Topics in Algebra: Cryptography - The theorem of Cayley–Bacharach

http://www.mat.univie.ac.at/~gagt/crypto2019

Martin Finn-Sell
martin.finn-sell@univie.ac.at

Here we present a proof of the Cayley–Bacharach theorem. We begin by recalling some useful facts, and then proving the result. [1]

Theorem 1. *(Bézout) Let C_1, C_2 be two plane curves over a field $\boldsymbol{k}$ whose defining polynomials F_1, F_2 are relatively prime and have degrees d_1 and d_2. Then there intersection $C_1 \cap C_2$ in $\mathbb{P}^2(\boldsymbol{k}')$, where $\boldsymbol{k}$' is an algebraically closed field containing $\boldsymbol{k}$, counted with their multiplicities, consists of $d_1 d_2$ points.*

This version differs from the notes of Tao. We remark that the version he is working with follows from this result, since the number of points (up to multiplicities) actually included in $\mathbf{k}$ will be smaller than $d_1 d_2$, and the notion of "common component" agrees with the notion of "relatively prime" we use above.

The second thing we need to know is that given any pair of points, there is a unique line between them - similarly, for any five points there is a quadric and 9 points a cubic. For a justification of these points, think about the linear algebraic formulation of these statements - for instance given two points $A = (a_0, a_1)$ and $B = (b_0, b_1)$, then the line between them $L = \{(x, y) \mid ax + by = c\}$ is overdefined - we have four values and three unknowns. The same is the case for higher degree curves as mentioned above.

Lemma 2. *Let $\boldsymbol{k}[x, y, z]_d$ be the space of homogeneous polynomials of degree d[2]. Then $\dim_k k[x, y, z]_d = \frac{(d+1)(d+2)}{2}$.*

Proof. Count the polynomials by figuring out a basis. □

Let $R_d = \mathbb{P}(\mathbf{k}[x, y, z]_d)$, and $\mathbb{P}(R_d(P_1, ..., P_n)) = \{M \in R_d \mid M(P_i) = 0 \text{ for all } i = \{1, ..., n\}\}$. When $\mathbf{k}$ is algebraically closed, and $n \leq \frac{(d+1)(d+2)}{2} - 1$, the subspace $R_d(P_1, ..., P_n)$ of R_d has dimension at most $\frac{(d+1)(d+2)}{2} - n - 1$.

[1] https://terrytao.wordpress.com/2011/07/15/pappuss-theorem-and-elliptic-curves/ would provide an alternative source - as an exercise translate that version into this one.

[2] recall that elements of $\mathbf{k}[x, y, z]_d$ define plane curves of degree d over k

If $\Omega = \{P_1, ..., P_n\} \subset \mathbb{P}^2(k)$ is a set of points, then Ω **defines** l **conditions** on polynomials of degree d if the codimension of $R_d(\Omega)$ is l. We say that Ω defines independent conditions if the codimension of $R_d(\Omega)$ in R_d is exactly $|\Omega| = n$.

Proposition 3. *Let $\Omega = \{P_1, ..., P_n\} \subset \mathbb{P}^2(k)$ be any collection of $n \leq 2d + 2$ points. Then the points of Ω fail to determine independent conditions on curves of degree d if and only if either $d + 2$ of the points are colinear, or $n = 2d + 2$ and Ω is contained in a conic.*

Proof. The "if" direction: If $d + 2$ points of Ω lie on a line L, then by Bézout's theorem any curve of degree d must contain L. The subset of curves of degree d containg L has dimension $\binom{d+2}{2} - \binom{d+1}{2} = d + 1$. The remaing $n - (d + 2)$ points can impose at most $n - (d + 2)$ conditions, so we see that Ω imposes at most $n - 1$ conditions. A similar argument for the second case completes that direction.

The "only if" direction. We must do induction on both the degree d and the number of points n. The induction hypothesis for n will allow us to assume that **no proper subset of** Ω does not impose independent conditions on curves of degree d. If we were supposing that Ω does not impose independent conditions, then this hypothesis states that any curve of degree d that contains all but one point of Ω in fact contains all of Ω.

We note that for $d = 1$, the result is satisfied (The reader should check this).

For arbitrary d satisfying $n \leq d + 1$ the result is also easy - to exhibit a curve of degree d containing all but one point $P_n \in \Omega$ - and we do this by taking the union of general lines L_i through P_i for $i \in \{1, ..., n - 1\}$ and any curve of degree $d - n + 2$ not passing through P_n.

Now we take arbitrary d satisfying $n > d + 1$.

Suppose first that Ω contains $d+1$ points on a line L. Suppose that no further points belong to L, and let Ω' be the complementary set of $n - (d + 1)$ points of Ω. We claim that Ω' must fail to impose independent conditions on curves of degree $d - 1$ - otherwise we could find a curve M of degree $d - 1$ containing all but one point of Ω' and then $L \cup M$ would be a curve of degree d containing all but one point of Ω.

By induction, Ω' must consist of exactly $d+1$ points on a line L', and thus either L contains $d + 2$ points, or $n = 2d + 2$ and Ω lies on the conic $L \cup L'$.

Next, suppose that only some line L contains $l \geq 3$ points of Ω. By the previous argument, the remaining $n-l$ points of Ω must fail to impose independent conditions on curves of degree $d - 1$, and so must include at least $d + 1$ colinear points - which is precisely what we ended up considering in the previous paragraph.

We are done now, except for the case that Ω contains no three colinear points. Choose any three points $P_1, ..., P_3$ in Ω and let Ω' be the complement of these three points in Ω. If for any i the points of $\Omega' \cup \{P_i$ impose independent conditions on curves of degree $d - 1$, we are done - for then we can find a curve C of degree $d - 1$ containing Ω' but not P_i, and then the union of C with the line joining the remaining P_j and P_k is a curve of degree d containing all of Ω except P_i.

Thus, we can suppose that $\Omega' \cup \{P_i\}$ fails to impose independent conditions on curves of degree $d-1$. Since it cannot contain $d+1$ colinear points, we have by induction that $n = 2d+2$ and for each i the set $\Omega' \cup \{P_i\}$ is contained in a conic C_i. In the case $d = 2$, we are done since six points fail to impose indepenent conditions on conics if and only if they lie on a conic.

If $d \geq 3$ then Ω' contains at least 5 points, no three colinear and so there can be at most one conic coontaining Ω, thus all the conics C_i must be equal to a single conic curve C which then contains all of Ω. □

Now we can prove the Cayley–Bacharach theorem.

Theorem 4. *(Cayley–Bacharach) Let* $P_1, ..., P_8$ *be points in* $\mathbb{P}^2(\overline{k})$*, no 4 on a line and no 7 on a conic then there is a 9th point* Q *such that any cubic through* $P_1, ..., P_8$ *also passes through* Q*.*

Proof. We apply the above proposition when $d = 3$, $\Omega = \{P_1, ..., P_8\}$ (so $n = 8$). In this case, Ω must determine independent conditions on cubics - as if we suppose not then we will find our other hypotheses in contradiction to the equivalence in Proposition 1.

Unpacking what this definition means - $R_3(\Omega)$ has codimension 8, but the dimension of R_3 is 9. So there is a cubic containing $P_1, ..., P_8$ in general position, and it must also pass through one more point Q satisfying the conditions by Bézout's theorem. □