UNIVERSITY OF NORTH CAROLINA
Department of Statistics
Chapel Hill, N. C.

Mathematical Sciences Directorate
Air Force Office of Scientific Research
Washington 25, D. C.

AFOSR Report No. 912

ON THE EQUATION $a^{2+n}=b^{2+m}c^{2+p}$ IN A FREE GROUP

by

M. P. Schützenberger

University of North Carolina

June, 1961
Contract No. AF 49(638)-213

Institute of Statistics
Mimeograph Series No. 290

On the Equation $a^{2+n}=b^{2+m}c^{2+p}$ in a Free Group

M. P. Schützenberger

The problem of proving that in a free group G the equation $a^{2+n}=b^{2+m}c^{2+p}$ $(n, m, p \geq o)$ has only trivial solutions has been attacked first by R. G. Lyndon.(1) E. Schenkman (2) generalized Lyndon's result and proved by group theoretic arguments that the result is true for all values of n when m and p are equal to n.

In this note we show that brute force alone is quite enough in the general case. For this, we replace the equation in G by two equations in F, the free monoid generated by a fixed set of generators of G together with their inverses. Thus, if ϕ is the canonical homomorphism $F \longrightarrow G$, and if $|f|$ denotes the length of the element $f \in F$, we can provide F with an involution $f \longrightarrow \bar{f}$ such that $\phi\bar{f} = (\phi f)^{-1}$ and $|f| = |\bar{f}|$. The complement F* of the ideal of F generated by all elements of the form $f\bar{f}$ ($|f| \neq 0$) is just the set of all words which are in reduced form.

With this notation, there corresponds to each element of G a unique $f \in F^*$ of the form $f_1 f_2 \bar{f}_1$ where f_2 belongs to the subset $F^{**} \subset F^*$ of the words $f_2 \in F^*$ such that any cyclically equivalent word f_2' also belongs to F*. Here, as usual, we say that f_2 and f_2' are cyclically equivalent ($f_2 \sim f_2'$) if $f = f_3 f_4$ and $f' = f_4 f_3$ for some $f_3, f_4 \in F$.

In the first part we state several more or less well-known simple facts about F and F* that are repeatedly used later. Basically, they are nothing more than F. W. Levy's theorem (3) on free monoids. (If $f_1 f_2 = f_3 f_4$ and $|f_1| \geq |f_3|$ then $f_1 = f_3 f_5$ and $f_4 = f_5 f_2$ for some $f_5 \in F$) or the remark that $f_1 \bar{f}_2 = f_2 f_3 \in F^*$ and $|f_2| \geq |f_1|$ imply

$f_1 = f_2 = f_3 = e$, the neutral element of F.

In the second and third parts, we verify that the equations $a^{2+n} = (bf)^{1+m}\, b\bar{g}\, (c\bar{f})^{1+p}\, c\ g \in F^*$ and $\bar{g}\, a^{2+n}\, g = b^{2+m}\, c^{2+p} \in F^*$, respectively, have only trivial solutions (i.e. that they imply $f = g = e$, and $a = d^{n_1}$; $b = d^{n_2}$; $c = d^{n_3}$ for some $d \in F$).

In the last part we show that the proposed equation in G reduces to one of the two above forms. It will appear that the only really painful cases here are those where n, m and p have small values. Thus it would not seem impossible to give a complete list of solutions for large enough values of the exponents of such equations as $a^{2+n} = b^{2+m}\, c^{2+p}\, d^{2+q}$. However, the prospect of treating one by one the score or so of equations in F to which this simple relations in G corresponds looks somewhat preposterous since no algorithmic procedure is known as yet that could harness a machine to the task.

I. 1. If $ab = bc$ then, either $a = c = d^{n_1}$ and $b = d^{n_2}$ for some $d \in F$,(1) or $a = dd'$, $b = (dd')^n d$ and $c = c'd$, for some $d, d' \in F$.

---

(1) Since we are dealing with a monoid, the exponents are non-negative numbers; it is understood that for any $f \in F$, $f = e$, the neutral element.

Proof:

Let us assume that the result has been already proved when $|a'b'| < |ab|$.

If $|a| \leq |b|$, one has $b = ab'$ and the given equation simplifies to $ab' = b'c$; consequently, because of the induction hypothosis, $a = dd'$; $b' = (dd')^n d$; $c = d'd$ and thus $b = (dd')^{n+1} d$; if in addition, $a = c$, then, $a = c = d^{n1}$; $b' = d^{n2}$ and $b = d^{n1+n2}$.

If $|a| > |b|$, one has $a = bd'$ and the equation shows that $c = d'b$. Then, if $a \neq c$ the result follows directly by taking $d = b$ and if $a = c$,

$d' =$

we have the new relation $bd' = d'c$ from which we deduce $d' = d^{n_1^3}$; $b = d^{n_2}$ and finally $a = c = d^{n_1+n_2}$.

I. 2. If $a^{2+n} = (bc)^{1+m}\, bd$ with $|a| < |(bc)^m\, b|$, then $a = g^{n_1}$ and $bc = g^{n_2}$ for some $g \in F$.

Proof:

Let us assume first that $|a| \leq |b|$. We define the integers P_1, P_2, P_3 and the elements of Fa_i $(1 \leq i \leq b)$ by the following relations: $b = a^{1+p1}a_1$; $bc = a^{1+p1+p2}a_3$; $bcb = a^{1+p1+p2+p3}a_5$ where

---

(1) Since we are dealing with a monoid, the exponents are non negative numbers; it is understood that for any f F, $f^o = e$, the neutral element.

$a = a_1a_2 = a_3a_4 = a_5a_6$. Thus, $b = a^{1+p1}a_1 = a_4a^{p3}a_5$.

If $p_3 = 1 \pm p_3'$ the last relation gives $a_3a_4a^{p1}a_1 = a_4a_3a_4a^{p3}a_5$; consequently $a_3a_4 = a_4a_3 = a$ and, since by definition $b = a^{1+p1+p2}a_3$, the result follows from (I.1.).

If $p_3 = 0$, we must have also $p_1 = 0$ and $b = a_3a_4a_1 = a_4a_5$. Consequently, $|a_5| \geq |a_3|$ and, taking into account that $a = 3\, a_3a_4 = a_5a_6$, we obtain again $a_3a_4 = a_4a_3$. The rest of the proof remains the same as above.

Let us assume now that $|a| > |b|$ and, consequently, that $m = 1 + n'$ since, by hypothesis, $|a| \leq |(bc)^m b$.

If $|a| \leq |bc|$, $b' = bc$; $c' = e$; $d' = (bc)^{p'}bd$, and since by hypothesis $|a| \leq |b'|$ the result is proved.

If $|a| > |bc|$, we define m' and b' by $|a^{1+m'}| \leq |(bc)^{2+n'}|$ $= |a^{1+m'}b'|$ and $b'c' = a$. We now write $bc = a'$ and we are back to an equation of the same type as the original one but with $d = e$. Since, now $|a'|$ $(= |bc|) < |b'c'|$ $(= |a|)$, the result is proved in all cases.

It can be observed that by taking the special case $c = d = e$, the above result shows that the relation $a^{1+n} = b^{1+m}$ implies that $a = g^{n1}$ and $b = g^{n2}$. The same conclusion follows from the relation $(a_1a_2)^{a+n}a_1 = (b_1b_2)^{2+m}b_2$ since, assuming for instance that $|a_1a_2| \leq |b_1b_2|$, this relation implies another one which can be given the form $(a_1a_2)^{2+n'} = (b_1b_2)^2b'$ with b' a left factor of b_1b_2.

I.3. If both a and $\bar{a}$ are generalized factors[1] of $b^n \in F^{**} - \{ e \}$, then $b = ac\bar{a}c'$ with c and c' different of e.

Proof:

(1) We first notice that for any $u,v \in F$ the two relations $uv = v'\bar{u} \in F^*$, $|u| \geq |v|$ imply $u = v'w$ and $\bar{u} = wv$. Consequently $w = \bar{w}$ and $v' = \bar{v}$. Because $uv \in F^*$, this entails $w = e$ and finally, $uv = u\bar{u} \in F^*$ from which the conclusion $u = v = e$ instantly follows.

(2) We now come back to the proof the property stated. Because a and $\bar{a}$ are generalized factors of b^n we must have relations $a = b'^{m}b'_1$, $\bar{a} = b''_4b''^{m}$, $b' = b'_1b'_2$, $b'' = b''_3b''_4$; $b \sim b' \sim b''$

We cannot have $m > 0$ because, then, the above relations would give an equation $b' = \bar{b}'$ with $b' \sim b''$, that is, $b' = b_6b_5$; $b'' = b_5b_6$ and $b_5b_6 = \bar{b}_5\bar{b}_6$. Finally, we would have $b_5 = b_6 = b = e$ in contradiction with $b \neq e$, because of our remark (1) and of the hypothesis $b \in F^{**}$.

(1) By a generalized factor y of $f \in F$ we mean any factor of a word f' cyclically equivalent to f.

Thus m has to be zero and both a ($=b'_1$) and $\bar{a}$ ($= b''_2 = \bar{b}_1$) are generalized factors of b. The relation b' ($= ab'_2$) $\sim$ b" ($=b''_3\bar{a}$) implies:

either $b' = ab'_1 = b''_5\ \bar{a}\ b''_4$ with $b''_3 = b''_4b''_5$ and because of (1), $b' = ac\bar{a}c'$ with $b''_5 = ac$ and $b''_4 = c'$;

or $b' = ab'_1 = \bar{a}_1b''\bar{a}_2$ with $\bar{a} = \bar{a}_2\bar{a}_1$. The hypothesis $b'\epsilon F^{**}$ shows then that $e = \bar{a}_1 = a_1$ and we are back to the previous case.

I.4. If $\bar{c}$ and $\bar{d}$ are generalized factors of a, and if a is a generalized factor of a word b belonging to the sub monoid generated by c and d, then the hypothesis $b\epsilon F^*$ entails c = d = a = b = e.

Proof:

The statement implies that $\bar{c}$ and $\bar{d}$ are themselves generalized factors of b. According to the remark (1) above there is no relation $\bar{c} = c'v$ or vc' with $c = c''c'$ or $= c'c''$ with $c' \neq e$.

Thus, assuming for instance that $|c| \geq |d|$, we deduce that $c' = \bar{d}u$ with $c' \sim c$ (that is, $c' = c'_2c'_1$ and $c = c'_1c'_2$) and $\bar{c} = d'_2d'^{1+m}$ with $d \sim d' = d'_1d'_2$. Comparing these relations we obtain $c' = \bar{d}u$, $\bar{c} = \bar{d}\ d'_2$, $c'_2c'_1 = \bar{d}u$ and $\bar{c}'_2c'_1 = \bar{d}\ d'_2$. Consequently, d = c = e since $d,c \leftarrow F^*$.

II. The equation (E):

$$a^{2+n} = (bf)^{1+m}\ b\ \bar{g}\ (c\bar{f})^{1+p} \quad \epsilon\ g \in F^*$$

has only trivial solutions when f or g reduces to e.

Proof:

By a trivial solution we mean one in which f = g = e and $a = d^{n1}$; $b = d^{n2}$; $c = d^{n3}$ for some $d\epsilon F$. The restruction that f or g

reduces to e is not unnecessary. The case where g = e is used in the proof of III below and the case where f = e is the one which corresponds to the similar equation in the free group.

It is useful to observe that the equation (E) is in fact symmetric in b and c in the sense that it can also be written

$$a^{2+n} = (c\bar{f})^{1+p} c\ g\ (bf)^{1+m}\ b\bar{g} \text{ with } a' \sim a.$$

For the sake of clarity the proof is split into several parts. In II.1. we assume that $|a| \leq |(bf)^{1+m}|$ and we verify that because a belongs to F** this implies $|a| \leq |(bf)^{m}b|$; this last inequality almost instantly delivers the result. In II.2. we verify by considerations on the length of the elements that we have in fact covered all cases where $n \geq 2$. In II.3. we deal with the case of n = 1 and in II.4. with that of n = 0. In these two cases we show that (E) implies another equation of the same type but strictly shorter and the result follows easily by induction.

II.1. Let us consider first the special case where $|a| = |(bf)^{1+m}|$; under this hypothesis (E) simplifies to $f\ (bf)^{n+m+mn} = \bar{g}\ (c\bar{f})^{1+p} c\ g$.

If f = e this gives $b^{n+m+mn} = \bar{g}\ c^{2+b} g$. Then either b = c = g = e, or else, $c \neq e$ entials $n + m + mn > 0$ and, because of I4, g and $\bar{g}$ are factors of b or, more accurately, $b = \bar{g}\ b'g$. Since $a^{2+n} = b^{2+m}\ \bar{g}\ c^{2+p} g \in F^*$, b^2 also belongs to F* and, finally, g = e. Now, the equation reduces to the system $a = b^{1+m}$, $b^{n+m+mc} = c^{2+p}$ and the result is proved by a straight forward application of I.1. If g = e, we observe that $(c\bar{f})^{2+p} \in F^*$. Thus, $f(bf)^{n+m+mn}\bar{f} = (c\bar{f})^{1+b}\ c\bar{f} \Longleftarrow F^*$ and, consequently, $f\bar{f} \in F^*$, that is f = e. The end of the proof is the same as above.

Let us suppose now that $|(bf)^m b| < |a| < |(bf)^{1+m}|$. The equation (E) can be replaced by the system

$$a = (bf)^m bf_1;\ a^{1+n} = f_2 b\bar{g}\ (c\bar{f})^{1+p} cg,\ f = f_1 f_2.$$

If $m > o$ or if $|f_1| \geq |f_2|$, we compare the left factors of length $|f_2 b|$ of a and a^{1+n} and we obtain the equation

$$bf_3 = f_2 b \text{ with } f_3 \text{ a left factor of } f.$$

If $m = o$ and $|f_1| < |f_2|$, we use a factor of length $|bf_1|$ and we obtain

$$b_1 b_2 f_1 = f_2 b_1 \text{ with } b_1 b_2 = b.$$

In both cases, since $f \neq e$, (I.1) gives either

$$f_2 = uv,\ f_3 = vu,\ b = (uv)^k u$$

or $f_2 = uv,\ b_2 f_1 = v_3 u,\ b_1 = (uv)^k u.$

Now $\bar{f}$ is a generalized factor of a and also, because according to our hypothesis a is a left factor of $(bf)^{1+m}$, it is a generalized factor of b. Thus, in particular $\bar{v}\bar{u}$ has to be a generalized factor of $(uv)^k u$ or of $(uv)^{k+1} u$. Since $a^{2+n} \in F^*$, we know by (I.4.) that this implies $u = v = e$ and, consequently, the hypotheses $|(bf)^m b| < |a| < |(bf)^{1+m}|$ and $a^{2+n} \in F^*$ are contradictory. Let us finally suppose that $|a| \leq |(bf)^m b|$. Then, (I.2) applies and we can write $a = d^{1+n}$ and $bf = d^{1+n2}$. Again $\bar{f}$ is a generalized factor of a, f is a right factor of d^{1+n2} and, consequently, $\bar{f}$ and f are generalized factors of d. Thus $d = d'f$ because of $bf = d^{1+n2}$ and we can simplify (E) to $(fd')^{n3} f = \bar{g}\ (c\bar{f})^{1+p} c\ g$.

This is an equation we already encountered in the special case of $|a| = |bf|^{1+m}$. Thus we have in all cases $f = g = e$, $a = d^{1+n}$, $b = d^{1+n2}$, $d^{n3} = c^{2+p}$ and the result is an immediate consequence of (I.2).

II. 2. Because of the symmetry of equation (E) we can now make the following standing hypotheses:

$|a| > |(bf)^{1+m}|$; $|a| > |(\bar{c}f)^{1+p}|$ and, for instance,

$|(bf)^{1+m} b| \geq |(c\bar{f})^{1+p} c|$.

Because g and $\bar{g}$ are both generalized factors of a, $|a| \geq 2\,|g|$ and (E) can be replaced by the system

$a^{n1}\, a_1'\, \bar{g} = (bf)^{1+m}\, b\bar{g}$, $a_2'\, g a^{n2} = (c\bar{f})^{1+p}\, cg$, $a = a_1'\, \bar{g}\, a_2'\, g$ where $n_1 + n_2 = 1 + n$ and $|a^{n1} a_1 \bar{g}\,| \geq |a_2'\, g a^{n2}|$. This last inequality gives $n_1 \geq n_2$ and we can write $n_1 = 1 + n_1'$. Now, $|a| > |(bf)^{1+m}|$ and $|(bf)^{1+m}\, b| = |a^{n_1'}\, a_1'\,|$ show that $|b| > |a^{n_1'}\, a_1'|$ and that, consequently, $n_1' = 0$. This proves that n = 1 or 0 depending upon $n_2 = 1$ or 0.

We can now rewrite (E) as the following system:

$a = (bf)^{1+m} b_1$, $a^{1+n} = b_2 \bar{g}\, (c\bar{f})^{1+p} cg$, $b = b_1 b_2$, $b_1 \neq e$.

We compare the left factors of length b of a and of a^{1+n} and, applying (I.1), we obtain the following expressions which will be used till the end of the proof:

$b_1 = uv$, $b_2 = (uv)^{k'}\, u$, $a = ((uv)^{1+k'} uf)^{1+m} uv$, $\bar{g}\, (c\bar{f})^{1+p} cg = v\, u\, f\, ((uv)^{1+k'} uf)^{m} u\, v\, a^{n}$. The last equation shows that v can be written as $\bar{g}\, v' g$ with $v' \neq e$ since, because $uv \neq e$, we can always assume that $v \neq e$. According to these equations the inequality $|(bf)^{1+m} b\,| \geq |\,(cf)^{1+b} c|$ becomes for n = 1 $|uv|\,(-2 + k' - m - mk') + |u|\,(1-m) + |f|\,(-1-m) + |f|\,(-1-m) + 2|g| \geq 0$.

Because of $|v| > 2|g|$ this is only possible when m = 0 and k' = 2+k. Then the inequality $|a| > |(cf)^{1+p}|$ becomes simply $|c| + 2\,|g| > 2\,|uv| + |f|$.

When n = 0 the corresponding inequalities are always trivially satisfied.

II. 3. We now consider the case where n = 1 and where since m = 0 and k' = 2+k remarked above, we have:

$b = (uv)^{3+k} u$; $a = (uv)^{3+k} u\, f\, uv$; $\bar{g}(c\bar{f})^{1+p} c\; g = v\, u\, f (uv)^{4+k} u\, f\, u\, v$; $v = \bar{g}\, v'\, g$ with the inequalities

$k|u\ v| + |u| + 2\ |g| \geq |f|$ and $|c| + 2\ |g| > 2\ |uv| + |f|$.

Thus

$(c\ \bar{f})^{2+p} = v'\ g\ u\ f\ (u\ v)^{4+k}\ u\ f\ u\ \bar{g}\ v'\ \bar{f}$

that is

$c'^{2+p} = (uv)^{4+k}\ u\ (f\ u\ \bar{g}\ v'\bar{f}v'guf)$ for some c' cyclically equivalent to $c\bar{f}$.

If $|c'| \leq |(uv)^{3+k}u|$ we can apply I.2 and prove that there exists some a' which is such that $c' = a'^{n1}$ and $uv = a'^{n2}$. Consequently $u\ f\ u\ \bar{g}\ v'\bar{f}v'guf = a'^{n''}$, with $n'' = 2 + n'$ since $uv = a'^{n2}$. Now, this last equation can be written as $a''^{2+n'} = (uf)^2\ u\ \bar{g}\ (v'\bar{f})^1 v'\ g$ for some a'' cyclically equivalent to a'. This, at last, is an equation of the same type as (E) but with $a''^{2+n'}$ strictly shorter than a^{2+n}. Thus, by induction $f = g = e$; $u = d^{n1}$; $v' = d^{n2}$ for some $d \in F$ and the result is proved by reverting to the above expressions for a, b, c as functions of u and v.

It remains to discuss the case where $|c'| = |cf| > |(uv)^{3+k}u|$ which we shall prove to be incompatible with the hypotheses $a \in F^{**}$ and for $y = e$. The above inequality can be written as

$|\bar{g}\ (c\bar{f})^{1+p} c\ g| + |f| = |uv|\ (6 + k) + |u| + 3\ |f| >$

$(2 + p)\ |(uv)^{3+k}u| + 2\ |g|$

$= |uv|\ (6 + 2k + 3p + pk) + |u|\ (2 + p) + 2\ |g|,$

that is,

$3\ |f| > |uv|\ (k + 3p + pk) + |u|\ (1+p)+2|g|$

and it cannot be satisfied when $f = e$.

When $g = e$ we observe that since $|c| > 2\ |uv| + |f|$, the equation $(c\bar{f})^{1+p} c = v\ u\ f\ (uv)^{4+k} u\ f\ u\ v$ gives one or the other of the two systems of relations $c = v\ u\ f\ (uv)^{1+k''}$ $u_1 = u_4 (vu)^{1+k''} f\ u\ v; u_1 u_2 = u_3 u_4 = u$

$c = v\,u\,f\,(uv)^{1+k''}\ uv_1 = v_4u(vu)^{1+k''}\ f\,u\,v; v_1v_2 = v_3v_4 = v.$

In both cases we cancel on the left a factor of length $|vu|$ and we obtain

$$f\,(uv)^{1+k''}u_1 = u_4(vu)^{k''}f\,u\,v \quad \text{or}$$

$$f\,(uv)^{1+k''}uv_1 = v_4u(vu)^{k''}\ f\,u\,v;$$

Now $\bar{f}c \in F^*$ implies $\bar{f}u_4 \in F^*$ or $\bar{f}v_4 \in F^*$. Thus $f\bar{f} \in F^*$ and finally $f = e$.

II. 4. The case where $n = 0$ is quite simple.

We can write (E) as the system

$$(bf)^{1+m} = a_1a_2a_1;\ \bar{g}\ (c\bar{f})^{1+p}c\ g = a_2;\ a = a_1a_2.$$

Consequently, $(bf)^{2+m} = a_1\bar{g}(c\bar{f})^{1+p}c\ g\ a_1f$, that is

$$a'^{2+m} = a_1f\ a_1\ \bar{g}\ (c\bar{f})^{1+p}c\ g \quad \text{for } a' \sim bf.$$

Again we are back to an equation of the same type as (E) but strictly shorter. Thus, by induction, $f = g = e$, $a' = d^{n1}$, $a_1 = d^{n2}$ and $c = d^{n3}$ for some $d \in F$. Since, then, $a = a_1c^{2+p}$ the result is proved.

III. The equation

$$g\ a^{2+n}\ \bar{g} = b^{2+m}\ c^{2+p} \in F^* \text{ implies } g = e$$

Proof:

If a, b, c or $g = e$ the equation reduces to the equation (E) and the result is proved. In the other cases it can be written as the system

$$g = (b'b'')^{m'}b' = (\bar{c}'\bar{c}'')^{p'}\bar{c}';\ (a'a'')^{n'}a' = (b''b')^{m''}b'';$$

$$(a''a')^{n''}a'' = (c''c')^{p''}c'';$$

with

$$n' + n'' = 1 + n;\ m' + m'' = 1 + m;\ p' + p'' = 1 + p.$$

This displays a useful symmetry with respect to (a,n), (b,m) and (c,p). As above, the proof goes by eliminating successively all possible subcases.

III.1. The result is true if $m' = p' = 0$.

Indeed, we multiply the two last equations of the system and obtain

$$a^{2+n} = (b''f)^{1+m}\, b''\, (c''\bar{f})^{1+p} c'' \text{ with } f = b' = \bar{c}'$$

Thus, applying the results of II, we know that $f = e$ and that a, $b'' = b$ and $c'' = c$ are powers of certain element d: Consequently $g = e$ because $d \in F^{**}$. Thus, because of the symmetry, we can always assume now that $m' + p'$, $n' + m''$, $n'' + p \geq 1$.

III. 2. The result is true if $m' = n'' = 0$.

Indeed the equations can be written as

$$b' = (\bar{c}'\bar{c}'')^{1+p'_1}\, \bar{c}'; \quad a'' = (c''c')^{1+p''_1} c'';$$

$$(a'a'')^{1+n} a' = (b''b')^{1+m} b''.$$

Because of (I.4), it will be enough either to show directly that a'' (or b') is a factor of b' (or of a'') or to prove first that $a'a'' = d^{n_1}$; $b''b' = d^{m_1}$ and then to compare the left factors of length $|d|$ of these two relations.

Now, according to the remark made at the end of (I.2), $a'a'' = d^{n_1}$ and when both n and m are different from zero we have $b''b' = d^{m_1}$ as a consequence of the relation $(a'a'')^{1+n}\, a'' = (b''b')^{1+m} b''$. Thus we can assume from now on that $n = 0$ and we first discard the case where m is even, by observing that $a'a''a' = (b''b')^{m+1} b'' = (b''b')\ \ b''b'b''(b'b'')$ implies that one of the two elements a'' and b' is a factor of the other one. Let now $n = 0$ and $m = 1 + 2k$, that is $a'a''a' = (b''b')^{2+2k} b''$.

If $|a'| \leq |b''|$, b' is a factor of a''. If $|a'| > |b''|$, we have $|a'a''| \leq |(b''b')^{1+2k} b''|$, thus $(a'a'')^2 = (b''b')^{2+2k} b''a''$ and because of (I.2) $a'a'' = d^{n_1}$ and $b''b' = d^{n_2}$.

III. 3. The result is true if $m' = n' = 0$.

Indeed, because of (III.1) and (III.2) we have

$$b' = (\bar{c}\,\bar{c}")^{1+p1}\bar{c}'; \quad a' = (b"b')^{1+m1}b" \ (a"a')^{1+n1}\ a" = (c"c')^{p"}c',$$

That is

$$(a" \ (b" \ (\bar{c}'\bar{c}")^{1+p1}\ \bar{c}')^{1+m1})^{1+n1}\ a" = (c"c')^{p"}\ c'.$$

Thus, $\bar{c}'\bar{c}" = e$, because of (I.4), since $\bar{c}'\bar{c}"$ is a generalized factor of $(c"c')^{p"}c'$.

This last remark applies to the six pairs $(m'n')$, $(m',p")$, $(n'p")$, $(n"p')$, $(p',m")$, $(m",n")$ because of symmetry and together with (III.1) and (III.2) this shows that the result is proved when two or more of the six exponents m', $m"$, n', $n"$ p', $p"$ are zero.

III. 4. The result is true if $m' = 0$ and $|b'| > |a|$.

Taking into account what has been already proved we have only to consider the equations

$$b' = (\bar{c}'\bar{c}")^{1+p1}\bar{c}', (c"c')^{1+p2}\ c" = (a"a')^{1+n2}a", (a'a")^{1+n2}a' = (b"b')^{1+m2}b"$$

Let $b_1 \sim b$ be defined by $b_1' = \bar{c}"\bar{c}'(\bar{c}"\bar{c}')^{p1}\bar{c}'$. Since $|b_1| \geq |a|$ the last equation gives a relation $b' = a_1^{1+n'2}a'$ with $a_1 \backsim a'a"; a_1'a_1" = a_1$ and the second equation gives $\bar{c}"(\bar{c}'\bar{c}")^{1+p2} = \bar{a}"\bar{a}')^{n2}\ \bar{a}"$.

Thus, by comparing the left factors of length $|a_1|$ of the two expressions of b_1, we get $a_1 = \bar{a}"\bar{a}'$, that is $a = e$, since $a_1 \backsim a'a"$.

III. 5. The result is true if $m' = 0$ and $|a| > |b'|$ or if $m' > 0$.

If $m' > 0$ we can assume by symmetry that $|a| \geq |b| \geq |c|$ and we replace the first of the three equations used in (III.4) by $(b'b")^{1+m1}b' = (\bar{c}'\bar{c}")^{1+p1}c_1$.

We note that with these hypotheses we always have $|a| \geq |c|$.

Let us define $a_1 \sim a'a''$ by $a_1 = b'(b''b')^{1+m2}b'_1$ where b'_1 is a left factor of $b''b'$. Then we also have $a_1 = c_1^{1+p2}c'_1$ with $c_1 \sim c''c'$ and c'_1, a left factor of c_1.

We now compare the left factor of length $|c|$ of the two expressions of a_1 which have been obtained and of the relation $b'(b''b')^{m'} = (\bar{c}'\bar{c}'')^{1+pl}\bar{c}'$. As in (III.4) we get $c_1 = \bar{c}'\bar{c}''$ and this shows that $c = e$.

Thus the result is proved in all cases.

IV. In this section we give a complete proof that the equation $a'^{2+n} = b'^{2+m}c'^{2+p}$ in G implies one of the two equations in F discussed in III and IV above.

With a view to possible generalisations we establish the following slightly more detailed result IV.1.

Here $f \longrightarrow f^*$ (respectively, $f \longrightarrow f^{**}$) denotes the mapping $F \longrightarrow F^*$ (respectively, $F \longrightarrow F^{**}$) defined by the conditions $\phi f = \phi f^*$ and $f^* \in F^*$ (respectively, $f^{**} \in F^{**}$ and $f^* = \bar{f}_1 f^{**} f_1$ for some $f_1 \in F$).

IV. 2. To any $b, c \in F$ there corresponds one $u \in F$ which is such that at least one of the following equations hold.

$$(\bar{u}\, b\, c\, u)^{**} = (\bar{u}\, b\, u)^{**}(\bar{u}\, c\, u)^{*}$$

$$(\bar{u}\, b\, u)^{**} = (\bar{u}\, b\, c\, u)^{**}\,(\bar{u}\, \bar{c}\, u)^{*}$$

$$(\bar{u}\, c\, u)^{**} = (\bar{u}\, \bar{b}\, u)^{*}\,(\bar{u}\, b\, c\, u)^{**}$$

$$(\bar{u}\, b\, c\, u)^{*}\,(\bar{u}\, b\, u)^{**}\,(\bar{u}\, c\, u)^{**}$$

Proof:

We assume that $|b^{**}| \geq |c^{**}|$ and we use repeatedly the fact that for any $f, f' \in F$ the relation $f^{**} \sim f'^{**}$ is $(\bar{f}_1 f f_1)^{*} = f'$ for some $f_1 \in F$. The element u is constructed by induction as a product $u_1u_2\ldots\ldots$.

Let us assume first that $b = t\, b^{**}\, \bar{t}$ and take $u_1 = t$. We have:

$(\bar{t}\ b\ c\ t)^* = w_1 a_1 \bar{w}_1$ (where $a_1 = (\bar{t}\ b\ c\ t)^{**}$)

$(\bar{t}\ b\ t)^* = b^{**}$

$(\bar{t}\ c\ t)^* = v_1 c_1 \bar{v}_1$ (where $c_1 = (\bar{t}\ c\ t)^{**}$ and

$w_1\ a_1\ \bar{w}_1 = (b^{**} v_1\ c\ \bar{v}_1)^*$.

We now have to consider separately several cases and subcases.

1) If $v_1 = e$, we put $b^{**} = f_1 h_1$ and $c_1 = \bar{h}_1 g_1$ with h_1 defined by the condition that $f_1 g_1 \in F^*$ and we consider separately

   11) If $g_1 = e$, that is, if $w_1 a_1 \bar{w}_1 = f_1$ and $b^{**} = f_1 \bar{c}_1$, we have $b^{**} = (\bar{u}_1\ h\ c\ u_1)^*\ (\bar{u}_1\ \bar{c}\ u)^{**}$ and the result is proved.

   12) If $g_1 \neq e$ we also have $f_1 \neq e$ since, by hypothesis $|b^{**}| \geq |c^{**}| = |c_1^{**}|$.

   Thus the three relations $f_1 g_1 \in F^*$, $f_1 h_1 \in F^*$ and $\bar{h}_1 g_1 \in F^{**}$ imply $h_1 f_1 g_1 \bar{h}_1 \in F^*$ and if we take $u_2 = h_1$ we obtain:

   $(\bar{u}_2 \bar{u}_1\ b\ c\ u_1 u_2)^* = w_2 a_2 \bar{w}_2$ (with $a_2 \in F^{**}$),

   $(\bar{u}_2 \bar{u}_1\ b\ u_1 u_2)^* = h_1 f_1 \in F^{**}$,

   $(\bar{u}_2 \bar{u}_1\ c\ u_1 u_2)^* = g_1 \bar{h}_1 \in F^*$ and $w_2 a_2 \bar{w}_2 = h_1 f_1 g_1 \bar{h}_1$.

Now, the result is proved if $|w_2| \leq |g_1 \bar{h}_1|$. If this inequality does not hold we have $\bar{w}_2 = \bar{w}_3 g_1 h_1$: Thus, $h_1 f_1 = g_1 \bar{h}_1 w_3 a_2 \bar{w}_3$ and the result is finally proved by taking $u = u_1 u_2 u_3$ with $u_3 = g_1 \bar{h}_1$.

2) If $v_1 \neq e$, we still write $b^{**} = f_1 h_1$ $v_1 = \bar{h}_1 v_1'$ with $f_1 v_1' \in F^*$ and we take $u_2 = \bar{h}_1$. Thus we get:

$(\bar{u}_2 \bar{u}_1\ b\ c\ u_1 u_2)^* = w_2 a_2 \bar{w}_2$ (with $a_2 \in F^{**}$)

$(\bar{u}_2 \bar{u}_1\ b\ u_1 u_2)^* = h_1 f_1 \in F^{**}$

$(\bar{u}_2 \bar{u}_1\ c\ u_1 u_2)^* = v_1'\ c_1 \bar{v}_1'$ (with $c_1 \in F^{**}$)

$w_2\ a\ \bar{w}_2 = (h_1 f_1 v_1'\ c_1 \bar{v}_1)^*$.

Now:

If $v_1' = e$ we are back to the case 1 above,

If $v_1' \neq e$; and $f_1 = e$ we are back to the case 2,

If $v_1' \neq e$ and $f_1 \neq e$ we are back to the case 12. and this concludes the proof.

We now apply this to the equation $a^{2+n} = b'^{2+m}\, c'^{2+p}$ in G, the free group, by taking $b = b^{2+m}$ and $c = c'^{2+p}$ in IV.1 and we thus obtain either one equation of type (E) (with f = e) or one equation of the type discussed in III depending upon the fact that we get one of the first three cases of the fourth case listed in IV.1.

REFERENCES

(1) R. C. Lyndon. "The equation $a^2b^2 = c^2$ in free groups", Michigan Mathematical Journal, 6 (1959), pp. 89-95.

(2) E. Schenkman. "The equation $a^nb^n = c^n$ in a free group", Annals of Mathematics, 70 (1959), pp. 562-564.

(3) F. W. Levy. "On semigroups", Bulletin Calcutta Mathematical Society, 36 (1944), pp. 191-196.