12. Q is positive semi-definite.

Lecturer: Massimo Lauria

http://www.csc.kth.se/~lauria/sos14/

In this lecture, we complete the proof initiated in Lecture 11. In particular, we prove that if $\ell - 1 < r < n - \ell + 1$ and $\ell \leq \lfloor n/2 \rfloor$, then the quadratic form Q defined in Lecture 11 is positive semi-definite over the space of polynomials of degree at most ℓ.

Let $P_{\leq \ell}$ be the space of multilinearized polynomials over $\mathbb{K}$ in n variables of degree at most ℓ and with $P_t \subseteq P_{\leq \ell}$ the space of *homogeneous* polynomials of degree t. We have that each P_t is a vector space: given a polynomial $p \in P_t$ the I-th coordinate p_I of that polynomial is just the coefficient of the term $\prod_{i \in I} x_i$ as it appears in p.

We recall the definition of the quadratic form Q of monomials from the previous lecture: let

$$B_k := \frac{r(r-1)\cdots(r-k+1)}{n(n-1)\cdots(n-k+1)},$$

then

$$Q(x_I, x_J) = B(X_{I \cup J}) = B_{|I \cup J|}.$$

Theorem 1. *If $\ell - 1 < r < n - \ell + 1$ and $\ell \leq \lfloor n/2 \rfloor$ then $Q \succeq 0$ over $P_{\leq \ell}$*[1].

[1] Dima Grigoriev. Complexity of positivstellensatz proofs for the knapsack. *computational complexity*, 10(2):139–154, 2001

The proof will be based on the following three steps corresponding to the sections of this lecture:

- Decompose $P_{\leq \ell}$ into a direct sum of spaces $P(u)$;
- Show that Q as a linear operator over $P_{\leq \ell}$ is invariant on each $P(u)$;
- $Q \succeq 0$ on each $P(u)$.

Decomposition of the space $P_{\leq \ell}$

Consider the following two linear operators: $C_t : P_t \to P_{t+1}$ and $D_t : P_{t+1} \to P_t$. Let $p = \sum_{I:|I|=t} p_I x_I$ be a polynomial in P_t, where $x_I := \prod_{i \in I} x_i$.

$$C_t(p) := \sum_{I:|I|=t} \sum_{i \notin I} p_I \cdot x_{I \cup \{i\}}. \tag{1}$$

Similarly we define D_t for polynomials $q = \sum_{J:|J|=t+1} q_J x_J$ in P_{t+1}:

$$D_t(q) := \sum_{J:|J|=t+1} \sum_{j \in J} q_J \cdot x_{J \setminus \{j\}}. \tag{2}$$

Starting with some polynomial $u \in P_t$ we want to lift it to some $u^{(m)} \in P_m$ for each $m \leq \ell$:

$$u^{(m)} := \begin{cases} 0 & \text{if } m < t \\ u & \text{if } m = t \\ C_{m-1}(u^{(m-1)}) & \text{otherwise} \end{cases}$$

Notice that given $u = \sum_I u_I x_I \in P_t$ then the coefficient of $u^{(y)}$ corresponding to a set Y of size y is

$$[u^{(y)}]_Y = \sum_{I \subseteq Y} u_I.$$

For $u \in P_t$ let $P(u) := \mathrm{Span}\Big(\big\{u^{(m)}\big\}_{m \leq \ell}\Big)$. We observe that we can represent $P(u)$ using another basis. This is not needed in this section but we put it here just for matter of clarity. It will be needed in the next section.

Proposition 2. *Let $u \in P_t$ then*

$$P(u) = \mathrm{Span}\Big(u, \Big\{\overline{(\sum x_i - r)(\sum x_i)^m u}\Big\}_{m \in [\ell - t - 1]}\Big),$$

where given a polynomial q with $\overline{q}$ we denote its multilinearized version.

Proof. It is sufficient to prove that for each $m \in [\ell - t - 1]$ we have that $\overline{(\sum_i x_i)^{m-t} u} \in \mathrm{Span}(u^{(t)}, \ldots, u^{(m)})$ and the coefficient of $u^{(m)}$ is not 0. In order to do this we just notice that if $m > t$ then

$$u^{(m)} = \sum_{I:\, |I|=t} \sum_{\substack{J \subseteq I^c \\ |J|=m-t}} u_I x_{I \cup J}.$$

Hence it is easy to see that the expansion of $\overline{(\sum_i x_i)^{m-t} u}$ can be expressed as a linear combination of $u^{(t)}, \ldots, u^{(m)}$. Then also $\overline{(\sum x_i - r)(\sum x_i)^m u}$ has the same property hence we can use those polynomials as a basis of $P(u)$. □

This section is devoted to prove the following theorem:

Theorem 3 (Decomposition of $P_{\leq \ell}$)**.**

$$P_{\leq \ell} = \bigoplus_{t=1}^{\ell} \bigoplus_{u \in \mathrm{Basis}(\mathrm{Ker}\, D_{t-1})} P(u). \tag{3}$$

Clearly we have a decomposition of $P_{\leq \ell}$ as a direct sum $P_{\leq \ell} = \bigoplus_{t=0}^{\ell} P_t$ but we need a more fine grained decomposition inside each P_t. Then we will rearrange the spaces in a way somehow transversal w.r.t. the decomposition above.

Lemma 4. *Let $m < \ell \leq \lfloor n/2 \rfloor$ then for each $u \in \mathrm{Ker}\, D_{t-1}$*

$$D_m C_m(u^{(m)}) = (n - m - t)(m - t + 1) u^{(m)}. \quad \square$$

Proposition 5. *Let $A_0 := P_0$ and $A_t := \mathrm{Ker}\, D_{t-1}$, for $t > 0$, then*

$$P_t = A_t \oplus C_{t-1}(A_{t-1}) \oplus C_{t-1}C_{t-2}(A_{t-2}) \oplus \cdots \oplus C_{t-1}C_{t-2}\cdots C_0(A_0).$$

Proof. By induction on t and using Lemma 4 we have that $D_t C_t(P_t) = P_t$. This imply that $\mathrm{Ker}\, D_t \cap C_t(P_t) = \{0\}$ and then by a dimension argument we have that

$$\dim P_{t+1} = \dim \mathrm{Ker}\, D_t + \dim \mathrm{Im} D_t = \dim \mathrm{Ker}\, D_t + \dim C_t(P_t),$$

where the last equality follows from the fact that $\dim C_t(P_t) = \dim \mathrm{Im} D_t = \dim P_t$. Hence $P_{t+1} = \mathrm{Ker}\, D_t \oplus C_t(P_t)$ and this can be expanded obviously in the form required by the proposition. □

We are almost done for the desired decomposition of $P_{\leq \ell}$:

$$
\begin{aligned}
& P_{\leq \ell} \\
& \| \\
& P_0 = A_0 \\
& \oplus \\
& P_1 = A_1 \oplus C_0(A_0) \\
& \oplus \\
& P_2 = A_2 \oplus C_1(A_1) \oplus C_1C_0(A_0) \\
& \oplus \\
& \vdots \\
& \oplus \\
& P_\ell = A_\ell \oplus C_{\ell-1}(A_{\ell-1}) \oplus \ldots \oplus C_{\ell-1}C_{\ell-2}\cdots C_1C_0(A_0)
\end{aligned}
$$

Hence we can group together by diagonals the objects referring to the same A_t obtaining the desired decomposition:

$$P_{\leq \ell} = \bigoplus_{t=0}^{\ell} \bigoplus_{u \in \mathrm{Basis}(A_t)} P(u).$$

The linear operator associated to Q is invariant on $P(u)$

Proposition 6. *Let $Q^{(y,t)}$ be the restriction of Q seen as a linear operator from P_t to P_y and $u \in P_t$ and*

$$\mu_{y,t} := \sum_{j=0}^{t} (-1)^j \binom{t}{j} B_{y+j}.$$

then

$$Q^{(y,t)}(u) = \mu_{y,t} u^{(y)}.$$

and Q maps $P(u)$ in itself.

Proof. Before starting the proof we recall that, by definition, $u^{(y)} = 0$ if $y < t$. Let $u \in A_t$, $u = \sum_{I:\,|I|=t} u_I x_I$ and $[Q^{(y,t)}(u)]_Y$ be the component of $Q^{(y,t)}(u)$ corresponding to the set Y of size y, i.e. the coefficient of the term x_Y of that image.

$$
\begin{aligned}
[Q^{(y,t)}(u)]_Y = \sum_{I:\,|I|=t} B(x_Y x_I) u_I &= \sum_{X \subseteq Y} \sum_{\substack{Y \cap I = X \\ |I|=t}} B(x_Y x_I) u_I = \\
&= \sum_{X \subseteq Y} \sum_{\substack{Y \cap I = X \\ |I|=t}} B_{y+t-|X|} u_I = \\
&= \sum_{j=0}^{t} B_{y+j} \sum_{I:\,|I \cap Y| = t-j} u_I.
\end{aligned} \tag{4}
$$

By the inclusion-exclusion principle we have then, if $y < t$ $Q^{(y,t)}(u) = 0$, and in the other case

$$
\begin{aligned}
[Q^{(y,t)}(u)]_Y \overset{(4)}{=\cdots=} \sum_{j=0}^{t} B_{y+j} (-1)^j \binom{t}{j} \sum_{\substack{I:\, I \subseteq Y \\ |I|=t}} u_I = \\
= \sum_{j=0}^{t} B_{y+j} (-1)^j \binom{t}{j} [u^{(y)}]_Y = \mu_{y,t} [u^{(y)}]_Y.
\end{aligned}
$$

We have now to prove that Q maps $P(u)$ in itself. In order to do this we prove by induction on m that $Q(u^{(m)}) \in P(u)$. The base case is what we just finished to prove. Moreover, as proved in Proposition 2 we have that $\overline{(\sum_i x_i)^{m-t}u} \in \mathrm{Span}(u^{(t)}, \dots, u^{(m)})$, from which follows immediately that

$$\overline{(\sum_i x_i - r)(\sum_i x_i)^{m-t}u} \in \mathrm{Span}(u^{(t)}, \dots, u^{(m+1)}),$$

with non-zero coefficient of $u^{(m+1)}$. Hence

$$Q(\overline{(\sum_i x_i - r)(\sum_i x_i)^{m-t}u}) \in \mathrm{Span}(Q(u^{(t)}), \dots, Q(u^{(m+1)})),$$

but $Q(\overline{(\sum_i x_i - r)(\sum_i x_i)^{m-t}u}) = 0$ and by induction hypothesis we have that $Q(u^{(j)}) \in P(u)$ for each $j \leq m$, hence we have also that $Q(u^{(m+1)}) \in P(u)$. □

Q is positive semidefinite

Lemma 7.

$$\mu_{y,t} = \frac{\prod_{j=1}^{y}(r+1-j)\prod_{j=0}^{t-1}(n-r-j)}{n(n-1)\cdots(n-y-t+1)}. \tag{5}$$

Proof. Consider the following functional equation for some $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$

$$\begin{cases} f(y,0) = B_y \\ f(y,t+1) = f(y,t) - f(y+1,t) \end{cases} \tag{6}$$

There is only one possible solution of (7). We show that both sides of equation (5) are solutions of (7), hence they are equal.

Let $g(y,t)$ the RHS of equation (5). Clearly we have that $g(y,0) = B_y$ and

$$g(y+1,t) + g(y,t+1) =$$
$$= g(y,t) \cdot \frac{r-y}{n-y-t} + g(y,t) \cdot \frac{n-r-t}{n-y-t} = g(y,t).$$

Regarding $\mu_{y,t}$ clearly we have that $\mu_{y,0} = B_y$. To prove the other part of equation (7) just observe that

$$\mu_{y,t+1} = \sum_{j=0}^{t+1}(-1)^j \binom{t+1}{j} B_{y+j} =$$
$$\overset{(\star)}{=} \sum_{j=0}^{t}(-1)^j \binom{t}{j} B_{y+j} + \sum_{j=1}^{t+1}(-1)^j \binom{t}{j-1} B_{y+j} =$$
$$= \mu_{y,t} + \sum_{k=0}^{t}(-1)^{k+1} \binom{t}{k} B_{y+k+1} =$$
$$= \mu_{y,t} - \mu_{y+1,t}.$$

The equality $(\star)$ follows from the Newton identity $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$. □

Lemma 8. *Let $y \geq t$ then $\mu_{t,y} = \binom{n-2t}{y-t}\mu_{y,t}$.* □

Proposition 9. *Q has rank ≤ 1.*

Proof. We use the matrix associated to the quadratic form Q to define a linear operator q. The rank of Q is exactly the dimension of the image of q and this is invariant w.r.t. a change of basis. We use the basis of $P(u)$ used in Proposition 2. As we already observed in the last lecture we have that $B(\overline{(\sum_i x_i - r)p}) = 0$ for any polynomial p. Hence the image of q has dimension ≤ 1. □

Theorem 10 (Q is positive-semidefinite)**.** *Let $t \leq \ell$ and $u \in \operatorname{Ker} D_{t-1}$, if $\ell - 1 < r < n - \ell + 1$ and $\ell \leq \lfloor n/2 \rfloor$ then $Q \succeq 0$ over $P(u)$. Hence, by Theorem 3, $Q \succeq 0$ over $P_{\leq \ell}$.*

Proof. Let M be the matrix with (y,t)-entry $\mu_{y,t}$. By the previous proposition and Proposition 6 we have that M has rank ≤ 1. Hence,

$$\mu_{t,t}\mu_{y,y} - \mu_{y,t}\mu_{t,y} = 0. \tag{7}$$

By Lemma 8 $\mu_{y,t}\mu_{t,y} \geq 0$ and hence by equation (7) then $\operatorname{sgn}(\mu_{t,t}) = \operatorname{sgn}(\mu_{y,y})$. But by Lemma 5 we have that $\mu_{t,t} \geq 0$. And if we are in the range of parameters considered in the hypothesis then $\mu_{t,t} > 0$. Hence $\operatorname{Tr}(M) = \sum_{i=t}^{\ell} \mu_{i,i} > 0$. But this means, as $\operatorname{rank}(M) = 1$ that the only non-zero eigenvalue of M is positive. Hence $Q \succeq 0$ over $P(u)$. □

References

[Gri01] Dima Grigoriev. Complexity of positivstellensatz proofs for the knapsack. *computational complexity*, 10(2):139–154, 2001.