An algorithm to calculate the Jennings series in polynomial time

Marco Costantini

Aachen
December, 6th 2003

Let p be a prime and G a finite group (not necessarily a p-group).

In this talk:

- I will remind you what the Jennings series of G (with respect to p) is;
- after that, I will show that the known algorithm to compute the Jennings series of G requires too much time and memory, and works only if G is a p-group;
- in order to save time and memory, I will define the compressed Jennings series (cJs for short), that contains the same information as the Jennings series;
- then I will present an efficient algorithm to compute the cJs;
- finally I will give you a counterexample to show that this algorithm cannot be further improved.

Let K be a field of characteristic p, and Δ the augmentation ideal of the group algebra KG.

The elements of the Jennings series are called also the *(modular) dimension subgroups* of G, and are defined by:

$$D_i(G) := G \cap (1 + \Delta^i) \tag{1}$$

These subgroups can be calculated using the recursive formula [Jennings '41]:

$$D_i(G) := D_m(G)^p [G, D_{i-1}(G)], \tag{2}$$

with $m := \lfloor i/p \rfloor$;

or using the explicit expression [Lazard '54]:

$$D_i(G) := \prod_{jp^k \geq i} \gamma_j(G)^{p^k}. \tag{3}$$

This series is also known as the *Zassenhaus–Jennings–Lazard series*, and its elements are also denoted as $\kappa_i(G)$.

Remark 1. Let G be a group of order p^d. While the length of the lower central series or of the lower p-series* is linear in d, the length of the Jennings series of G may be not only polynomial in d, but even exponential in d.

Example 2. The Jennings series of the cyclic group of order p^d has length $p^{d-1}+1$.

*The (descending or lower) (exponent-)p(-central) series is defined by $P_1(G) := G$, $P_{i+1}(G) := [P_i(G), G]P_i(G)^p$.

Remark 3. Let now G be a group but not a p-group. There is another limitation which applies to the Jennings series, and not to the lower central series and to the lower p-series: when $D_i(G) = D_{i+1}(G) \neq \{1\}$, with p dividing the order of $D_{i+1}(G)$, we do not know whether we have reached the end of the calculation or not.

Example 4. Let $G := C_9 \times S_3$ or $SmallGroup(54, 4)$ be the direct product of the cyclic group with 9 elements and the symmetric group with 6 elements, and let us consider the 3-Jennings series of G. We have $D_2(G) = D_3(G) \neq \{1\}$, but the calculation is not concluded, because $D_3(G) \neq D_4(G)$. $D_4(G)$ has order 6 and $D_4(G) = D_5(G) \neq \{1\}$ and, for any $j > 4$, we have $D_j(G) = D_{j+1}(= D_4(G))$.

Definition 5. The *compressed Jennings series* (*cJs*) of G is the (finite) sequence of sets

$$\{\{G_1, n_1\}, \{G_2, n_2\}, \{G_3, n_3\}, \cdots, \{G_c, n_c\}\}, \quad (4)$$

such that

- $\{G_1, G_2, G_3, \cdots, G_c\}$ are all the subgroups of G that are elements of the Jennings series of G, in the same order, but without repetitions;

- and, for every i, the index n_i is the position in which the subgroup G_i appears for the first time in the Jennings series of G.

(Since the elements of the series are not subgroups but couples formed by a subgroup and a number, the cJs is not a series in the usual sense.)

Let G be a group of order $p^d k$, with k not divided by p and possibly equal to 1.

It is "useful" to calculate an element $D_{i+1}(G)$ of the Jennings series iff $D_i(G) \neq D_{i+1}(G)$.

Since repeated subgroups of Jennings series are possible, and the number of such subgroups can be exponential in d, it is necessary to "guess" in advance which subgroup is useful to calculate and which is not.

We will see the criterion to guess; for this we need a theorem.

Let us denote with $(n)_{p'}$ the biggest divisor of n relatively prime with p (the *p-complement*).

Theorem 6 (Shalev '90). *Let $D_m(G) = D_{m+1}(G)$, let i be an integer bigger than m, and let $(i)_{p'} \geq (m)_{p'}$.*

Then $D_i(G) = D_{i+1}(G)$.

To calculate the cJs, we calculate all the first terms, with the recursive formula (2), as we were calculating the Jennings series. After we have arrived to the first index $m+1$ such that $D_m(G) = D_{m+1}(G)$, to calculate the remaining part of the cJs, we can use the Shalev's theorem to know which subgroups of the Jennings series do not need to be calculated because they are the same as other already calculated subgroups.

We have to know the index $j+1 = j(i)+1$ of the term $D_{j+1}(G)$, that is necessary to consider after considering the index $i+1$ and the subgroup $D_{i+1}(G)$. Let u be the minimum of the $(m)_{p'}$ with m such that $m \leq i$, and $D_m(G) = D_{m+1}(G)$.

Let i be of the form $i = rp^s$, with $r = (i)_{p'}$. We will consider the two cases $D_{i+1}(G) = D_i(G)$ and $D_{i+1}(G) \neq D_i(G)$:

(=) If r=1, then we have arrived to the end of the calculation, in the sense that $D_i(G) = D_{i+k}(G)$, for every $k > 0$.

Otherwise we jump to $j := (\lfloor r/p \rfloor + 1)p^{s+1}$: this is the minimum multiple of $p^s + 1$ greater than i, and also $\left((\lfloor r/p \rfloor + 1)p^{s+1}\right)_{p'} < (r)_{p'}$.

Proceeding in this way, for each i such that $D_i(G) = D_{i+1}(G)$, we bring up to date the value of u, by $u := (i)_{p'}$, as $(i)_{p'}$ is already less than the previous u.

(≠) In this case, let us consider the index $j := i + p^s$. If $(j)_{p'} < u$, we calculate the subgroup $D_{j+1}(G)$; if instead $(j)_{p'} = u$, we already know that $D_{j+1}(G)$ will be the same as the subgroup calculated before, and we can jump directly to the next index, and it will be therefore $j := (\lfloor r/p \rfloor + 1)p^{s+1}$, where now r, s are such that $j = rp^s$, with $r = (j)_{p'}$.

Theorem 7. *Let G be a group of order $p^d k$, with k relatively prime with p (possibly $k = 1$), and let us consider the cJs of G respect to p.*

Then the length of the cJs is less than $d + 2$, and the number of subgroups that are calculated "uselessly" (in the sense that they are the same as already calculated subgroups) is less than d. The calculation of the cJs requires a number of steps that is linear in d and, even if G is not a p-group, the calculation terminates.

Example 8. Suppose that we have calculated the cJs of the G until the subgroup $D_{i+1}(G)$, and let u be (as above) the minimum p-complement by which there is a repeated subgroup. Let F be a free group, and $F_u := F/\gamma_u(F)$ be the relatively free group of class $u - 1$.

Then, up to the index $i + 1$, the Jennings series of the group $G \times F_u$ has the repetitions in the same indexes as the Jennings series of G; and, with the j calculated as above, $D_{j+1}(G \times F_u) \neq D_{i+1}(G \times F_u)$.