If $U \subseteq V = \mathbb{F}^n$, then $\dim U + \dim U^\perp = n$.

"Fix a orthonormal basis..." – why can't you do this?

might not be able to normalize a vector (dividing by char)

Build a matrix whose kernel is $U^\perp$.

Basis of U: $e_1, \ldots, e_j$

$$\underbrace{\begin{pmatrix} e_1 & \text{———} \\ & \vdots \\ e_j & \text{———} \\ & 0 \end{pmatrix}}_{\text{projection matrix } (A)} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} e_1 \cdot x_1 \\ \vdots \\ e_j \cdot x_j \\ 0 \end{pmatrix}$$

If $\uparrow$ is all 0, then $\underline{x} \perp U$. $(\underline{x} \perp \underline{e_i} \ \forall i)$, so $U^\perp$ is $\ker A$.

Use rank-nullity theorem...

$\dim U = \dim \operatorname{im} A$

$\dim U^\perp = \dim \ker A$ so $\dim U + \dim U^\perp = n$.

$\square$

For all $A \in \mathbb{Z}^{k \times \ell}$ and any prime p,

$$rk_p(A) \leq rk_0(A).$$

$\det \not\equiv kp$

$\neq 0$

$A = \left(\left(\quad \right) \quad \right)$

in $\mathbb{F}_0$, det $\neq 0$

$k \times k$ nonsingular submatrix

If we know $v_1, \ldots, v_n$ are lin. indep in $\mathbb{F}_p$ and linearly dependent in $\mathbb{Q}$,

$$0 = \sum_{i=1}^{n} \frac{r_i}{s_i} v_i$$

Multiply both sides by $\max\{s_i \mid i \in [n]\}! \ldots$

$\longrightarrow$ take $\gcd\left(\frac{s_{max}!}{s_i} r_i \,\middle|\, i \in [n]\right)$

$$0 = \sum_{i=1}^{n} \boxed{\left(\frac{s_{max}!}{s_i}\right) r_i} \, v_i$$

after factoring out gcd, no shared factors of p,

$\in \mathbb{Z}$ so not a trivial comb. in $\mathbb{F}_p$. $\square$

Find $rk_2(J_n - I_n)$.

$J_n = (1)_{n\times n}$ $\quad$ $I_n = \begin{pmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ 0 & & & & 1 \end{pmatrix}$

$$J_n - I_n = \begin{pmatrix} 0 & & & 1 \\ & 0 & & \\ & & \ddots & \\ 1 & & & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 1 & \cdots & 1 \\ & 0 & & 1 \\ & & \ddots & \\ 1 & & & 0 \end{pmatrix}$$

$|rk(A) - rk(B)| \leq rk(A+B)$

$n-1 \leq rk(J_n - I_n)$

$$\sim \begin{pmatrix} n-1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & & & \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & 1 & 0 \\ 1 & 1 & \cdots & 0 & 1 \end{pmatrix}$$

$rk_2(J_n - I_n) = n-1$ if odd

$n-1 \equiv 0 \pmod 2$ if n is odd, so $rk_2(J_n - I_n) \leq n-1$.

$\equiv 1 \pmod 2$ if n is even, so $rk_2(J_n - I_n) = n$.

Assume cols $u_1, \ldots, u_n$ are linearly dependent

Then $\exists i$ s.t

$$u_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} a_j u_j \quad \text{where } a_j \in \{0,1\}.$$

(WLOG let $i=1$.)

$u_1 = u_2 a_2 + \ldots + u_n a_n$ where $a_i \in \{0,1\}$.

from 1^{st} row:

$0 = a_2 \cdot 1 + a_3 \cdot 1 + \ldots + a_n \cdot 1 = a_2 + \ldots + a_n$

all other rows:

$1 = a_2 \cdot 1 + a_3 \cdot 1 + \ldots + a_j \cdot 0 + \ldots + a_n \cdot 1$

subtract ...

$a_i = 1 \quad \forall i$

But if even, then sum ~~of~~ of odd # of 1's is odd, so $0 = 1$. — contradiction

$$\mathrm{rk}\begin{pmatrix} 0 & & & 1 \\ & 0 & & \\ & & \ddots & \\ 1 & & & 0 \end{pmatrix} = \mathrm{rk}\begin{pmatrix} -1 & 1 & & & 0 \\ & -1 & 1 & & \\ 0 & & \ddots & \ddots & 1 \\ & & & -1 & 1 \\ 1 & 1 & 1 & \cdots & 1 \; 0 \end{pmatrix}$$

$$= \mathrm{rk}\begin{pmatrix} -1 & 1 & & & 0 \\ 0 & -1 & \ddots & & 1 \\ \vdots & & \ddots & -1 & 1 \\ 0 & \cdots & & 0 & n-1 \end{pmatrix}$$

If n is odd, last col all 0...

$\mathrm{rk} = n-1$.

If n is even, full rank: n.

Subtracting the identity reduces all eigenvalues by 1:

$\det(tI - A) = f_A$

$f_{A-I} = \det(tI - (A - I)) = \det((t+1)I - A)$.

For J_n over $\mathbb{R}$:

$J_n \to (\underbrace{0, \ldots, 0}_{n-1}, n)$

$n-1 \leftarrow$ by rank-nullity.

$J_n - I_n \to (-1, \ldots, -1, n-1)$

$\mathbb{F}_2 \to \equiv (1, \ldots, 1, n-1)$

$J_n - I_n : (1, 1, \ldots, 1, n-1)$

eigenvalues.

If n is odd,

$\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$ - eigenvector for $\lambda = 0$ in $\mathbb{F}_2^n$.

By rank-nullity, $rk_2(J_n - I_n) = n-1$.

$f_{J_n} = t^{n-1}(t-n)$ (over $\mathbb{R}$).

$= t^n - nt^{n-1}$

we get char poly to be same mod 2

(arithmetic operations preserved).

For even values of n, J_n is not diagonalizable over $\mathbb{F}_2$.

For odd values of n, J_n is diagonalizable.

$$\det \begin{pmatrix} 0 & & 1 \\ & 0 & \\ 1 & \ddots & 0 \end{pmatrix} = (0 + (n-1)1)(0-1)^{n-1}$$

$$= (n-1)(1)^{n-1} = n-1$$

Lecture

Euclidean space: V - vector space over $\mathbb{R}$ with pos. def. symmetric inner product.

$\|v\| = \sqrt{\langle v, v \rangle}$ norm

$v \perp w$: $\langle v, w \rangle = 0$.

$e_1, \dots, e_k$ is an orthonormal system if

$\langle e_i, e_j \rangle = \delta_{ij}$. (Kronecker δ)

always lin. indep.

ONB - orthonormal basis.

Thm. If dim V is finite (or countable), then V has an ONB.

Proof Take a basis, orthogonalize it (Gram-Schmidt), normalize it.

Thm. If dim V is finite (or countable), then every orthonormal system can be completed to an orthonormal basis.

Proof Take orthonormal system, complete to basis, orthogonalize and normalize.

$$\overbrace{\underbrace{e_1, \dots, e_k}_{\substack{\text{ON} \\ \text{system} \\ \Downarrow \\ \text{lin. indep.}}}, \underbrace{v_{k+1}, \dots, v_n}_{\text{extend to basis}}}^{\text{basis}} \to \text{orth. (GS)}$$

$$\downarrow$$

$$e_1, \dots, e_k, f_{k+1}, \dots, f_n$$

orthogonal

$$\underbrace{e_1, \dots, e_k}_{\substack{\text{ON} \\ \text{system}}}, \underbrace{v_1, \dots, v_n}_{\text{basis}} \to \text{orth. (GS)}$$

$$\downarrow$$

$$e_1, \dots, e_k, 0, f_{k+1}, 0, \dots, 0, f_n, \dots 0$$

Throw out 0s – how do we know this is sufficient?

First n inputs span same as first n outputs $\forall n$. ~ so will form basis if considering all

Tuesday, July 18, 2017 10:44 AM

Consider Euclidean spaces $(V, \langle \cdot,\cdot \rangle_V)$ and $(W, \langle \cdot,\cdot \rangle_W)$.

An <u>isometry</u> of Euclidean spaces is an isomorphism $f: V \to W$ s.t.

$$(\forall x, y \in V)(\underbrace{\langle x, y \rangle_V = \langle f(x), f(y) \rangle_W}_{\text{preserves inner product}}).$$

V, W are isometric if there exists an isometry $V \to W$.

<u>Thm</u> If $\dim V = n$ then V is isometric to $\mathbb{R}^n$ wrt standard dot product

<u>Proof</u> Pick an ONB in V: $e_1, \dots, e_n$, and let $f_1, \dots, f_n$ be the standard basis of $\mathbb{R}^n$.

$f_1, \dots, f_n$ is ON wrt. standard dot product

$x \in V$ $\quad \underline{x} = \sum \alpha_i e_i \quad \underline{x} \mapsto \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \in \mathbb{R}^n$

Tuesday, July 18, 2017 10:52 AM

$$\varphi(\underline{x}) = [x]_{\underline{e}} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$$

$\varphi : V \to \mathbb{R}^n$ isomorphism

NTS: φ preserves inner product, i.e.

$$(\forall x, y \in V)(\langle \underline{x}, \underline{y} \rangle = [x]_{\underline{e}}^T [y]_{\underline{e}})$$

$\underline{x} = \sum \alpha_i e_i$ $\quad \langle \underline{x}, \underline{y} \rangle = \langle \sum \alpha_i e_i, \sum \beta_j e_j \rangle$

$\underline{y} = \sum \beta_j e_j$

$$\overset{\text{by bilinearity}}{=} \sum_i \sum_j \alpha_i \beta_j \underbrace{\langle e_i, e_j \rangle}_{\delta_{ij}}$$

$$= \sum_{i=1}^{n} \alpha_i \beta_i$$

$$= [\alpha_1 \cdots \alpha_n] \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix}$$

$$= [x]_{\underline{e}}^T [y]_{\underline{e}} \qquad \square$$

Cauchy - Schwarz:

$$|\langle x, y \rangle| \le \|x\| \cdot \|y\|$$

Claim: equiv. to triangle inequality: $\|u + v\| \le \|u\| + \|v\|$.

Cauchy - Schwarz $\Rightarrow$ Δ ineq.

NTS: $\|u+v\|^2 \overset{?}{\leq} \|u\|^2 + \|v\|^2 + 2 \cdot \|u\| \cdot \|v\|$

$\downarrow$

$\langle u+v, u+v \rangle$

$\downarrow$ bilinearity

$\langle u,u \rangle + \langle v,v \rangle + \langle u,v \rangle + \langle v,u \rangle$

$\cancel{\|u\|^2} + \cancel{\|v\|^2} + 2\langle u,v \rangle \overset{?}{\leq} \cancel{\|u\|^2} + \cancel{\|v\|^2} + 2\|u\|\|v\|$

$\langle u,u \rangle = \|u\|^2$

$\langle v,v \rangle = \|v\|^2$

$\langle u,v \rangle = \langle v,u \rangle$

$\langle u,v \rangle \leq \|u\| \cdot \|v\|$ ✓ by Cauchy - Schwarz.

Note: $|\langle x,y \rangle| \leq \|x\| \cdot \|y\|$

equiv

$\langle x,y \rangle \leq \|x\| \cdot \|y\|$

$\downarrow$

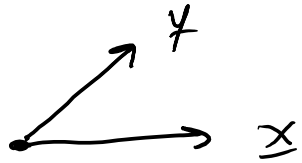
$-\langle x,y \rangle = \langle -x,y \rangle \leq \|-x\| \cdot \|y\| = \|x\| \cdot \|y\|$.

$\square$

All steps reversible (w/o absolute value), so $\Uparrow$ ✓.

$\therefore$ To prove C-S, it suffices to prove Δ-ineq

V is Euclidean space.



NTS: $\|\underline{x}+\underline{y}\| \leq \|\underline{x}\| + \|\underline{y}\|$

Let $\mathcal{U} = \text{span}(\underline{x}, \underline{y})$

$\dim \mathcal{U} \leq 2$ (by 1^{st} miracle)

$\therefore$ $\mathcal{U}$ is isometric to $\mathbb{R}^k$, $k \leq 2$.

$\mathcal{U}$ isometrically embeds in the plane, but Δ-ineq. holds in plane, so Δ-ineq carries over by isometry. $\square$

<u>Cor.</u> If $f, g \in C[0,1]$,
$\uparrow$ continuous functions

then $\left(\int_0^1 f \cdot g \cdot w \, dt\right)^2 \leq \int_0^1 f^2 w \cdot \int_0^1 g^2 \cdot w$.

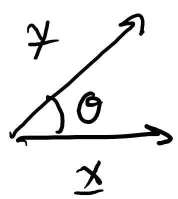
(w is weight func.)

In Euclidean space:

distance $(\underline{x}, \underline{y}) := \|\underline{x} - \underline{y}\|$.

This satisfies the Triangle Inequality. (Do)

angle $\underline{x}, \underline{y} \neq 0$



$$\langle \underline{x}, \underline{y} \rangle = \|\underline{x}\| \cdot \|\underline{y}\| \cdot \cos \theta$$

$$\cos \theta := \frac{\langle \underline{x}, \underline{y} \rangle}{\|\underline{x}\| \cdot \|\underline{y}\|}$$

Solve this for θ: possible?

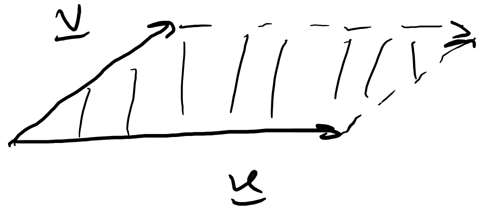
Yes, by Cauchy - Schwartz, $|\langle x, y \rangle| \leq \|x\| \cdot \|y\|$,

So $\dfrac{\langle x, y \rangle}{\|x\| \cdot \|y\|} \in [-1, 1]$.

(will give unique soln between 0 and π.)

<u>Cor.</u> Law of Sines and Law of Cosines holds in any Euclidean spaces.

$\underline{u}, \underline{v} \in \mathbb{R}^2$ parallelogram spanned by $\underline{u}, \underline{v}$



$$\mathrm{Para}(\underline{u}, \underline{v}) = \{\alpha \underline{u} + \beta \underline{v} \mid 0 \le \alpha, \beta \le 1\}.$$

DO If $\underline{u}, \underline{v} \in \mathbb{Z}^2$, then $\mathrm{area}(\mathrm{Para}(\underline{u}, \underline{v})) \in \mathbb{Z}$.

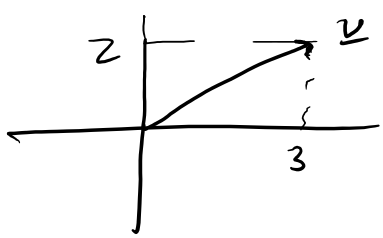
DO If $\underline{u}, \underline{v}, \underline{w} \in \mathbb{Z}^3$, then

$\mathrm{vol}(\mathrm{Para}(\underline{u}, \underline{v}, \underline{w})) \in \mathbb{Z}$. (Parallelepiped)

If $\underline{u}, \underline{v} \in \mathbb{Z}^3$, then $\mathrm{area}(\mathrm{Para}(\underline{u}, \underline{v})) \in \mathbb{Z}$?

No

$\underline{u} \in \mathbb{Z}^2 \not\Rightarrow \mathrm{length}(\underline{u}) \in \mathbb{Z}$



lengths of $\underline{u}$: $\sqrt{3^2 + 2^2}$

$= \sqrt{13}$

DO If $\underline{u}, \underline{v} \in \mathbb{Z}^3$, then $\mathrm{area}(\mathrm{Para}(\underline{u}, \underline{v}))$ is sqrt of an integer

If $u_1, \dots, u_n \in \mathbb{Z}^n$ is a basis of $\mathbb{R}^n$, then

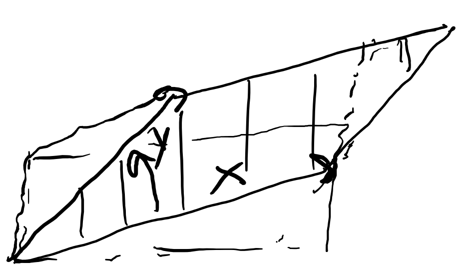
$\mathrm{vol}_n(\mathrm{Para}(u_1, \dots, u_n)) \in \mathbb{Z}$.

If $u_1, \dots, v_k \in \mathbb{Z}^n$ are lin. indep,

then $\mathrm{vol}_k(\mathrm{Para}(u_1, \dots, u_n))$ is sqrt of an int

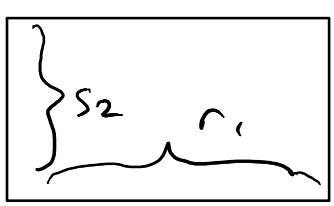
---

$\mathbb{R}^2$



$$\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$$

Claim: area $= \pm$ det. (depends on clockwise or counterclockwise) or LHR/RHR in 3-D.

$\le$ 

$$\begin{pmatrix} r_1 & 0 \\ 0 & s_2 \end{pmatrix}$$

C

det $\nearrow$ $= r_1 s_2 =$ area rect

But this cutting and pasting doesn't change det (col/row ops), so $\pm$ det $=$ area. $\square$

<u>Thm</u> $Vol_n(v_1, \dots, v_n) = \pm \det$.

(If lin. dep., vol is 0 and det is 0.)

This settles full-rank ?'s. What about the others?

k-dim volume in n-dim Euclidean space $(k \le n)$

(1) If $v_1, \dots, v_k \in V$ orthogonal, then

$$\mathrm{vol}_k(\underbrace{\mathrm{para}(v_1, \dots, v_k}_{\text{brick}})) = \prod_{i=1}^{k} \|v_i\|.$$

(2) Vol. is additive: If $A, B \subseteq U \le V$, with $\dim U = k$, and $A \cap B = \emptyset$ then

$$\mathrm{Vol}_k(A \cup B) = \mathrm{Vol}_k(A) + \mathrm{Vol}_k(B).$$

<u>Def</u> If $v_1, \dots, v_k \in V$, where V is a Euclidean space (any dim), the <u>Gram matrix</u> of $v_1, \dots, v_k$ is

$$G(v_1, \dots, v_k) = (\langle v_i, v_j \rangle)_{k \times k}$$

This matrix is symmetric b/c inner product is.

DO G is positive semidefinite.

DO G is nonsingular $\Leftrightarrow$ $v_1, \dots, v_k$ are lin. indep.

$\Updownarrow$

i.e. $\underbrace{\det G}_{\text{Gram determinant / Gramian}} \neq 0$

DO In fact, $rk(G(v_1, \dots, v_k)) = rk(v_1, \dots, v_k)$.

If $V = \mathbb{R}^n$ wrt. standard dot product:

$$A = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_k \\ | & & | \end{pmatrix}_{n \times k}$$

then $G(v_1, \dots, v_k) = A^T A$.

we had Exercise: over $\mathbb{R}$, $rk(A^T A) = rk(A)$. $\square$

DO Give simpler proof of $\uparrow$ via

$rk(G(v_1, \dots, v_k)) = rk(v_1, \dots, v_k)$

DO Thm. If $v_1, v_2, \dots, v_k \in V$ (Euclidean space),

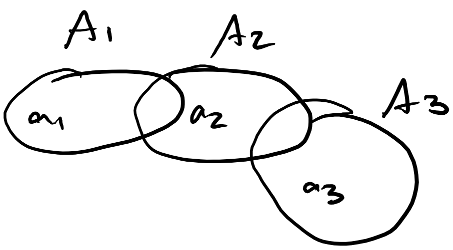
$$\mathrm{Vol}_k(v_1, \dots, v_k) = \sqrt{\underbrace{\det(G(v_1, \dots, v_n))}_{\text{Gramian - integer}}}.$$

Tuesday, July 18, 2017 11:53 AM

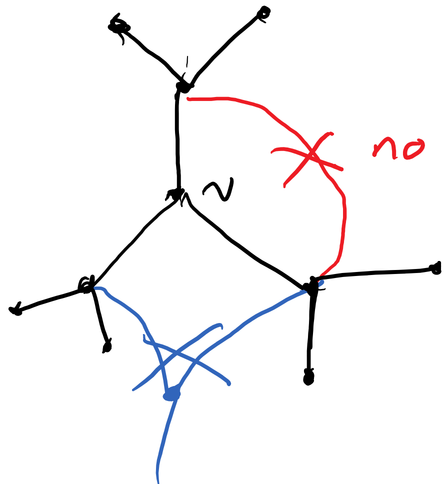
If G k-regular of girth ≥ 5 then $n \geq k^2+1$.
(HW for today).

Take a vertex v (root).

$1 + k + k(k-1)$
$= k^2+1$



$|\cup A_i| \overset{?}{=} \sum a_i$



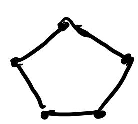
$\therefore$ must have at least k^2+1 vertices.

Is this bound tight?

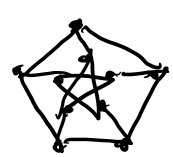
Case of equality...

$k=1$ $n = 1^2+1 = 2$

$k=2$ $n = 2^2+1 = 5$



$k=3$ $n = 3^2+1 = 10$



(Petersen)

Works for
$k=7$ $n = 7^2+1 = 50$
Hoffmann-Singleton graph

$k=57$ works?

Thm If $n = k^2+1$ then $k = \{1,2,3,7,57\}$.

Does not work for $k=4,5,6$.
$\boxed{\text{Proof tomorrow!}}$