Additional notes on combinatorial nullstellensatz

Péter Csikvári

This is some additional text to Noga Alon's Combinatorial nullstellensatz.

1. Around the Chevalley-Warning theorem

Theorem 1.1. *Let p be a prime and let $\mathbb{F}_p$ be the finite field with p elements, and $P_1 = P_1(x_1, \dots, x_n), \dots, P_m = P_m(x_1, \dots, x_n) \in \mathbb{F}_p[x_1, \dots, x_n]$ such that $\sum_{i=1}^m \deg P_i < n$, then the number of common zeros of $P_1, \dots, P_m$ is divisible by p. In particular, if they have one common zero then they have at least p common zeros.*

Lemma 1.2. *Let $k < p-1$ then*

$$\sum_{a \in \mathbb{F}_p} a^k = 0,$$

where we count in $\mathbb{F}_p$.

Proof. The polynomial $x^k - 1$ has at most k zeros so there must be a $c \neq 0$ such that $c^k \neq 1$, since there are $p-1$ non-zero elements in $\mathbb{F}_p$. Let

$$S_k = \sum_{a \in \mathbb{F}_p} a^k.$$

Then

$$c^k S_k = c^k \sum_{a \in \mathbb{F}_p} a^k = \sum_{a \in \mathbb{F}_p} (ca)^k = \sum_{a \in \mathbb{F}_p} a^k = S_k$$

since multiplying by c simply permutes the elements of $\mathbb{F}_p$. Hence $(c^k - 1)S_k = 0$. Since $c^k - 1 \neq 0$ we have $S_k = 0$. □

Lemma 1.3. *Let $P = P(x_1, \dots, x_n) \in \mathbb{F}_p[x_1, \dots, x_n]$ such that $\deg P < n(p-1)$. Then*

$$\sum_{(a_1, \dots, a_n) \in \mathbb{F}_p^n} P(a_1, \dots, a_n) = 0.$$

Proof. It is enough to prove the lemma for a monomial $Q = x_1^{t_1} \dots x_n^{t_n}$ since the claim follows from the linearity of the statement. Note that

$$\sum_{(a_1, \dots, a_n) \in \mathbb{F}_p^n} Q(a_1, \dots, a_n) = \sum_{(a_1, \dots, a_n) \in \mathbb{F}_p^n} a_1^{t_1} \dots a_n^{t_n} = \left(\sum_{a_1 \in \mathbb{F}_p} a_1^{t_1} \right) \dots \left(\sum_{a_n \in \mathbb{F}_p} a_n^{t_n} \right).$$

Since $t_1 + \cdots + t_n < n(p-1)$ there is some t_i such that $t_i < p-1$, but then

$$\sum_{a_i \in \mathbb{F}_p} a_i^{t_i} = 0$$

by the previous lemma. Hence

$$\sum_{(a_1,\ldots,a_n)\in\mathbb{F}_p^n} a_1^{t_1} \ldots a_n^{t_n} = \left(\sum_{a_1\in\mathbb{F}_p} a_1^{t_1}\right) \ldots \left(\sum_{a_n\in\mathbb{F}_p} a_n^{t_n}\right) = 0.$$

□

Now we are ready to prove Theorem 1.1.

Proof of Theorem 1.1. Let us consider the polynomial

$$P(x_1, \ldots, x_n) = \prod_{i=1}^{m} (1 - P_i(x_1, \ldots, x_n)^{p-1}).$$

Note that

$$\deg P \leq (p-1)\left(\sum_{i=1}^{m} \deg P_i\right) < (p-1)n.$$

Hence by the previous lemma we have

$$\sum_{(a_1,\ldots,a_n)\in\mathbb{F}_p^n} P(a_1, \ldots, a_n) = 0.$$

Note that if $(a_1, \ldots, a_n)$ is not a zero of some polynomial P_i then

$$P_i(a_1, \ldots, a_n)^{p-1} = 1$$

in $\mathbb{F}_p$ by the little Fermat's theorem. Hence $P(a_1, \ldots, a_n) = 0$ in this case. On the other hand if $(a_1, \ldots, a_n)$ is a common zero of all polynomials P_i then clearly $P(a_1, \ldots, a_n) = 1$. Hence

$$0 = \sum_{(a_1,\ldots,a_n)\in\mathbb{F}_p^n} P(a_1, \ldots, a_n) = N,$$

where N denotes the number of common zeros of $P_1, \ldots, P_m$. Hence $p \mid N$. □

Theorem 1.4 (Erdős-Ginzburg-Ziv)**.** *Given $a_1, \ldots, a_{2p-1}$ integers. Then there always exists $i_1 < i_2 < \cdots < i_p$ such that $p \mid a_{i_1} + \cdots + a_{i_p}$.*

Proof. Clearly, we can regard $a_1, \dots, a_{2p-1}$ as elements of $\mathbb{F}_p$. Let us consider the polynomials

$$P_1(x_1, \dots, x_{2p-1}) = \sum_{i=1}^{2p-1} x_i^{p-1} \qquad \text{and} \qquad P_2(x_1, \dots, x_{2p-1}) = \sum_{i=1}^{2p-1} a_i x_i^{p-1}.$$

Note that $\deg P_1 + \deg P_2 = 2(p-1) < 2p-1 = n$, and P_1 and P_2 have a trivial common zero, namely $(0, 0, \dots, 0)$. Hence there is another common zero $(c_1, \dots, c_{2p-1})$. Let N be the number of non-zero elements among the c_i's. Then $P_1(c_1, \dots, c_{2p-1}) = N$, so $p \mid N$. Note that $0 < N \leq 2p-1$. Hence $N = p$. If $c_{i_1}, \dots, c_{i_p}$ are the non-zero elements then

$$0 = P_2(c_1, \dots, c_{2p-1}) = \sum_{j=1}^{p} a_{i_j}.$$

Hence we found p elements whose sum is zero in $\mathbb{F}_p$. □

From this one can easily deduce the following stronger version of the Erdős-Ginzburg-Ziv theorem.

Theorem 1.5 (Erdős-Ginzburg-Ziv)**.** *Let n be a positive integer. Given $a_1, \dots, a_{2n-1}$ integers. Then there always exists $i_1 < i_2 < \dots < i_n$ such that $n \mid a_{i_1} + \dots + a_{i_n}$.*

Proof. We will show that if the statement is true for integers m and k, then it is also true for mk. Indeed, let $a_1, \dots, a_{2mk-1}$ be integers. Since the statement is true for m, and $2mk-1 \geq 2m-1$ there must be m integers such that their sum is divisible by m. By rearranging the numbers we can assume that $m \mid a_1 + \dots + a_m$. Let us delete these numbers from $a_1, \dots, a_{2mk-1}$ and repeat the argument. Again by rearranging the numbers we can assume that $m \mid a_{m+1} + \dots + a_{2m}$. Then we delete these numbers and repeat this argument. We can do it as long as we have at least $2m-1$ numbers. After $2k-2$ rounds we still have $2mk-1-m(2k-2) = 2m-1$ numbers so we can do this process $2k-1$ times. Then let us apply the statement for k and the numbers

$$\frac{a_1 + \dots + a_m}{m}, \frac{a_{m+1} + \dots + a_{2m}}{m}, \dots, \frac{a_{(2k-2)m+1} + \dots + a_{(2k-1)m}}{m}.$$

Among these $2k-1$ numbers there are k whose sum is divisible by k. This means that among the original numbers there are mk numbers whose sum is divisible by mk.

Since we already know that the claim is true for primes, we immediately see that the statement is true for every positive integer n. (For $n = 1$ the claim is trivial.) □

Remark 1.6. As we have seen the heart of the argument was really the prime case. For this special case, you can find another proof in Noga Alon's Combinatorial nullstellensatz. For sake of fun, here we sketch a combinatorial proof of this case.

If there is some $t \in \mathbb{F}_p$ which appears at least p times among $a_1, \ldots, a_{2p-1}$ then we are done. If there is no such t element then it is possible to rearrange the numbers as follows: $a_0, a_1, a_2, \ldots, a_{2(p-2)+1}, a_{2(p-1)}$ such that $a_1 \neq a_2$, $a_3 \neq a_4, \ldots, a_{2(p-2)+1} \neq a_{2(p-1)}$ (why?). Then let us consider the set $S_i = \{a_0\} + \{a_1, a_2\} + \cdots + \{a_{2i-1}, a_{2i}\}$, it means that we consider all sums where the sum contains exactly one element from each $\{a_{2j-1}, a_{2j}\}$. We will show that S_i has at least $i+1$ elements in $\mathbb{F}_p$ by induction. This is true for S_0 and if it is true for S_i, then all we have to show is that $|S_i| \neq |S_{i+1}|$ unless $S_i = S_{i+1} = \mathbb{F}_p$. If $|S_i| = |S_{i+1}|$, then $S_i + a_{2i+1} = S_i + a_{2i+2}$, but then $S_i = S_i + (a_{2i+1} - a_{2i+2})$ which would mean that if $r \in S_i$ then $r + (a_{2i+1} - a_{2i+2}) \in S_i$, $r + 2(a_{2i+1} - a_{2i+2}) \in S_i$,... so $S_i = \mathbb{F}_p$. If $|S_i| \neq |S_{i+1}|$ then since $S_i + a_{2i+1} \subseteq S_{i+1}$ we have $|S_i| < |S_{i+1}|$ so $|S_{i+1}| \geq |S_i| + 1 \geq i + 2$. Of course, if $S_i = \mathbb{F}_p$ then $|S_i| = p \geq i + 1$. Hence $|S_{p-1}| \geq p$, i. e., $|S_{p-1}| = p$ and $0 \in S_p$ which means that 0 is a sum of p elements.

Remark 1.7. One can modify the proof of Lemma 1.3 to get the following variant of the statement: if P has degree $n(p-1)$ then the value of

$$\sum_{(a_1,\ldots,a_n) \in \mathbb{F}_p^n} P(a_1, \ldots, a_n)$$

only depends on the coefficient of the term $x_1^{p-1} \ldots x_n^{p-1}$. If it is not 0, then the above sum is not zero either which means that for some $(a_1, \ldots, a_n)$ we have $P(a_1, \ldots, a_n) \neq 0$ which is often what we need. It might occur that it is not easy to see what's the coefficient of the term $x_1^{p-1} \ldots x_n^{p-1}$ in P. Then there is one more idea which can help: modify P such a way that the obtained polynomial Q has exactly the same max degree terms. Now if you can modify P such a way that the sum

$$\sum_{(a_1,\ldots,a_n) \in \mathbb{F}_p^n} Q(a_1, \ldots, a_n)$$

has exactly one non-zero term, say $Q(c_1, \ldots, c_n)$ then we immediately know that that the coefficient of $x_1^{p-1} \ldots x_n^{p-1}$ is $Q(c_1, \ldots, c_n)$, and so

$$\sum_{(a_1,\ldots,a_n) \in \mathbb{F}_p^n} P(a_1, \ldots, a_n) = Q(c_1, \ldots, c_n) \neq 0$$

so there must be some $(a_1, \dots, a_n)$ for which $P(a_1, \dots, a_n) \neq 0$. A very similar plan will be carried out in the next section.

2. Quantitative nullstellensatz

Theorem 2.1. *(Quantitative nullstellensatz) Let $\mathbb{F}$ be an arbitrary field. Let $P(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$. Let $A_1, \dots, A_n \subseteq \mathbb{F}$ such that $|A_i| = t_i + 1$, and $\deg P \leq t_1 + \dots + t_n$. Let us introduce the polynomials $\phi_i(x) = \prod_{s \in A_i}(x - s)$. Then the coefficient of $x_1^{t_1} \dots x_n^{t_n}$ is exactly*

$$\sum_{a_1 \in A_1} \dots \sum_{a_n \in A_n} \frac{P(a_1, \dots, a_n)}{\phi_1'(a_1) \dots \phi_n'(a_n)},$$

where ϕ_i' is the derivative of ϕ_i.

Proof. First, let us prove the statement for $n = 1$. Let $P(x) = \sum_{k=0}^{t} c_k x^k$ be a polynomial of degree at most t (so it might occur that $a_t = 0$), and A be a set of size $t + 1$. We will use Lagrange's interpolation: let us consider the polynomial

$$Q(x) = \sum_{a \in A} P(a) \frac{\prod_{\substack{a' \in A \\ a' \neq a}} (x - a')}{\prod_{\substack{a' \in A \\ a' \neq a}} (a - a')}.$$

Then $Q(a) = P(a)$ for any $a \in A$, and both polynomials have degree at most t, so $P - Q$ is a polynomial of degree at most t vanishing at at least $t + 1$ points. So $P - Q \equiv 0$, i. e., $P(x) = Q(x)$. By comparing the coefficient of x^t we get that

$$c_t = \sum_{a \in A} \frac{P(a)}{\prod_{\substack{a' \in A \\ a' \neq a}} (a - a')} = \sum_{a \in A} \frac{P(a)}{\phi'(a)},$$

where $\phi(x) = \prod_{a \in A}(x - a)$. This is exactly the statement of the theorem for $n = 1$.

Next we prove the theorem for arbitrary positive integer n. Note that it is enough to prove the claim for monomials since if the claim is true for P_1, P_2, then it is true for $c_1 P_1 + c_2 P_2$ since both the coefficient of $x_1^{t_1} \dots x_n^{t_n}$ and the expression

$$\sum_{a_1 \in A_1} \dots \sum_{a_n \in A_n} \frac{P(a_1, \dots, a_n)}{\phi_1'(a_1) \dots \phi_n'(a_n)},$$

are linear in P. Now assume that $Q(x_1, \dots, x_n) = x_1^{r_1} \dots x_n^{r_n}$, then

$$\sum_{a_1 \in A_1} \dots \sum_{a_n \in A_n} \frac{Q(a_1, \dots, a_n)}{\phi_1'(a_1) \dots \phi_n'(a_n)} = \sum_{a_1 \in A_1} \dots \sum_{a_n \in A_n} \frac{a_1^{r_1} \dots a_n^{r_n}}{\phi_1'(a_1) \dots \phi_n'(a_n)} =$$

$$= \left(\sum_{a_1 \in A_1} \frac{a_1^{r_1}}{\phi_1'(a_1)} \right) \cdots \left(\sum_{a_n \in A_n} \frac{a_n^{r_n}}{\phi_n'(a_n)} \right).$$

Assume that $r_1 + r_2 + \cdots + r_n \leq t_1 + t_2 + \cdots + t_n$. If $r_i = t_i$ for all i then applying the case $n = 1$ separately to each term we get that the last expression is 1 which is indeed the coefficient of $x_1^{t_1} \dots x_n^{t_n}$. If there is some i such that $r_i \neq t_i$, then there must be some j such that $r_j < t_j$. Then by the case $n = 1$ we have

$$\sum_{a_j \in A_j} \frac{a_j^{r_j}}{\phi_j'(a_j)} = 0$$

since in the polynomial x^{r_j}, which is a polynomial of degree at most t_j, the coefficient of x^{t_j} is 0. So in this case the whole product is 0 which is exactly the coefficient of $x_1^{t_1} \dots x_n^{t_n}$ in $Q(x_1, \dots, x_n) = x_1^{r_1} \dots x_n^{r_n}$. Hence we are done. □

As an application we will consider Dyson's conjecture and its q-analogue generalization.

Theorem 2.2. *(Dyson's conjecture, proved independently by Gunson and Wilson.) The constant term of*

$$\prod_{1 \leq i \neq j \leq n} \left(1 - \frac{x_i}{x_j}\right)^{a_i}$$

is equal to

$$\frac{(a_1 + a_2 + \cdots + a_n)!}{a_1! \dots a_n!}.$$

We will actually prove a generalization of this theorem, most precisely a q-analogue of this statement.

Theorem 2.3. *(Andrews's conjecture, proved by Zeilberger and Bressoud.) Let q be fixed and let*

$$(t)_k = (1 - t)(1 - tq) \dots (1 - tq^{k-1}).$$

Then the constant term of

$$\prod_{1 \leq i < j \leq n} \left(\frac{x_i}{x_j}\right)_{a_i} \left(q\frac{x_j}{x_i}\right)_{a_j}$$

is equal to

$$\frac{(q)_{a_1 + a_2 + \cdots + a_n}}{(q)_{a_1} \dots (q)_{a_n}}.$$

Before we start to prove Theorem 2.3 let us see how these theorems are related to each other and to the combinatorial nullstellensatz.

Note that

$$\prod_{1\le i\neq j\le n}\left(1-\frac{x_i}{x_j}\right)^{a_i}=\prod_{1\le i<j\le n}\left(1-\frac{x_i}{x_j}\right)^{a_i}\left(1-\frac{x_j}{x_i}\right)^{a_j}=$$

$$=\frac{1}{x_1^{m_1}\dots x_n^{m_n}}\prod_{1\le i<j\le n}(x_j-x_i)^{a_i}(x_i-x_j)^{a_j},$$

where $m_i=\sum_{k=1}^n a_k-a_i$. Let's introduce the notation $\sigma=\sum_{k=1}^n a_k$. Then the Dyson's conjecture is equivalent with saying that the coefficient of $x_1^{\sigma-a_1}\dots x_n^{\sigma-a_n}$ in the polynomial

$$\prod_{1\le i<j\le n}(x_i-x_j)^{a_i}(x_j-x_i)^{a_j}$$

is

$$\frac{(a_1+a_2+\dots+a_n)!}{a_1!\dots a_n!}.$$

On the other hand,

$$\prod_{1\le i<j\le n}\left(\frac{x_i}{x_j}\right)_{a_i}\left(q\frac{x_j}{x_i}\right)_{a_j}=$$

$$=\prod_{1\le i<j\le n}\left(1-\frac{x_i}{x_j}\right)\left(1-q\frac{x_i}{x_j}\right)\dots\left(1-q^{a_i-1}\frac{x_i}{x_j}\right)\cdot\left(1-q\frac{x_j}{x_i}\right)\dots\left(1-q^{a_j}\frac{x_j}{x_i}\right)=$$

$$=\frac{1}{x_1^{\sigma-a_1}\dots x_n^{\sigma-a_n}}\prod_{1\le i<j\le n}(x_j-x_i)(x_j-qx_i)\dots(x_j-q^{a_i-1}x_i)\cdot(x_i-qx_j)(x_i-q^2x_j)\dots(x_i-q^{a_j}x_j).$$

Andrews's conjecture is equivalent with saying that the coefficient of $x_1^{\sigma-a_1}\dots x_n^{\sigma-a_n}$ in the polynomial

$$\prod_{1\le i<j\le n}(x_j-x_i)(x_j-qx_i)\dots(x_j-q^{a_i-1}x_i)\cdot(x_i-qx_j)(x_i-q^2x_j)\dots(x_i-q^{a_j}x_j)$$

is

$$\frac{(q)_{a_1+a_2+\dots+a_n}}{(q)_{a_1}\dots(q)_{a_n}}=\frac{(a_1+\dots+a_n)_q!}{(a_1)_q!\dots(a_n)_q!}$$

since

$$(q)_m=(1-q)^m(1+q)(1+q+q^2)\dots(1+q+q^2+\dots+q^{m-1}).$$

So if we plug $q=1$ in this statement we will get back Dyson's conjecture.

Let us start to prove Theorem 2.3. This proof is due to Z. Nagy and Gy. Károlyi. Let us again consider the polynomial

$$F(x_1,\dots,x_n)=\prod_{1\le i<j\le n}\prod_{t=0}^{a_i-1}(x_j-q^t x_i)\prod_{t=1}^{a_j}(x_i-q^t x_j).$$

According to the quantitative nullstellensatz the coefficient of $x_1^{\sigma-a_1}\dots x_n^{\sigma-a_n}$ in $F(x_1,\dots,x_n)$ is exactly

$$\sum_{r_1\in A_1}\cdots\sum_{r_n\in A_n}\frac{F(r_1,\dots,r_n)}{\phi_1'(r_1)\dots\phi_n'(r_n)},$$

where ϕ_i' is the derivative of ϕ_i, where A_i are sets of size $\sigma-a_i+1$, and $\phi_i(x)=\prod_{r\in A_i}(x-r)$. The trick is to choose the sets A_i carefully.

Lemma 2.4. *Let $A_i=\{1,q,q^2,\dots,q^{\sigma-a_i}\}$. Then $F(r_1,\dots,r_n)=0$ for all $(r_1,\dots,r_n)\in A_1\times A_2\times\cdots\times A_n$ except if $r_k=q^{\sigma_k}$, where $\sigma_k=\sum_{j=0}^{k-1}a_j$.*

Remark 2.5. Note that $\sigma_1=0,\sigma_2=a_1$ and $\sigma_{n+1}=\sigma$.

Proof. Let $r_i=q^{\alpha_i}$. Note that $F(r_1,\dots,r_n)=0$ if for some $i<j$ we have

$$0\le\alpha_j-\alpha_i\le a_i-1$$

or

$$1\le\alpha_i-\alpha_j\le a_j.$$

This can be rephrased as follows: if $F(r_1,\dots,r_n)\neq 0$ then if $\alpha_k\ge\alpha_m$ then $\alpha_k-\alpha_m\ge a_m$ and if $m<k$ the inequality is strict.

So let us assume that for some permutation π of the numbers $1,2,\dots,n$ we have

$$\alpha_{\pi(1)}<\alpha_{\pi(2)}<\cdots<\alpha_{\pi(n)}.$$

Then

$$\sigma-a_{\pi(n)}=\sum_{j=1}^{n-1}a_{\pi(j)}\le\sum_{j=2}^{n}(\alpha_{\pi(j)}-\alpha_{\pi(j-1)})=\alpha_{\pi(n)}-\alpha_{\pi(1)}\le\alpha_{\pi(n)}\le\sigma-a_{\pi(n)}.$$

There must be equality everywhere which means that (i) $\alpha_{\pi(1)}=0$ (ii) $a_{\pi(j)}=\alpha_{\pi(j)}-\alpha_{\pi(j-1)}$ for all $j=2,\dots,n$. Note that in the last inequality, equality can only hold if $\pi(j)>\pi(j-1)$. So π is the identity permutation, and since $\alpha_1=0$ and $\alpha_j-\alpha_{j-1}=a_{j-1}$, we have $\alpha_j=\sigma_j$. □

Hence the coefficient of $x_1^{\sigma-a_1}\dots x_n^{\sigma-a_n}$ in $F(x_1,\dots,x_n)$ is exactly

$$\frac{F(q^{\sigma_1},\dots,q^{\sigma_n})}{\phi_1'(q^{\sigma_1})\dots\phi_n'(q^{\sigma_n})},$$

where ϕ_i' is the derivative of ϕ_i, where $\phi_i(x) = \prod_{t=0}^{\sigma-a_i}(x-q^t)$. Now we take a deep breath and start to count.

$$F(q^{\sigma_1},\dots,q^{\sigma_n}) = \prod_{1\le i<j\le n}\left(\prod_{t=0}^{a_i-1}(q^{\sigma_j}-q^{\sigma_i+t})\prod_{t=1}^{a_j}(q^{\sigma_i}-q^{\sigma_j+t})\right) =$$

$$= (-1)^u q^v \prod_{1\le i<j\le n}\frac{(q)_{\sigma_j-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}}\cdot\frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_i}} = (-1)^u q^v \prod_{1\le i<j\le n}\frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}},$$

where

$$u = \sum_{1\le i<j\le n} a_i = \sum_{i=1}^{n}(n-i)a_i,$$

and

$$v = \sum_{1\le i<j\le n}\left(\sum_{t=0}^{a_i-1}(\sigma_i+t)+\sum_{t=1}^{a_j}\sigma_i\right) = \sum_{1\le i<j\le n}\left(\binom{\sigma_{i+1}}{2}-\binom{\sigma_i}{2}+a_j\sigma_i\right) =$$

$$= \sum_{i=2}^{n+1}\binom{\sigma_i}{2}+\sum_{i=1}^{n}\sigma_i(\sigma-\sigma_{i+1}).$$

Now let's consider the product

$$\prod_{1\le i<j\le n}\frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}}.$$

Let's study which indices does not cancel in the enumerator and the denominator. The indices $\sigma_i-\sigma_1$, where i goes from 3 to $n+1$ only appear in the enumerator, but not in the denominator. (Note that $\sigma_1=0$, so $\sigma_i-\sigma_1=\sigma_i$, while $\sigma_{n+1}=\sigma$.) Also the indices $\sigma_{n+1}-\sigma_i$, where i goes from 2 to n, only appear in the enumerator. On the other hand, the terms $\sigma_{i+1}-\sigma_i$, where i goes from 2 to $n-1$, only appear in the denominator. It is also true that $\sigma_i-\sigma_i=0$ only appears in the denominator, but $(q)_0=1$ so it doesn't matter. Note that everything else cancels. Hence

$$\prod_{1\le i<j\le n}\frac{(q)_{\sigma_{j+1}-\sigma_i}}{(q)_{\sigma_j-\sigma_{i+1}}} = \prod_{i=3}^{n+1}(q)_{\sigma_i}\prod_{i=2}^{n-1}(q)_{\sigma_{n+1}-\sigma_i}\prod_{i=2}^{n-1}\frac{1}{(q)_{\sigma_{i+1}-\sigma_i}}.$$

Next let us consider $\phi_i'(q^{\sigma_i})$.

$$\phi_i'(q^{\sigma_i}) = \prod_{t=0}^{\sigma_i-1}(q^{\sigma_i}-q^t)\prod_{t=\sigma_i+1}^{\sigma-a_i}(q^{\sigma_i}-q^t) = (-1)^{\sigma_i}q^{\tau_i}(q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}},$$

where

$$\tau_i = \binom{\sigma}{2} + \sigma_i(\sigma - \sigma_{i+1}).$$

Hence $u = \sum_{i=1}^{n}(n-i)a_i = \sum_{i=1}^{n}\sigma_i$ and $v = \sum_{i=1}^{n}\left(\binom{\sigma}{2} + \sigma_i(\sigma - \sigma_{i+1})\right)$. Hence

$$\frac{F(q^{\sigma_1}, \ldots, q^{\sigma_n})}{\phi_1'(q^{\sigma_1}) \ldots \phi_n'(q^{\sigma_n})} = \frac{\prod_{i=3}^{n+1}(q)_{\sigma_i} \prod_{i=2}^{n-1}(q)_{\sigma_{n+1}-\sigma_i} \prod_{i=2}^{n-1} \frac{1}{(q)_{\sigma_{i+1}-\sigma_i}}}{\prod_{i=1}^{n}((q)_{\sigma_i}(q)_{\sigma-\sigma_{i+1}})}.$$

Now since $\sigma_{n+1} = \sigma$ then we have

$$\frac{F(q^{\sigma_1}, \ldots, q^{\sigma_n})}{\phi_1'(q^{\sigma_1}) \ldots \phi_n'(q^{\sigma_n})} = \frac{(q)_\sigma}{(q)_{\sigma_2}(\prod_{i=2}^{n-1}(q)_{\sigma_{i+1}-\sigma_i})(q)_{\sigma_{n+1}-\sigma_n}} =$$

$$= \frac{(q)_{a_1+a_2+\cdots+a_n}}{(q)_{a_1}\prod_{i=2}^{n-1}(q)_{a_i}(q)_{a_n}} = \frac{(q)_{a_1+a_2+\cdots+a_n}}{\prod_{i=1}^{n}(q)_{a_i}}$$

We are done!