An effective version of the Lazard correspondence

Serena Cicalò (Cagliari)

Jointly with:
Willem A. de Graaf (Trento) and Michael R. Vaughan-Lee (Oxford)

Group Theory in Trento 2012
Trento, June 7th, 2012

The Lazard correspondence

Definition. The Lazard correspondence is an isomorphism between the categories of nilpotent Lie rings with order p^n and nilpotency class c and finite p-groups with the same order and nilpotency class, provided $c < p$.

Using the Baker-Campbell-Hausdorff formula and its inverses, it is possible to define:

- a group structure on a Lie ring of order p^n and nilpotency class $< p$;
- a Lie ring structure on a p-group of class $< p$.

These operations are mutually inverse. The same set gets the structure of a Lie ring and of a p-group.

We have developed algorithms to carry out this correspondence.

The Baker-Campbell-Hausdorff formula

Let x and y be non-commutative indeterminates over $\mathbb{Q}$, then

$$e^x e^y \neq e^{x+y}.$$

The product $e^x e^y$ was studied by Campbell in 1898, Baker in 1905 and Hausdorff in 1906.

The BCH-formula asserts $e^x e^y = e^{z(x,y)}$, with

$$\begin{aligned} z(x,y) &= x + y + \frac{1}{2}[x,y] + \frac{1}{12}[x,x,y] - \frac{1}{12}[y,x,y] \\ &\quad -\frac{1}{24}[y,x,x,y] - \frac{1}{720}[x,x,x,x,y] + \ldots. \end{aligned}$$

where the bracket is the commutator defined as $[x,y] := xy - yx$ and we use the right normed convention.

Many authors, as Dynkin in 1947, Goldberg in 1956, Reinsch in 2000 and Casas and Murua in 2009, found methods to compute the coefficients of $z(x, y)$.

Remark. For x and y in a nilpotent Lie ring, $z(x, y)$ is a finite sum and the denominators of the coefficients only have prime factors smaller then $c + 1$.

Example. If $c = 5$, we have

$$\begin{aligned} z(x,y) \quad = \quad & x + y + \frac{1}{2}[x,y] + \frac{1}{12}[x,x,y] - \frac{1}{12}[y,x,y] - \frac{1}{24}[y,x,x,y] \\ & - \frac{1}{720}[x,x,x,x,y] - \frac{1}{120}[x,y,x,x,y] - \frac{1}{360}[x,y,y,x,y] \\ & + \frac{1}{360}[y,x,x,x,y] + \frac{1}{120}[y,y,x,x,y] + \frac{1}{720}[y,y,y,x,y] \end{aligned}$$

where all denominators involve only prime factors $2, 3$ and 5.

A similar formula follows from z for the commutator:

$$[\![e^{x}, e^{y}]\!] := e^{-x}e^{-y}e^{x}e^{y} = e^{w(x,y)},$$

where $w(x, y)$ is an infinite sum of Lie elements.

We have found a method for computing explicitly this formula.

The first few components of w are given by:

$$\begin{aligned} w(x,y) &= [x,y] - \frac{1}{2}[x,x,y] - \frac{1}{2}[y,x,y] + \frac{1}{6}[x,x,x,y] \\ &\quad + \frac{1}{4}[y,x,x,y] + \frac{1}{6}[y,y,x,y] - \frac{1}{24}[x,x,x,x,y] + \dots . \end{aligned}$$

We use z and w to go from a Lie ring L of order p^n and nilpotency class $c < p$ to a p-group, with the same order and nilpotency class, in the following way:

$$\begin{aligned} ab &= z(a,b) = a + b + \frac{1}{2}[a,b] + \frac{1}{12}[a,a,b] - \frac{1}{12}[b,a,b] \\ &\quad -\frac{1}{24}[b,a,a,b] - \frac{1}{720}[a,a,a,a,b] + \dots, \end{aligned}$$

$$\begin{aligned} [\![a,b]\!] &= w(a,b) = [a,b] - \frac{1}{2}[a,a,b] - \frac{1}{2}[b,a,b] + \frac{1}{6}[a,a,a,b] \\ &\quad +\frac{1}{4}[b,a,a,b] + \frac{1}{6}[b,b,a,b] - \frac{1}{24}[a,a,a,a,b] + \dots, \end{aligned}$$

for all $a, b \in L$.

The inverse formulas

We can invert the previous formulas to go from a p-group to a Lie ring.

We have found a general formula for the repeated commutators of e^x and e^y:

$$[\![e^{x_{i_k}}, \ldots, e^{x_{i_1}}, e^x, e^y]\!] = e^V,$$

where $x_{i_k}, \ldots, x_{i_1} \in \{x, y\}$ and V is an infinite sum of Lie elements.

This formula is obtained inductively, that is, if we put

$$[\![e^{x_{i_{k-1}}}, \ldots, e^{x_{i_1}}, e^x, e^y]\!] = e^{V'},$$

we have

$$e^V = [\![e^{x_{i_k}}, e^{V'}]\!] = e^{w(x_{i_k}, V')}.$$

The first inverse formula is

$$e^{x+y} = h_1(e^x, e^y) = e^x e^y \prod_{i \geq 2} e^{\alpha_i V_i},$$

where e^{V_i} are commutators in e^x and e^y and the exponents α_i are in $\mathbb{Q}$ (they depend on the order in which the V_i are listed).

Similarly, the second inverse formula is

$$e^{[x,y]} = h_2(e^x, e^y) = [\![e^x, e^y]\!] \prod_{i \geq 3} e^{\beta_i V_i}.$$

We have found a method for computing explicitly h_1 and h_2.

Theorem. To find the α_i for all commutators of length t in h_1 we have to solve the following equation:

$$\left[e^x e^y \prod_{i\geq 2} e^{\alpha_i V_i}\right]_t = \frac{1}{t!}(x+y)^t.$$

Similarly to find the β_i for the length t in h_2 the equation is:

$$\left[[\![e^x, e^y]\!] \prod_{i\geq 3} e^{\beta_i V_i}\right]_t = \begin{cases} \frac{1}{(\frac{t}{2})!}[x,y]^{\frac{t}{2}}, \text{ if } t \text{ is even,} \\ 0, \text{otherwise.} \end{cases}$$

Constructing h_1

For $t = 2$ we put $e^{V_2} := e^w = [\![e^x, e^y]\!]$. We consider

$$\left[e^x e^y e^{\alpha_2 w}\right]_2 = \left[(1 + z + \frac{1}{2}z^2)(1 + \alpha_2 w)\right]_2.$$

Expanding the equation becomes

$$\frac{1}{2}[x, y] + \frac{1}{2}(x + y)^2 + \alpha_2[x, y] = \frac{1}{2}(x + y)^2 \Rightarrow \alpha_2 = -\frac{1}{2}.$$

For $t = 3$ we put $e^{V_3} := [\![e^x, e^x, e^y]\!]$ and $e^{V_4} := [\![e^y, e^x, e^y]\!]$. Then

$$\left[e^x e^y e^{-\frac{1}{2}w} e^{\alpha_3 V_3} e^{\alpha_4 V_4}\right]_3 = \left[(1+z+\frac{1}{2}z^2+\frac{1}{6}z^3)(1-\frac{1}{2}w)(1+\alpha_3 V_3)(1+\alpha_4 V_4)\right]_3,$$

and we obtain

$$\left(\alpha_3 + \frac{1}{12}\right)[x, x, y] + \left(\alpha_4 - \frac{1}{12}\right)[y, x, y] = 0 \Rightarrow \alpha_3 = -\frac{1}{12} \text{ and } \alpha_4 = \frac{1}{12}.$$

For $t = 4$, we put $e^{V_5} := [\![e^x, e^x, e^x, e^y]\!]$, $e^{V_6} := [\![e^y, e^x, e^x, e^y]\!]$, $e^{V_7} := [\![e^x, e^y, e^x, e^y]\!]$, $e^{V_8} := [\![e^y, e^y, e^x, e^y]\!]$.

The equation becomes

$$\left(\alpha_5 + \frac{1}{24}\right)[x,x,x,y] + (\alpha_6 + \alpha_7)[y,x,x,y] + \left(\alpha_8 - \frac{1}{24}\right)[y,y,x,y] = 0,$$

hence $\alpha_5 = -\frac{1}{24}$, $\alpha_6 + \alpha_7 = 0$ e $\alpha_8 = \frac{1}{24}$.

If we choose $\alpha_6 = \alpha_7 = 0$ we obtain

$$h_1(e^x, e^y) = e^z e^{-\frac{1}{2}V_2} e^{-\frac{1}{12}V_3} e^{\frac{1}{12}V_4} e^{-\frac{1}{24}V_5} e^{\frac{1}{24}V_8} \dots .$$

The first few components of h_1 are given by:

$$\begin{aligned} h_1(e^x, e^y) \quad = \quad & e^x e^y \llbracket e^x, e^y \rrbracket^{-\frac{1}{2}} \llbracket e^x, e^x, e^y \rrbracket^{-\frac{1}{12}} \llbracket e^y, e^x, e^y \rrbracket^{\frac{1}{12}} \\ & \llbracket e^x, e^x, e^x, e^y \rrbracket^{-\frac{1}{24}} \llbracket e^y, e^y, e^x, e^y \rrbracket^{\frac{1}{24}} \\ & \llbracket e^x, e^x, e^x, e^x, e^y \rrbracket^{-\frac{19}{720}} \cdots . \end{aligned}$$

For h_2 we have:

$$\begin{aligned} h_2(e^x, e^y) \quad = \quad & \llbracket e^x, e^y \rrbracket \llbracket e^x, e^x, e^y \rrbracket^{\frac{1}{2}} \llbracket e^y, e^x, e^y \rrbracket^{\frac{1}{2}} \llbracket e^x, e^x, e^x, e^y \rrbracket^{\frac{1}{3}} \\ & \llbracket e^y, e^x, e^x, e^y \rrbracket^{\frac{1}{4}} \llbracket e^y, e^y, e^x, e^y \rrbracket^{\frac{1}{3}} \\ & \llbracket e^x, e^x, e^x, e^x, e^y \rrbracket^{\frac{1}{4}} \cdots . \end{aligned}$$

Setting up the correspondence

We use h_1 and h_2 to go from a p-group G of order p^n and nilpotency class $c < p$ to a Lie ring of the same order and nilpotency class in the following way:

$$\begin{aligned} g + h &= h_1(g,h) = gh[\![g,h]\!]^{-\frac{1}{2}}[\![g,g,h]\!]^{-\frac{1}{12}}[\![h,g,h]\!]^{\frac{1}{12}} \\ &\quad [\![g,g,g,h]\!]^{-\frac{1}{24}}[\![h,h,g,h]\!]^{\frac{1}{24}}[\![g,g,g,g,h]\!]^{-\frac{19}{720}}\cdots, \\ [g,h] &= h_2(g,h) = [\![g,h]\!][\![g,g,h]\!]^{\frac{1}{2}}[\![h,g,h]\!]^{\frac{1}{2}}[\![g,g,g,h]\!]^{\frac{1}{3}} \\ &\quad [\![h,g,g,h]\!]^{\frac{1}{4}}[\![h,h,g,h]\!]^{\frac{1}{3}}[\![g,g,g,g,h]\!]^{\frac{1}{4}}\cdots, \end{aligned}$$

for all $g, h \in G$.

Let G be a p-group of nilpotency class $c < p$. There is a presentation of G, called the power-commutator presentation, with generators $g_1, \ldots, g_n$ and relations

$$\begin{array}{rcll} g_i^p & = & g_{i+1}^{\alpha_{i+1}^{(i)}} \cdots g_n^{\alpha_n^{(i)}}, & \text{for } 1 \leq i \leq n \text{ and } \alpha_k^{(i)} < p; \\ \llbracket g_j, g_i \rrbracket & = & g_{j+1}^{\beta_{j+1}^{(i,j)}} \cdots g_n^{\beta_n^{(i,j)}}, & \text{for } 1 \leq i < j \leq n \text{ and } \beta_k^{(i,j)} < p. \end{array}$$

For all $g \in G$, there are $\lambda_1, \ldots, \lambda_n < p$ such that

$$g = g_1^{\lambda_1} \cdots g_n^{\lambda_n}.$$

Theorem. Let $g = g_1^{\lambda_1} \cdots g_n^{\lambda_n} \in G$, for $\lambda_1, \ldots, \lambda_n < p$. There are $\mu_1, \ldots, \mu_n < p$ such that

$$g = \mu_1 g_1 + \ldots + \mu_n g_n.$$

Proof. By the Lazard correspondence

$$g = z(g_1^{\lambda_1}, g_2^{\lambda_2} \cdots g_n^{\lambda_n}) \;\Rightarrow\; g = \lambda_1 g_1 + g' \;\Rightarrow\; g' = -\lambda_1 g_1 + g$$

$$g_1^{\lambda_1} = \lambda_1 g_1 \;\Rightarrow\; g' = g_1^{-\lambda_1} + g.$$

Hence

$$g' = h_1(g_1^{-\lambda_1}, g) = g_1^{-\lambda_1} g \tilde{g} = g_2^{\lambda_2} \cdots g_n^{\lambda_n} \tilde{g},$$

where $\tilde{g} \in \langle g_3, \ldots, g_n \rangle$. It follows that $g' \in \langle g_2, \ldots, g_n \rangle$ and we can repeat the reasoning for g' an so on. □

In order to compute the Lie ring structure of G we transform the relations of G into relations that hold in the Lie ring.

For $1 \leq i < j \leq n$ we have

$$pg_i = g_i^p = g_{i+1}^{\alpha_{i+1}} \cdots g_n^{\alpha_n} = \beta_{i+1} g_{i+1} + \ldots + \beta_n g_n,$$

and

$$[g_j, g_i] = h_2(g_j, g_i) = g_{j+1}^{\gamma_{j+1}} \cdots g_n^{\gamma_n} = \delta_{j+1} g_{j+1} + \ldots + \delta_n g_n,$$

for some $\alpha_k, \beta_k, \gamma_k, \delta_k < p$.

Remark. Once we have the Lie ring structure on G we have two representation of a $g \in G$, a product representation (coming from the group structure) and a sum representation (coming from the Lie ring structure).
We can use the BCH-formula to efficiently switch between the representations.

Implementations

We have implemented the algorithms in MAGMA with a 3.16 GHz processor.

	h_1		h_2		BCH	
weight	time	# terms	time	# terms	time	# terms
12	526	1519	433	1517	0.13	985
13	2329	3055	2013	3053	0.47	2521
14	11137	6111	12493	6109	0.92	4056

Remark. The number of terms of the BCH-formula roughly doubles with each increase of the weight. The running times much more than double. So it will be possible to go a bit further (until weight 15 or 16), but we cannot realistically hope to go much beyond that.

The main operation for performing the Lazard correspondence is the evaluation of the BCH-formula for given x, y of a nilpotent Lie ring, and the formulae for h_1 and h_2 for given g, h of a p-group.

In order to do this efficiently, we encode these formulae as labeled binary trees.

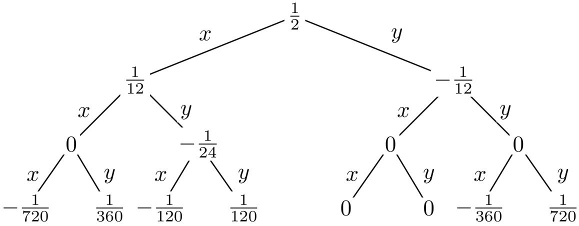
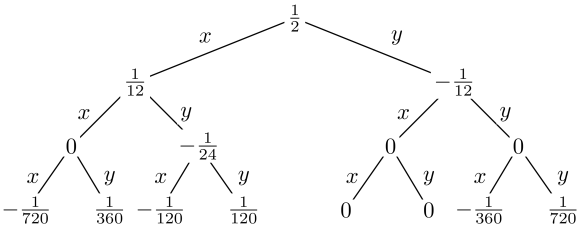
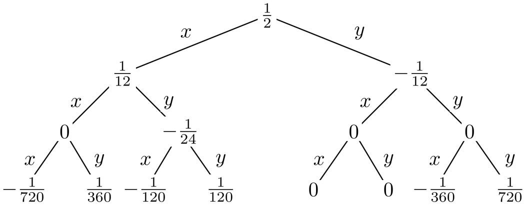


Figure: Tree corresponding to the part of the BCH-formula up to weight 5

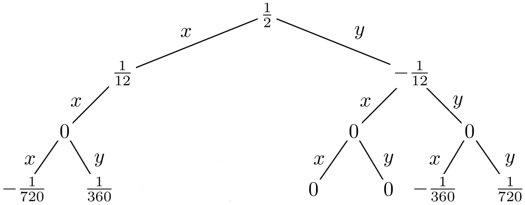


- The edges of the tree are labeled x or y;
- the root of the tree corresponds to $[x, y]$;
- every node corresponds to a commutator;
- every node has a label, which is the coefficient of the corresponding commutator in the BCH-formula;
- in order to determine the commutator corresponding to any other node, we take the path to the root, and record the labels.

Main advantage: when evaluating $z(x, y)$ we find that a certain commutator u in x and y is zero, then we can discard the entire subtree below the node corresponding to u.



If, for example, $[y, x, x, y] = 0$ the tree becomes:



A GAP package: LieRing

We have written a GAP package, LieRing that contains, among other things, an implementation of the algorithms for computing the Lazard correspondence. The package is able to deal with groups and rings up to class 14.

In particular it contains two functions:

- `PGroupToLieRing`: it computes the Lie ring structure of a p-group of class $< p$.
- `LieRingToPGroup`: it computes the group structure of a Lie ring of order p^n and class $< p$.

The functions `PGroupToLieRing` and `LieRingToPGroup` both return a record with 4 components:

- `pgroup`: the group;
- `liering`: the Lie ring;
- `GtoL`: a function mapping elements of the group to elements of the Lie ring;
- `LtoG`: a function mapping elements of the Lie ring to elements of the group.

Example. We take a 13-group G of class 5.

```
gap> F := FreeGroup(IsSyllableWordsFamily,"a","b","c","d", "e", "f", "g");;
gap> a := F.1;; b := F.2;; c := F.3;; d := F.4;; e := F.5;; f := F.6;; g:=F.7;;
gap> rels := [ a^13, b^13/g, c^13, d^13, e^13, f^13, g^13,
> Comm(b,a)/c, Comm(c,a)/d, Comm(d,a)/e, Comm(e,a)/f, Comm(f,a), Comm(g,a),
> Comm(c,b)/(g^11), Comm(d,b)/g, Comm(e,b)/g, Comm(g,b), Comm(d,c)/(g^12),
> Comm(e,c), Comm(f,c), Comm(g,c), Comm(e,d), Comm(f,d), Comm(g,d), Comm(f,e),
> Comm(g,e), Comm(g,f)];;
gap> G := PcGroupFpGroup( F/rels );
<pc group of size 62748517 with 7 generators>
gap> r:= PGroupToLieRing(G);
rec( pgroup := <pc group of size 62748517 with 7 generators>,
liering := <Lie ring with 6 generators>,
GtoL := function( g0 ) ... end, LtoG := function( x0 ) ... end )
gap> f:= r.GtoL; h:= r.LtoG;
function( g0 ) ... end
function( x0 ) ... end
gap> L:= r.liering;
<Lie ring with 6 generators>
gap> b:= Basis(L);
Basis( <Lie ring with 6 generators>, [ v_1, v_2, v_3, v_4, v_5, v_6 ] )
gap> h(b[1]);
a^12*c*d^5*e^3*f^8*g^7
gap> f(h(b[1]));
v_1
```

Example. We take a nilpotent Lie ring K of class 4 and order 7^7.

```
gap> L:= FreeLieRing( Integers, ["a","b","c"] );;
gap> a:= L.1;; b:= L.2;; c:= L.3;;
gap> rels:= [ (b*a)*b, c*a, c*b-(b*a)*a, 7^2*a, 7*b-((b*a)*a)*a, 7*c-((b*a)*a)*a];;
gap> K:= FpLieRing( L, rels );
<Lie ring with 5 generators>
gap> r:= LieRingToPGroup(K);
rec( pgroup := <pc group of size 823543 with 7 generators>,
liering := <Lie ring with 5 generators>,
LtoG := function( x0 ) ... end, GtoL := function( g0 ) ... end )
gap> G:= r.pgroup;; f:= r.LtoG;; h:= r.GtoL;;
gap> u:= Random(K);
6*v_1+3*v_2+6*v_3+46*v_4+47*v_5
gap> f(u);
f1^6*f2^4*f3^5*f4^2*f5^4*f6^5*f7^4
gap> h(f(u));
6*v_1+3*v_2+6*v_3+46*v_4+47*v_5
```

An application of the Lazard correspondence: non-commuting graphs

Definition. Let G be a non abelian group with center $Z(G)$. The non-commuting graph of G, denoted by $\Gamma(G)$, is the graph with vertices the elements of $G \setminus Z(G)$ and where

$$g \sim h \quad \Leftrightarrow \quad [\![g, h]\!] \neq 1.$$

Problem. Is it possible that two non-isomorphic groups have isomorphic non-commuting graphs?

Answer. Yes!

We prove that by means of 6-dimensional nilpotent Lie rings and the Lazard correspondence.

Definition. Let L be a Lie ring with center $Z(L)$. The non-commuting graph of L, denoted by $\Gamma(L)$, is the graph with vertices the elements of $L \setminus Z(L)$ and

$$x \sim y \quad \Leftrightarrow \quad [x, y] \neq 0.$$

Consider the nilpotent Lie rings $L_1 \ncong L_2$ of order p^6, class $3 < p$:

$$L_1 := \langle y_1, \ldots, y_6 \mid [y_1, y_2] = y_4, [y_1, y_3] = y_5, [y_2, y_4] = y_6, [y_3, y_5] = y_6 \rangle,$$
$$L_2 := \langle x_1, \ldots, x_6 \mid [x_1, x_2] = x_4, [x_1, x_3] = x_5, [x_2, x_4] = x_6, [x_3, x_5] = 2x_6 \rangle.$$

Claim. $\Gamma(L_1) \cong \Gamma(L_2)$.

Proof. Let $u_1 = \alpha_1 x_1 + \ldots + \alpha_6 x_6, u_2 = \beta_1 x_1 + \ldots + \beta_6 x_6 \in L_2$.

$$\begin{aligned} [u_1, u_2]_{L_2} &= (\alpha_1\beta_2 - \alpha_2\beta_1)x_4 + (\alpha_1\beta_3 - \alpha_3\beta_1)x_5 \\ &\quad + (\alpha_2\beta_4 - \alpha_4\beta_2 + 2\alpha_3\beta_5 - 2\alpha_5\beta_3)x_6. \end{aligned}$$

Let $\psi : L_2 \to L_1$ with $\psi(x_5) = 2y_5$ and $\psi(x_i) = y_i$ for $i \neq 5$.

$$\begin{aligned} [\psi(u_1), \psi(u_2)]_{L_1} &= (\alpha_1\beta_2 - \alpha_2\beta_1)y_4 + (\alpha_1\beta_3 - \alpha_3\beta_1)y_5 \\ &\quad + (\alpha_2\beta_4 - \alpha_4\beta_2 + 2\alpha_3\beta_5 - 2\alpha_5\beta_3)y_6. \end{aligned}$$

$$\Rightarrow \quad u_1 \sim u_2 \;\Leftrightarrow\; \psi(u_1) \sim \psi(u_2) \quad \Rightarrow \quad \Gamma(L_2) \cong \Gamma(L_1). \quad \square$$

By the Lazard correspondence, to L_2 and L_1 correspond two p-groups G_2 and G_1.

Remark. Let L be a Lie ring of order p^n and nilpotency class at most $c < p$ and let G be the p-group that corresponds to L. For all $x, y \in L$ we have

$$0 \mapsto 1, \quad Z(L) \mapsto Z(G), \quad \text{and} \quad [x,y] = 0 \Leftrightarrow [\![g,h]\!] = 1$$

where $x \mapsto g$ and $y \mapsto h$.

Conclusion. $G_2 \ncong G_1$ and $\Gamma(G_2) \cong \Gamma(G_1)$.

Thank you!