Each two teams must have an even number of students in common.*

A curious example

Question (Even teams)

How many different teams can be formed from students in a class with $2n$ students subject to the following two conditions:

1. *Each team must have an even number of students.*
2. *Each two teams must have an even number of students in common.*

Question (Odd teams)

Let us modify this question slightly:

1. *Each team must have an odd number of students.*
2. *Each two teams must have an even number of students in common.*

Answer

Answer

1. *We can form n pairs of students. Each subset of the n pairs can form a team. Clearly, each team will have an even number of students and each two teams will have an even number of students in common. The total number of teams is* 2^n*, so if for instance, there are only 40 students in the class, we can form* 2^{20} *teams which is more than* $1,000,000$ *teams.*

Answer

Answer

1. *We can form n pairs of students. Each subset of the n pairs can form a team. Clearly, each team will have an even number of students and each two teams will have an even number of students in common. The total number of teams is* 2^n*, so if for instance, there are only 40 students in the class, we can form* 2^{20} *teams which is more than* $1,000,000$ *teams.*
2. *For the "odd" case, we can form 2n teams (each team will have 1 student). Another way, each team has* $2n-1$ *students, again we can form 2n teams. In case we have 40 students in class, we can form "only" 40 teams subject to the "odd" condition.*

Answer

Answer

1. *We can form n pairs of students. Each subset of the n pairs can form a team. Clearly, each team will have an even number of students and each two teams will have an even number of students in common. The total number of teams is* 2^n*, so if for instance, there are only 40 students in the class, we can form* 2^{20} *teams which is more than* $1,000,000$ *teams.*
2. *For the "odd" case, we can form 2n teams (each team will have 1 student). Another way, each team has* $2n-1$ *students, again we can form 2n teams. In case we have 40 students in class, we can form "only" 40 teams subject to the "odd" condition.*
3. *Is 2n the maximum number of teams that can be formed?*

Answer

Answer

1. *We can form n pairs of students. Each subset of the n pairs can form a team. Clearly, each team will have an even number of students and each two teams will have an even number of students in common. The total number of teams is* 2^n*, so if for instance, there are only 40 students in the class, we can form* 2^{20} *teams which is more than* $1,000,000$ *teams.*
2. *For the "odd" case, we can form 2n teams (each team will have 1 student). Another way, each team has* $2n-1$ *students, again we can form 2n teams. In case we have 40 students in class, we can form "only" 40 teams subject to the "odd" condition.*
3. *Is 2n the maximum number of teams that can be formed? How about* 2^n *teams? Is this the largest number of teams?*

Answer

Answer

1. *We can form n pairs of students. Each subset of the n pairs can form a team. Clearly, each team will have an even number of students and each two teams will have an even number of students in common. The total number of teams is* 2^n*, so if for instance, there are only 40 students in the class, we can form* 2^{20} *teams which is more than* $1,000,000$ *teams.*
2. *For the "odd" case, we can form 2n teams (each team will have 1 student). Another way, each team has* $2n-1$ *students, again we can form 2n teams. In case we have 40 students in class, we can form "only" 40 teams subject to the "odd" condition.*
3. *Is 2n the maximum number of teams that can be formed? How about* 2^n *teams? Is this the largest number of teams?*
4. *Is there an explanation for the discrepancy between the "even" and "odd" class?*

Linear Algebra to the recsue

Theorem (Odd teams)

The maximum number of odd teams from a class with 2n students, such that every pair of teams have an even number of students in common is 2n.

Linear Algebra to the recsue

Theorem (Odd teams)

The maximum number of odd teams from a class with $2n$ students, such that every pair of teams have an even number of students in common is $2n$.

Before we give a proof of this theorem we recall some fundamental facts about matrices.

Linear Algebra to the recsue

Theorem (Odd teams)

The maximum number of odd teams from a class with $2n$ students, such that every pair of teams have an even number of students in common is $2n$.

Before we give a proof of this theorem we recall some fundamental facts about matrices.

1. The rank of an $m \times n$ matrix is the number of linearly independent rows (columns).

Linear Algebra to the recsue

Theorem (Odd teams)

The maximum number of odd teams from a class with 2n students, such that every pair of teams have an even number of students in common is 2n.

Before we give a proof of this theorem we recall some fundamental facts about matrices.

1. The rank of an $m \times n$ matrix is the number of linearly independent rows (columns).
2. $M \times M^{tr}$ is a square matrix.

Linear Algebra to the recsue

Theorem (Odd teams)

The maximum number of odd teams from a class with 2n students, such that every pair of teams have an even number of students in common is 2n.

Before we give a proof of this theorem we recall some fundamental facts about matrices.

1. The rank of an $m \times n$ matrix is the number of linearly independent rows (columns).
2. $M \times M^{tr}$ is a square matrix.
3. $rank(M \times N) \leq \; min\{rank(M), rank(N)\}$

Linear Algebra to the recsue

Theorem (Odd teams)

The maximum number of odd teams from a class with 2n students, such that every pair of teams have an even number of students in common is 2n.

Before we give a proof of this theorem we recall some fundamental facts about matrices.

1. The rank of an $m \times n$ matrix is the number of linearly independent rows (columns).
2. $M \times M^{tr}$ is a square matrix.
3. $rank(M \times N) \leq \ min\{rank(M), rank(N)\}$
4. If M is an $n \times n$ matrix (a square matrix) then $rank(M) = n$ if and only if $Det(M) \neq 0$.

The Proof

Proof.

- Let $T_1, T_2, \ldots, T_k$ be k teams each with an odd number of students. Let t_i be the incidence vector coresponding to team T_i that is $t_i \in R^{2n}$.

The Proof

Proof.

- Let $T_1, T_2, \ldots, T_k$ be k teams each with an odd number of students. Let t_i be the incidence vector coresponding to team T_i that is $t_i \in R^{2n}$.
- We form the $k \times 2n$ matrix M as follows: $M_i = t_i$.

The Proof

Proof.

- Let $T_1, T_2, \ldots, T_k$ be k teams each with an odd number of students. Let t_i be the incidence vector coresponding to team T_i that is $t_i \in R^{2n}$.
- We form the $k \times 2n$ matrix M as follows: $M_i = t_i$.
- We note that $rank(M) \leq 2n$.

The Proof

Proof.

- Let $T_1, T_2, \ldots, T_k$ be k teams each with an odd number of students. Let t_i be the incidence vector coresponding to team T_i that is $t_i \in R^{2n}$.
- We form the $k \times 2n$ matrix M as follows: $M_i = t_i$.
- We note that $rank(M) \leq 2n$.
- Hence $M \times M^{tr}$ is a square matrix of order k and $rank(M \times M^{tr}) \leq 2n$.

The Proof

Proof.

- Let $T_1, T_2, \ldots, T_k$ be k teams each with an odd number of students. Let t_i be the incidence vector coresponding to team T_i that is $t_i \in R^{2n}$.
- We form the $k \times 2n$ matrix M as follows: $M_i = t_i$.
- We note that $rank(M) \leq 2n$.
- Hence $M \times M^{tr}$ is a square matrix of order k and $rank(M \times M^{tr}) \leq 2n$.
- If $k > 2n$ then $Det(M \times M^{tr}) = 0$.

The Proof

Proof.

- Let $T_1, T_2, \ldots, T_k$ be k teams each with an odd number of students. Let t_i be the incidence vector coresponding to team T_i that is $t_i \in R^{2n}$.
- We form the $k \times 2n$ matrix M as follows: $M_i = t_i$.
- We note that $rank(M) \leq 2n$.
- Hence $M \times M^{tr}$ is a square matrix of order k and $rank(M \times M^{tr}) \leq 2n$.
- If $k > 2n$ then $Det(M \times M^{tr}) = 0$.
- If $Det(A) = 0$ *then* $Det(A) \pmod 2 = 0$.

The Proof

Proof.

- Let $T_1, T_2, \ldots, T_k$ be k teams each with an odd number of students. Let t_i be the incidence vector coresponding to team T_i that is $t_i \in R^{2n}$.
- We form the $k \times 2n$ matrix M as follows: $M_i = t_i$.
- We note that $rank(M) \leq 2n$.
- Hence $M \times M^{tr}$ is a square matrix of order k and $rank(M \times M^{tr}) \leq 2n$.
- If $k > 2n$ then $Det(M \times M^{tr}) = 0$.
- If $Det(A) = 0 \ then \ Det(A) \pmod 2 = 0$.
- We note that $< t_i, t_j >= 0 \pmod 2$ if $i \neq j \quad and \quad < t_i, t_i >= 1 \pmod 2$.

The Proof

Proof.

- Let $T_1, T_2, \ldots, T_k$ be k teams each with an odd number of students. Let t_i be the incidence vector coresponding to team T_i that is $t_i \in R^{2n}$.
- We form the $k \times 2n$ matrix M as follows: $M_i = t_i$.
- We note that $rank(M) \leq 2n$.
- Hence $M \times M^{tr}$ is a square matrix of order k and $rank(M \times M^{tr}) \leq 2n$.
- If $k > 2n$ then $Det(M \times M^{tr}) = 0$.
- If $Det(A) = 0 \ then \ Det(A) \pmod 2 = 0$.
- We note that $< t_i, t_j >= 0 \pmod 2$ if $i \neq j \quad and \quad < t_i, t_i >= 1 \pmod 2$.
- But this means that $Det(M \times M^{tr}) \pmod 2 = 1$ a contradiction.

The Proof

Proof.

- Let $T_1, T_2, \ldots, T_k$ be k teams each with an odd number of students. Let t_i be the incidence vector coresponding to team T_i that is $t_i \in R^{2n}$.
- We form the $k \times 2n$ matrix M as follows: $M_i = t_i$.
- We note that $rank(M) \leq 2n$.
- Hence $M \times M^{tr}$ is a square matrix of order k and $rank(M \times M^{tr}) \leq 2n$.
- If $k > 2n$ then $Det(M \times M^{tr}) = 0$.
- If $Det(A) = 0$ *then* $Det(A) \pmod 2 = 0$.
- We note that $< t_i, t_j >= 0 \pmod 2$ if $i \neq j$ *and* $< t_i, t_i >= 1 \pmod 2$.
- But this means that $Det(M \times M^{tr}) \pmod 2 = 1$ a contradiction. **Conclusion:** $k \leq 2n$.

Fields

Definition

A **field** $\{F, +, \cdot\}$ *is a set together with two operations, usually called addition and multiplication, and denoted by* $+$ *and* $\cdot$ *respectively, such that the following axioms hold:*

1. $\{F, +\}$ *is a commutative group,* 0 *is the additive identity.*
2. $\{F \setminus \{0\}, \cdot\}$ *is a commutative group,* 1 *is the multiplicative identity.*
3. *The ditributive law holds:* $a \cdot (b + c) = a \cdot b + a \cdot c$.

Fields

Definition

A **field** $\{F, +, \cdot\}$ *is a set together with two operations, usually called addition and multiplication, and denoted by* $+$ *and* $\cdot$ *respectively, such that the following axioms hold:*

1. $\{F, +\}$ *is a commutative group,* 0 *is the additive identity.*
2. $\{F \setminus \{0\}, \cdot\}$ *is a commutative group,* 1 *is the multiplicative identity.*
3. *The ditributive law holds:* $a \cdot (b + c) = a \cdot b + a \cdot c$*.*

Example

The four most common fields are:

1. R*, the real numbers.*

Fields

Definition

A **field** $\{F, +, \cdot\}$ *is a set together with two operations, usually called addition and multiplication, and denoted by* $+$ *and* $\cdot$ *respectively, such that the following axioms hold:*

1. $\{F, +\}$ *is a commutative group,* 0 *is the additive identity.*
2. $\{F \setminus \{0\}, \cdot\}$ *is a commutative group,* 1 *is the multiplicative identity.*
3. *The ditributive law holds:* $a \cdot (b + c) = a \cdot b + a \cdot c$.

Example

The four most common fields are:

1. R*, the real numbers.*
2. Q*, the rational numbers.*

Fields

Definition

A **field** $\{F, +, \cdot\}$ *is a set together with two operations, usually called addition and multiplication, and denoted by* $+$ *and* $\cdot$ *respectively, such that the following axioms hold:*

1. $\{F, +\}$ *is a commutative group,* 0 *is the additive identity.*
2. $\{F \setminus \{0\}, \cdot\}$ *is a commutative group,* 1 *is the multiplicative identity.*
3. *The ditributive law holds:* $a \cdot (b + c) = a \cdot b + a \cdot c$.

Example

The four most common fields are:

1. R, *the real numbers.*
2. Q, *the rational numbers.*
3. C, *the complex numbers.*

Fields

Definition

A **field** $\{F, +, \cdot\}$ *is a set together with two operations, usually called addition and multiplication, and denoted by* $+$ *and* $\cdot$ *respectively, such that the following axioms hold:*

1. $\{F, +\}$ *is a commutative group,* 0 *is the additive identity.*
2. $\{F \setminus \{0\}, \cdot\}$ *is a commutative group,* 1 *is the multiplicative identity.*
3. *The ditributive law holds:* $a \cdot (b + c) = a \cdot b + a \cdot c$.

Example

The four most common fields are:

1. R*, the real numbers.*
2. Q*, the rational numbers.*
3. C*, the complex numbers.*
4. $GF(q)$ *finite fields of order* q.

Finite Fields

Finite fields play a very central role in communication security. Finite fields have the following properties:

Finite Fields

Finite fields play a very central role in communication security.
Finite fields have the following properties:

1. The order of a finite field is p^n for some prime p.

Finite Fields

Finite fields play a very central role in communication security.
Finite fields have the following properties:

1. The order of a finite field is p^n for some prime p.
2. For every prime p and positive integer n there is a unique (upto isomorphism) finite field of order $q = p^n$, denoted by $GF(q)$ named after the French mathematician Everist Galois.

Finite Fields

Finite fields play a very central role in communication security. Finite fields have the following properties:

1. The order of a finite field is p^n for some prime p.
2. For every prime p and positive integer n there is a unique (upto isomorphism) finite field of order $q = p^n$, denoted by $GF(q)$ named after the French mathematician Everist Galois.

Example

- $GF(2) = \{0, 1\}$ *with* $1 + 1 = 0$.

Finite Fields

Finite fields play a very central role in communication security.
Finite fields have the following properties:

1. The order of a finite field is p^n for some prime p.
2. For every prime p and positive integer n there is a unique (upto isomorphism) finite field of order $q = p^n$, denoted by $GF(q)$ named after the French mathematician Everist Galois.

Example

- $GF(2) = \{0, 1\}$ *with* $1 + 1 = 0$.
- $GF(p) = \{0, 1, \ldots, p - 1\}$, *where all arithmetic operations are done mod p.*

Finite Fields

Finite fields play a very central role in communication security. Finite fields have the following properties:

1. The order of a finite field is p^n for some prime p.
2. For every prime p and positive integer n there is a unique (upto isomorphism) finite field of order $q = p^n$, denoted by $GF(q)$ named after the French mathematician Everist Galois.

Example

- $GF(2) = \{0, 1\}$ *with* $1 + 1 = 0$.
- $GF(p) = \{0, 1, \ldots, p - 1\}$, *where all arithmetic operations are done mod p.*
- $GF(2^2) = \{0, 1, \alpha, 1 + \alpha\}$, *where* $\alpha + \alpha = 0, 1 + 1 = 0, \alpha \cdot \alpha = \alpha + 1$.

Vector spaces over fields

Definition

A vector space of dimension k over the field F, denoted by F^k is the set: $\{(x_1, x_2, \ldots, x_k)\}$ where $x_i \in F$ together with the following two operations:

1. $(x_1, x_2, \ldots, x_k) + (y_1, y_2, \ldots, y_k) = (x_1 + y_1, x_2 + y_2, \ldots, x_k + y_k)$
2. $\alpha(x_1, x_2, \ldots, x_k) = (\alpha \cdot x_1, \alpha \cdot x_2, \ldots, \alpha \cdot x_k)$

Vector spaces over fields

Definition

A vector space of dimension k over the field F, denoted by F^k is the set: $\{(x_1, x_2, \ldots, x_k)\}$ where $x_i \in F$ together with the following two operations:

1. $(x_1, x_2, \ldots, x_k) + (y_1, y_2, \ldots, y_k) = (x_1 + y_1, x_2 + y_2, \ldots, x_k + y_k)$
2. $\alpha(x_1, x_2, \ldots, x_k) = (\alpha \cdot x_1, \alpha \cdot x_2, \ldots, \alpha \cdot x_k)$

We shall make use of the **inner product** (also called scalar or Cartesian product of vectors) defined by:
$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >= \sum_{i=1}^{n} x_i y_i$.

Example

The 2-dimensional vector space $GF^2(5) = \{(i, j) | 0 \leq i, j \leq 4\}$.

Vector spaces over fields

Definition

A vector space of dimension k over the field F, denoted by F^k is the set: $\{(x_1, x_2, \ldots, x_k)\}$ where $x_i \in F$ together with the following two operations:

1. $(x_1, x_2, \ldots, x_k)+(y_1, y_2, \ldots, y_k) = (x_1+y_1, x_2+y_2, \ldots, x_k+y_k)$
2. $\alpha(x_1, x_2, \ldots, x_k) = (\alpha \cdot x_1, \alpha \cdot x_2, \ldots, \alpha \cdot x_k)$

We shall make use of the **inner product** (also called scalar or Cartesian product of vectors) defined by:
$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >= \sum_{i=1}^{n} x_i y_i$.

Example

The 2-dimensional vector space $GF^2(5) = \{(i, j)|0 \leq i, j \leq 4\}$.

$L = \{(x, y)|ax + by = c, \{a, b, c, x, y\} \in GF(5)$ a or b or both $\neq 0\}$ is a line in $GF^2(5)$

Vector spaces over fields

Definition

A vector space of dimension k over the field F, denoted by F^k is the set: $\{(x_1, x_2, \ldots, x_k)\}$ where $x_i \in F$ together with the following two operations:

1. $(x_1, x_2, \ldots, x_k) + (y_1, y_2, \ldots, y_k) = (x_1 + y_1, x_2 + y_2, \ldots, x_k + y_k)$
2. $\alpha(x_1, x_2, \ldots, x_k) = (\alpha \cdot x_1, \alpha \cdot x_2, \ldots, \alpha \cdot x_k)$

We shall make use of the **inner product** (also called scalar or Cartesian product of vectors) defined by:
$< (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) >= \sum_{i=1}^{n} x_i y_i$.

Example

The 2-dimensional vector space $GF^2(5) = \{(i, j) | 0 \leq i, j \leq 4\}$.

$L = \{(x, y) | ax + by = c, \{a, b, c, x, y\} \in GF(5)$ a or b or both $\neq 0\}$ is a line in $GF^2(5)$

Two lines are parallel if they do not have a point in common.

Some basic facts about vector spaces

- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is **linearly independent** if: $\sum_{i=1}^{m} \alpha_i v_i = 0 \to \alpha_i = 0$.

Some basic facts about vector spaces

- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is **linearly independent** if: $\sum_{i=1}^{m} \alpha_i v_i = 0 \rightarrow \alpha_i = 0.$
- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is a **basis** if every vector $u \in F^k$ can be expressed uniquely as a linear combination of $\{v_1, v_2, \dots v_m\} \subset F^k$: $\underline{u = \sum_{i=1}^{m} \alpha_i v_i}$

Some basic facts about vector spaces

- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is **linearly independent** if: $\sum_{i=1}^{m} \alpha_i v_i = 0 \rightarrow \alpha_i = 0$.
- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is a **basis** if every vector $u \in F^k$ can be expressed uniquely as a linear combination of $\{v_1, v_2, \dots v_m\} \subset F^k$: $u = \sum_{i=1}^{m} \alpha_i v_i$
- Let $W = \{w_1, v_2, \dots w_j\} \subset F^k$. The subspace spanned by W is the set of all linear combinations of $\{w_1, v_2, \dots w_j\}$.

Some basic facts about vector spaces

- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is **linearly independent** if: $\sum_{i=1}^{m} \alpha_i v_i = 0 \rightarrow \alpha_i = 0$.
- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is a **basis** if every vector $u \in F^k$ can be expressed uniquely as a linear combination of $\{v_1, v_2, \dots v_m\} \subset F^k$: $u = \sum_{i=1}^{m} \alpha_i v_i$
- Let $W = \{w_1, v_2, \dots w_j\} \subset F^k$. The subspace spanned by W is the set of all linear combinations of $\{w_1, v_2, \dots w_j\}$.
- If $\{v_1, v_2, \dots v_m\} \subset W \subset F^k$ is a basis then it is linearly independent.

Some basic facts about vector spaces

- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is **linearly independent** if: $\sum_{i=1}^{m} \alpha_i v_i = 0 \rightarrow \alpha_i = 0.$
- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is a **basis** if every vector $u \in F^k$ can be expressed uniquely as a linear combination of $\{v_1, v_2, \dots v_m\} \subset F^k$: $u = \sum_{i=1}^{m} \alpha_i v_i$
- Let $W = \{w_1, v_2, \dots w_j\} \subset F^k$. The subspace spanned by W is the set of all linear combinations of $\{w_1, v_2, \dots w_j\}$.
- If $\{v_1, v_2, \dots v_m\} \subset W \subset F^k$ is a basis then it is linearly independent.
- All bases have the same number of vectors (the dimension of the space).

Some basic facts about vector spaces

- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is **linearly independent** if: $\sum_{i=1}^{m} \alpha_i v_i = 0 \to \alpha_i = 0$.
- A set of vectors $\{v_1, v_2, \dots v_m\} \subset F^k$ is a **basis** if every vector $u \in F^k$ can be expressed uniquely as a linear combination of $\{v_1, v_2, \dots v_m\} \subset F^k$: $u = \sum_{i=1}^{m} \alpha_i v_i$
- Let $W = \{w_1, v_2, \dots w_j\} \subset F^k$. The subspace spanned by W is the set of all linear combinations of $\{w_1, v_2, \dots w_j\}$.
- If $\{v_1, v_2, \dots v_m\} \subset W \subset F^k$ is a basis then it is linearly independent.
- All bases have the same number of vectors (the dimension of the space).
- If $W_0 = \{w_1, w_2, \dots w_m \subset U \subset F^k\}$ is a linearly independent set and $m < dim(U)$ then we can add $dim(U) - m$ vectors to W_0 to form a basis of U.

The odd teams, revisited

Recall: if there are n students in a class and we wish to form teams such that every team has an odd number of students and each two teams have an even number of students in common then we cannot form more than n teams.

The odd teams, revisited

Recall: if there are n students in a class and we wish to form teams such that every team has an odd number of students and each two teams have an even number of students in common then we cannot form more than n teams.

Proof.

Let $\{T_1, T_2, \ldots, T_k\}$ be k teams satisfying both conditions. Let $v_1, v_2, \ldots, v_k$ be their characteristic vectors.

The odd teams, revisited

Recall: if there are n students in a class and we wish to form teams such that every team has an odd number of students and each two teams have an even number of students in common then we cannot form more than n teams.

Proof.

Let $\{T_1, T_2, \ldots, T_k\}$ be k teams satisfying both conditions. Let $v_1, v_2, \ldots, v_k$ be their characteristic vectors.
Claim: $v_1, v_2, \ldots, v_k$ is an independent set over $GF^n(2)$.

The odd teams, revisited

Recall: if there are n students in a class and we wish to form teams such that every team has an odd number of students and each two teams have an even number of students in common then we cannot form more than n teams.

Proof.

Let $\{T_1, T_2, \ldots, T_k\}$ be k teams satisfying both conditions. Let $v_1, v_2, \ldots, v_k$ be their characteristic vectors.
Claim: $v_1, v_2, \ldots, v_k$ is an independent set over $GF^n(2)$.
Indeed, assume that $\sum_{i=1}^{k} \alpha_i v_i = 0$. Note that $\alpha_i = 0$ *or* 1.

The odd teams, revisited

Recall: if there are n students in a class and we wish to form teams such that every team has an odd number of students and each two teams have an even number of students in common then we cannot form more than n teams.

Proof.

Let $\{T_1, T_2, \ldots, T_k\}$ be k teams satisfying both conditions. Let $v_1, v_2, \ldots, v_k$ be their characteristic vectors.
Claim: $v_1, v_2, \ldots, v_k$ is an independent set over $GF^n(2)$.
Indeed, assume that $\sum_{i=1}^{k} \alpha_i v_i = 0$. Note that $\alpha_i = 0$ *or* 1.
Consider the inner product $< v_j, \sum_{i=1}^{k} \alpha_i v_i > = 0$.

The odd teams, revisited

Recall: if there are n students in a class and we wish to form teams such that every team has an odd number of students and each two teams have an even number of students in common then we cannot form more than n teams.

Proof.

Let $\{T_1, T_2, \ldots, T_k\}$ be k teams satisfying both conditions. Let $v_1, v_2, \ldots, v_k$ be their characteristic vectors.
Claim: $v_1, v_2, \ldots, v_k$ is an independent set over $GF^n(2)$.
Indeed, assume that $\sum_{i=1}^k \alpha_i v_i = 0$. Note that $\alpha_i = 0$ *or* 1.
Consider the inner product $< v_j, \sum_{i=1}^k \alpha_i v_i > = 0$.
Since $T_i \cap T_j$ is even if $i \neq j$ $< v_i, v_j > = 0$

The odd teams, revisited

Recall: if there are n students in a class and we wish to form teams such that every team has an odd number of students and each two teams have an even number of students in common then we cannot form more than n teams.

Proof.

Let $\{T_1, T_2, \ldots, T_k\}$ be k teams satisfying both conditions. Let $v_1, v_2, \ldots, v_k$ be their characteristic vectors.
Claim: $v_1, v_2, \ldots, v_k$ is an independent set over $GF^n(2)$.
Indeed, assume that $\sum_{i=1}^{k} \alpha_i v_i = 0$. Note that $\alpha_i = 0$ *or* 1.
Consider the inner product $< v_j, \sum_{i=1}^{k} \alpha_i v_i > = 0$.
Since $T_i \cap T_j$ is even if $i \neq j$ $< v_i, v_j > = 0$
Therefore $< v_j, \sum_{i=1}^{k} \alpha_i v_i >= \alpha_j < v_j, v_j > = 0$

The odd teams, revisited

Recall: if there are n students in a class and we wish to form teams such that every team has an odd number of students and each two teams have an even number of students in common then we cannot form more than n teams.

Proof.

Let $\{T_1, T_2, \ldots, T_k\}$ be k teams satisfying both conditions. Let $v_1, v_2, \ldots, v_k$ be their characteristic vectors.
Claim: $v_1, v_2, \ldots, v_k$ is an independent set over $GF^n(2)$.
Indeed, assume that $\sum_{i=1}^{k} \alpha_i v_i = 0$. Note that $\alpha_i = 0$ *or* 1.
Consider the inner product $< v_j, \sum_{i=1}^{k} \alpha_i v_i > = 0$.
Since $T_i \cap T_j$ is even if $i \neq j$ $< v_i, v_j > = 0$
Therefore $< v_j, \sum_{i=1}^{k} \alpha_i v_i >= \alpha_j < v_j, v_j > = 0$ But $< v_j, v_j > = 1$ so $\alpha_j = 0$ or $k \leq n$. □

Why give multiple proofs?

Question

Why did we give two proofs for the odd teams problem?

Why give multiple proofs?

Question

Why did we give two proofs for the odd teams problem?
A theorem is true or false. If it is true, one proof should suffice, so why bother with a second proof?

Why give multiple proofs?

Question

Why did we give two proofs for the odd teams problem?
A theorem is true or false. If it is true, one proof should suffice, so why bother with a second proof?

Answer

It frequently happens that a proof may show connections with other mathematical objects not mentioned in the statement of the theorem.

Why give multiple proofs?

Question

Why did we give two proofs for the odd teams problem?
A theorem is true or false. If it is true, one proof should suffice, so why bother with a second proof?

Answer

It frequently happens that a proof may show connections with other mathematical objects not mentioned in the statement of the theorem.
For instance, the first proof shows how matrices can be used in this and potentially other similar situations.

Why give multiple proofs?

Question

Why did we give two proofs for the odd teams problem?
A theorem is true or false. If it is true, one proof should suffice, so why bother with a second proof?

Answer

It frequently happens that a proof may show connections with other mathematical objects not mentioned in the statement of the theorem.
For instance, the first proof shows how matrices can be used in this and potentially other similar situations.
The second proof introduces vector spaces. It may suggest a tool to solve other related problems.

Why give multiple proofs?

Question

Why did we give two proofs for the odd teams problem?
A theorem is true or false. If it is true, one proof should suffice, so why bother with a second proof?

Answer

It frequently happens that a proof may show connections with other mathematical objects not mentioned in the statement of the theorem.
For instance, the first proof shows how matrices can be used in this and potentially other similar situations.
The second proof introduces vector spaces. It may suggest a tool to solve other related problems.
For instance, how to add more teams if possible (see exercise).

Some more set problems...

Theorem

Assume you formed 23 teams in our class, each team having an odd number of students and any two teams have an even number of students in common. Prove that you can add 3 more teams each with an odd number of students such that any two different teams will have an even number of students in common.

Some more set problems...

Theorem

Assume you formed 23 teams in our class, each team having an odd number of students and any two teams have an even number of students in common. Prove that you can add 3 more teams each with an odd number of students such that any two different teams will have an even number of students in common.

Proof.

Left to you... □

Parallel lines in $GF^2(3)$

We have 9 school girls. They walk daily in 3 rows, each row has 3 girls. We wish to design a "walk" so that each girl will walk with every other girl exactly once.

Parallel lines in $GF^2(3)$

We have 9 school girls. They walk daily in 3 rows, each row has 3 girls. We wish to design a "walk" so that each girl will walk with every other girl exactly once.

Question

How many days are needed?

Parallel lines in $GF^2(3)$

We have 9 school girls. They walk daily in 3 rows, each row has 3 girls. We wish to design a "walk" so that each girl will walk with every other girl exactly once.

Question

How many days are needed?

Answer

Each girl walks with two other girls every day. So to walk with 8 other girls we need at least four days.

Let us design a solution:

Let us design a solution:
We identify each girl with a "point" in $GF^2(3)$. Every line in $GF^2(3)$ is a triple of girls. So each day we will schedule a set of three parallel lines.

Let us design a solution:
We identify each girl with a "point" in $GF^2(3)$. Every line in $GF^2(3)$ is a triple of girls. So each day we will schedule a set of three parallel lines.

The "girls" dressed as "points":
$\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$

Let us design a solution:
We identify each girl with a "point" in $GF^2(3)$. Every line in $GF^2(3)$ is a triple of girls. So each day we will schedule a set of three parallel lines.

The "girls" dressed as "points":
$\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$

A line thorugh the origin:

$$L_1 : \{(0,0),(0,1),(0,2)\}\ \textit{equation}:\ x = 0$$

Let us design a solution:
We identify each girl with a "point" in $GF^2(3)$. Every line in $GF^2(3)$ is a triple of girls. So each day we will schedule a set of three parallel lines.

The "girls" dressed as "points":
$\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$

A line thorugh the origin:

$L_1 : \{(0,0),(0,1),(0,2)\}$ *equation* : $x = 0$

Two parallel lines:

$L_2 : \{(1,0),(1,1),(1,2)\}$ *equation* : $x = 1$

$L_3 : \{(2,0),(2,1),(2,2)\}$ *equation* : $x = 2$

Let us design a solution:
We identify each girl with a "point" in $GF^2(3)$. Every line in $GF^2(3)$ is a triple of girls. So each day we will schedule a set of three parallel lines.

The "girls" dressed as "points":
$\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$

A line thorugh the origin:

$L_1 : \{(0,0),(0,1),(0,2)\}$ *equation* $: \; x = 0$

Two parallel lines:

$L_2 : \{(1,0),(1,1),(1,2)\}$ *equation* $: \; x = 1$

$L_3 : \{(2,0),(2,1),(2,2)\}$ *equation* $: \; x = 2$

This is the schedule for day 1. Note that all nine girls are walking.

Day two: Start with another line through the origin, say $x + y = 0$.

Let us design a solution:
We identify each girl with a "point" in $GF^2(3)$. Every line in $GF^2(3)$ is a triple of girls. So each day we will schedule a set of three parallel lines.

The "girls" dressed as "points":
$\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$

A line thorugh the origin:

$L_1 : \{(0,0),(0,1),(0,2)\}$ *equation* : $x = 0$

Two parallel lines:

$L_2 : \{(1,0),(1,1),(1,2)\}$ *equation* : $x = 1$

$L_3 : \{(2,0),(2,1),(2,2)\}$ *equation* : $x = 2$

This is the schedule for day 1. Note that all nine girls are walking.

Day two: Start with another line through the origin, say $x + y = 0$.
Now do the rest.

Theorem

16 students meet every morning to play Badminton (Za cau). They have four courts so they form 4 teams. Can you schedule the teams so that in five days every student will play with every other srtudent exactly once? (play with another student means be on court with him, not necessarily as a pair. For instance if 1 3 6 13 are playing then 1 will not play again with 3, 6, or 13).

Theorem

16 students meet every morning to play Badminton (Za cau). They have four courts so they form 4 teams. Can you schedule the teams so that in five days every student will play with every other srtudent exactly once? (play with another student means be on court with him, not necessarily as a pair. For instance if 1 3 6 13 are playing then 1 will not play again with 3, 6, or 13).

YES WE CAN!

Theorem

16 students meet every morning to play Badminton (Za cau). They have four courts so they form 4 teams. Can you schedule the teams so that in five days every student will play with every other srtudent exactly once? (play with another student means be on court with him, not necessarily as a pair. For instance if 1 3 6 13 are playing then 1 will not play again with 3, 6, or 13).

YES WE CAN!

Theorem

a. 25 friends meet for dinner at a restaurant. The restaurant has five tables. each table seats five persons. What is the smallest number of dinner parties needed so that each person will dine with every other person?

Theorem

16 students meet every morning to play Badminton (Za cau). They have four courts so they form 4 teams. Can you schedule the teams so that in five days every student will play with every other srtudent exactly once? (play with another student means be on court with him, not necessarily as a pair. For instance if 1 3 6 13 are playing then 1 will not play again with 3, 6, or 13).

YES WE CAN!

Theorem

a. 25 friends meet for dinner at a restaurant. The restaurant has five tables. each table seats five persons. What is the smallest number of dinner parties needed so that each person will dine with every other person?
b. Can you schedule these dinners so that every person will dine with every other person exactly once.

Theorem

16 students meet every morning to play Badminton (Za cau). They have four courts so they form 4 teams. Can you schedule the teams so that in five days every student will play with every other srtudent exactly once? (play with another student means be on court with him, not necessarily as a pair. For instance if 1 3 6 13 are playing then 1 will not play again with 3, 6, or 13).

YES WE CAN!

Theorem

a. 25 friends meet for dinner at a restaurant. The restaurant has five tables. each table seats five persons. What is the smallest number of dinner parties needed so that each person will dine with every other person?
b. Can you schedule these dinners so that every person will dine with every other person exactly once.

Should be easy now!