W7 D2
8/12/14

Voronoi's characterization of extreme forms / lattices

Def. $\Lambda \subseteq \mathbb{R}^n$ is extreme if $\Lambda \cap B(0,1) = \{0\}$, and in some neighbourhood $\mathcal{U}$ of Λ, $\forall \Lambda' \in \mathcal{U}$ is either similar to Λ, or $d(\Lambda') < d(\Lambda)$ or $\Lambda' \cap B(0,1) \neq \{0\}$ (local max. of $\frac{\lambda_1}{d(\Lambda)^{1/n}}$).

Def Q a pos. def. form is extreme $\left(Q = \sum_{i,j=1}^{n} a_{ij} x_i x_j, (a_{ij}) \in \mathrm{Sym}_n\right)$ if $\exists$ neighbourhood $\mathcal{U}$ of Q in the space of pos. def. quad. forms, $\forall Q' \in Q$, either $Q' = cQ$ for some $c \in \mathbb{R}$, or $\gamma(Q') < \gamma(Q)$ [where $\gamma(Q) = \min_{x \in \mathbb{Z}^n \setminus \{0\}} \frac{Q(x)}{\det(a_{ij})}$].

[both defs. are equiv.]

Let $\pm u_1, \dots, \pm u_s$ be the minimizers of Q – $\pm u_\ell \in \mathbb{Z}^n \setminus \{0\}$ and $Q(\pm u_\ell) = \min_{x \in \mathbb{Z}^n \setminus \{0\}} Q(x) = \gamma'$ [and $u_\ell, 1 \le \ell \le s$ are the only ones for which it's true], $1 \le \ell \le s$.

Def. Q is perfect if it's uniquely determined by the equations $Q(u_\ell) = \gamma'$, $1 \le \ell \le s$, i.e. $Q'(u_\ell) = \gamma'$, $1 \le \ell \le s \Rightarrow Q' = Q$.

If $Q'(x) = \sum_{i,j=1}^{n} b_{ij} x_i x_j$, let $t_{ij} = b_{ij} - a_{ij} \in \mathrm{Sym}_n$. Saying $Q(u_\ell) = Q'(u_\ell) = \gamma'$ is equiv. to saying $\sum_{i,j=1}^{n} t_{ij} u_i^{(\ell)} u_j^{(\ell)} = 0$ a lin. equation in t_{ij}, and Q perfect $\Leftrightarrow$ no $t_{ij} \in \mathrm{Sym}_n$ satisfy this lin. eq. for $1 \le \ell \le s$, except for the trivial $t_{ij} \equiv 0$.

Let $\tilde{A} = (\tilde{a}_{ij}) = \operatorname{adj} A$, $\tilde{a}_{ij} = \det A_{i,j} \cdot (-1)^{i+j}$, so $A^{-1} = \frac{1}{\det A} (\tilde{A})^t$.

for a quad. form Q, denote by $\tilde{Q}$ the adjoint form $\sum_{i,j=1}^{n} \tilde{a}_{ij} x_i x_j$.

Def Q is eutactic if $\exists \rho_1, \dots, \rho_s > 0$ s.t. $\tilde{Q}(x) = \sum_{\ell=1}^{s} \rho_\ell \langle u_\ell, x \rangle^2$.

Note $x \mapsto \langle x, u_\ell \rangle^2$ is a quad form of sig. $(1,0)$

Note $\tilde{a}_{ij} = \frac{\partial \det(a_{ij})}{\partial a_{ij}}$

Thm. (Voronoi) Q extreme $\Leftrightarrow$ Q perfect and eutactic.

Lemma $\underbrace{S_0, S_1 \in \mathrm{Sym}_n^+}_{(1-\theta)S_0 + \theta S_1 \in \mathrm{Sym}_n^+ \text{ (s.t. } \theta \in [0,1])}$ (sym. matrices A giving pos. def. forms, i.e. $A \in \mathrm{Sym}_n^+ \Leftrightarrow \exists P$ invertible s.t. $P^t A P = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$). Define $f: [0,1] \to \mathbb{R}$, $f(\theta) = \det((1-\theta)S_0 + \theta S_1)$, is strictly

... in particular ~~strictly~~ concave

[Recall f is strictly concave if $\forall a,b\in[0,1]$, any $\theta\in(0,1)$,

$f((1-\theta)a+\theta b) > (1-\theta)f(a)+\theta f(b)$.

f is strictly log-concave if $\log f$ is strictly concave.]

for positive functions

<u>Pf.</u> ~~Strictly log-conc. → Strictly conc.:~~

$\cancel{\log f((1-\theta)a+\theta b) > (1-\theta)\log f(a)+\theta\log f(b)=\log f(a)^{1-\theta}f(b)^{\theta}}$.

~~so,~~ $\cancel{f((1-\theta)a+\theta b)}$

First assume $S_0=\mathrm{diag}(\alpha_1,\dots,\alpha_n)$, $S_1=\mathrm{diag}(\beta_1,\dots,\beta_n)$. It's enough to check $\frac{d^2\log f(\theta)}{d\theta^2}<0$. But $f(\theta)=\det(\mathrm{diag}((1-\theta)\alpha_i+\theta\beta_i))$ so $\log f(\theta)=\sum_{i=1}^n\log((1-\theta)\alpha_i+\theta\beta_i)$, so $\frac{d^2\log f(\theta)}{d\theta^2}=\sum_{i=1}^n\frac{-(\beta_i-\alpha_i)^2}{((1-\theta)\alpha_i+\theta\beta_i)^2}<0$.

We just need to prove $\exists Q$ invertible s.t. Q^tS_0Q and Q^tS_1Q are both diag. — we know $\exists Q_1$ s.t. $Q_1^tS_0Q_1=I$, and $Q_1^tS_1Q_1$ is symm. so $\exists P$ orthogonal such that $P^{-1}Q^tS_1QP^t$ is diagonal, and $\cancel{P^tP}$ ~~is a diagonal matrix as well, so we can just tak~~ $\cancel{Q=Q_1P}$, so $P^{-1}=\mathrm{diag}(\frac{1}{\mu_1},\dots,\frac{1}{\mu_n})P^t$, and therefore $P^tQ_1^tS_1QP$ is diagonal as it is $\underbrace{P^tP}_{\text{diag}}\cdot\underbrace{P^{-1}Q_1^{-1}S_1Q_1P}_{\text{diag}}$. Also, $P^tQ_1^tS_0Q_1P=P^tP$ is diagonal as well, so we just take $Q=Q_1P$.

$\log\det S\geq\log\alpha$

<u>Cor.</u> $\{S\in Sym_n^+ \mid \det(S)\geq\alpha\}$ is convex.

<u>Cor.</u> If $\underbrace{S_0\neq S_1}_{\det(S_1)\geq\det(S_0)}$ then $\frac{d}{d\theta}\Big|_{\theta=0}\det((1-\theta)S_0+\theta S_1)>0$.

<u>pf.</u> by lemma, $\frac{d}{d\theta}\log\det((1-\theta)S_0+\theta S_1)>0$ but this is just $\frac{d}{d\theta}\det((1-\theta)S_0+\theta S_1)/\underbrace{\det S_0}_{>0}$.

<u>pf. of Voronoi's thm</u>

Let $Q(x)=\sum_{i,j=1}^n a_{ij}x_ix_j$ be a pos. def. quad. form represented by $A=(a_{ij})\in Sym_n$, $D=\det A$, $\pm u_1,\dots,\pm u_s$ the minimizers of Q, $(t_{ij})\in Sym_n$ parameters (not all zero). For $\rho\in\mathbb{R}$ define $Q_\rho(x)=\sum_{i,j=1}^n\underbrace{(a_{ij}+\rho t_{ij})}_{A_\rho}x_ix_j$, $D_\rho=\det A_\rho$. Note that $A_0=A$, $Q_0=Q$, $D_0=D$, so for $|\rho|<\varepsilon$

Q_ρ is pos. def. Assume Q is extreme, so $\gamma(Q) = \min_{x\in\mathbb{Z}^n\setminus\{0\}} \frac{Q(x)}{\det A^{1/n}} \le \gamma(Q_\rho)$ for small enough $|\rho|$. Then for each ρ close enough to 0, $\exists x \in \mathbb{Z}^n\setminus\{0\}$, $\frac{Q_\rho(x)}{D_\rho^{1/n}} \le \frac{Q(x)}{D^{1/n}}$.

For small enough ρ, x has to be a minimizer for Q, say $x = u_l$. So,

$$\frac{\sum_{i,j=1}^n (a_{ij}+\rho t_{ij}) u_i^{(l)} u_j^{(l)}}{D_\rho^{1/n}} \le \frac{\sum_{i,j=1}^n a_{ij} u_i^{(l)} u_j^{(l)}}{D^{1/n}} \quad (0) \quad [l \text{ may depend on } \rho].$$

Suppose Q isn't perfect. Then we can choose $\overset{\text{not all } 0}{t_{ij}}$ s.t. $\sum_{i,j=1}^n t_{ij} u_i^{(l)} u_j^{(l)} = 0$, $\overbrace{\text{so}\ D_\rho}^{(0)\text{ implies}} \ge D$. But this contradicts cor. 2, applied to $S_0 = (a_{ij})$, $S_1 = (a_{ij}+\rho t_{ij})$.

To show Q is eutactic, define $B = \{(\xi_{ij}) \in \mathrm{Sym}_n \mid \sum_{i,j=1}^n t_{ij}\xi_{ij} \ge 0\}$, a half space of B depending on (t_{ij}). Suppose $\forall l$, B contains $(\xi_{ij}) = (u_i^{(l)}, u_j^{(l)})$. Then (0) implies $D_\rho \ge D$ when ρ is non-negative. By cor. 2 again $0 < \frac{d}{d\rho} D_\rho = \sum_{i,j=1}^n t_{ij} \frac{\partial D}{\partial a_{ij}}\Big|_A = \sum_{i,j=1}^n t_{ij}\hat{a}_{ij}$. So, any half-space B in Sym_n which contains $(u_i^{(l)}, u_j^{(l)})$, also contains $(\hat{a}_{ij})$. So, $(\hat{a}_{ij})$ is contained in the intersection of all such half-spaces, which is exactly the convex cone generated by $(u_i^{(l)}, u_j^{(l)})$. So we can write ~~t_{ij}~~ $\hat{a}_{ij} = \sum_{l=1}^{s} \rho_l u_i^{(l)} u_j^{(l)}$, $\rho_l \ge 0$. [in fact we can show $\rho_l > 0$ by further analysis]. This proves one direction.

For the other, assume Q perfect and eutactic. Write $\hat{Q}(x) = \sum_{i,j=1}^n \hat{a}_{ij} x_i x_j$ the adj. form, $\hat{a}_{ij} = \frac{\partial D}{\partial a_{ij}}\Big|_A$. Chose (t_{ij}) s.t. $\sum_{i,j=1}^n t_{ij}\hat{a}_{ij} = 0$. Define D_ρ like before.

$D_\rho = \det(a_{ij}) + \rho \underbrace{\sum_{i,j=1}^n \hat{a}_{ij} t_{ij}}_{=0} + O(\rho^2) = D + O(\rho^2)$. Take $\rho_1, \dots, \rho_s$ positive ~~given by~~ s.t. $\hat{a}_{ij} = \sum_{l=1}^{s} \rho_l u_i^{(l)} u_j^{(l)}$ ($\exists$ such ρs by Q being eutactic), so $0 = \sum_{i,j=1}^n t_{ij}\hat{a}_{ij} = \sum_l \rho_l \underbrace{\sum_{i,j=1}^n t_{ij} u_i^{(l)} u_j^{(l)}}_{\text{Not all 0, by } Q \text{ perfect}}$.

So $\exists l_0$ $\sum_{i,j=1}^n t_{ij} u_i^{(l_0)} u_j^{(l_0)} < 0$, and therefore $\frac{\sum_{i,j=1}^n (a_{ij}+\rho t_{ij}) u_i^{(l_0)} u_j^{(l_0)}}{D_\rho^{1/n}}$ is less then $\frac{\sum_{i,j=1}^n a_{ij} u_i^{(l_0)} u_j^{(l_0)}}{D^{1/n}}$, for $\rho > 0$ sufficiently small.

This means that $\underset{\gamma(Q_\rho)\leq}{} \frac{Q_\rho(u_{\ell_0})}{D_\rho^{1/n}} \cancel{\#} < \frac{Q(u_{\ell_0})}{D^{1/n}} = \gamma(Q_\rho)$, ~~tb~~ for $\rho > 0$ sufficiently small. Therefore, the directional derivative WRT (t_{ij}) is negative ~~whereas~~ wherever $\sum_{ij=1}^{n} t_{ij}\hat{a}_{ij} = 0$, and γ goes down when walking in any direction in this subspace.

If t_{ij} are multiples of a_{ij}, $\sum_{ij=1}^{n} t_{ij}\hat{a}_{ij}$ is a multiple of D, so the direction of (a_{ij}) isn't in this 1 co-dim subspace. Moving in the direction of (a_{ij}) doesn't effect $\gamma(Q)$ [this is just rescaling]. So, γ has a local max. at Q, therefore Q is extreme.

Ideology of proof: Similar to $\max_{Q} \min_{x\in\mathbb{Z}^n\setminus\{0\}} Q(x)$ subject to $\det(a_{ij})$ fixed (∇f here is just $\hat{A}$).

Thm. (Voronoi) $\forall n\ \exists$ finitely many perfect forms. In particular, $\gamma(Q)$ has finitely many local maxima, and since the maximum is attained (Voronoi showed it is one of those) it is attained on one of them.

Voronoi wrote an algorithm for enumerating all n-dim. perfect forms.

To solve ~~pac~~ sphere-packing: enumerate perfect forms, (maybe check eutactic) and calculate $\gamma(Q)$ on each.

This was [assentially] the strategy for $n \leq 8$. Computationally hard for $n > 8$...

dim	# perfect forms	# extreme forms
1	1	1
2	1	1
3	2	2
4	3	3
5	7	6
6	33	30
7	10916	2048
8	> 500,000	?

$\underbrace{\qquad\qquad\qquad}_{\text{probably around } 10^6\ldots}$

Perfect & eutactic - intrinsic descriptions

recall perfect $\Leftrightarrow$ if $u_1, \ldots, u_s$ minimizers, then $\sum_{ij=1}^{n} t_{ij} u_i^{(\ell)} u_j^{(\ell)} = 0 \Rightarrow t_{ij} \equiv 0$. The common kernel of those s lin. functionals is trivial, hence they generate the ~~span~~ dual space. In particular $s \geq \dim \mathrm{Sym}_n = \frac{n(n+1)}{2}$.

Cor Define $\operatorname{Tr}(a_{ij})=\sum_{i,j=1}^{n} a_{ij}$. Since $(u_i^{(l)}, u_j^{(l)})$ generate the dual space, $\exists \rho_1,\dots,\rho_s$ s.t. $\sum_{l=1}^{s} \rho_l P_{u_l}$, where $P_x:(a_{ij}) \to \sum_{i,j=1}^{n} a_{ij}x_i x_j$

Fact If Q is eutatic $\rho_l > 0$ in the above formula. $\iff$ $\forall y \in \mathbb{R}^n, \|y\|^2 = \sum_{l=1}^{s} \rho_l \langle y, u_l\rangle^2$.

Corollaries of the algebraic theory of perfect & Eutactic forms

skipped

Def. A lattice is perfect (resp. eutactic) iff its shortest vectors WRT euclidean norm $u_1, \dots, u_l$ satisfy $\operatorname{span}\left((t_{ij}) \to \sum_{i,j=1}^{n} t_{ij} u_i^{(l)} u_j^{(l)}\right) = \operatorname{Sym}_n^*$ (resp. (*) $\operatorname{Tr} = \sum_{l=1}^{s} \rho_l P_{u_l}$ for $\rho_1, \dots, \rho_s > 0$).

Theorem any perfect lattice is ~~a scalar multiple of~~ similar to a sublattice of $\mathbb{Z}^n$

Cor $\forall n$, $\gamma_n^n \in \mathbb{Q}$.

Def. $\pm u_1, \dots \pm u_s$ are a eutactic set if (*) holds.

Thm This is true iff $\exists$ orthonormal basis $v_1, \dots, v_s$ of $\mathbb{R}^s$, a scalar $c > 0$ and an orth. proj. $P: \mathbb{R}^s \to \mathbb{R}^n$, s.t. $\pm u_l = \pm c P(v_l)$.

i.e., to construct a eutactic set, take an orthogonal $s \times s$ matrix, delete last $s-n$ rows, multiply by a scalar and take the columns.

In fact, all eutactic set can be found that way.

Prop. eutactic set is always invariant under an irreducible subgroup of orthogonal transformation.

Big finite groups are connected to eutatic lattices.