An Example CRIME calculation: The cohomology ring of Q_8

September 6, 2006

Let $G = Q_8 = \left\langle x, y \,\middle|\, x^2 = y^2 = (xy)^2, x^4 = 1 \right\rangle = \left\langle x, y, z \,\middle|\, x^2 = y^2 = z = (xy)^2, x^4 = 1 \right\rangle$. Observe that z in the second presentation is redundant, but simplifies the notation later. In GAP, we execute the following commands.

```
gap> G:=SmallGroup(8,4);
<pc group of size 8 with 3 generators>
gap> Pcgs(G);
Pcgs([ f1, f2, f3 ])
```

Then a little manipulation in GAP reveals that `f1`, `f2`, and `f3`, correspond with x, y, and z from the presentation above, and with i, j, and -1 from the standard presentation of Q_8.

Let $k = \mathbb{F}_2$. It's well known that k has a periodic minimal kG-projecive resolution. To see this, we start with the following commands.

```
gap> C:=CohomologyObject(G);
<object>
gap> ProjectiveResolution(C,10);
[ 1, 2, 2, 1, 1, 2, 2, 1, 1, 2, 2 ]
```

`ProjectiveResolution` returns the kG-ranks of the terms of the minimal projective resolution. These numbers are called the *Betti numbers* of the resolution. Therefore, this tells us that k has a minimal kG-projective resolution

$$P_* : \qquad \cdots \longrightarrow kG \xrightarrow{\partial_4} kG \xrightarrow{\partial_3} (kG)^2 \xrightarrow{\partial_2} (kG)^2 \xrightarrow{\partial_1} kG \xrightarrow{\epsilon} k \longrightarrow 0 \tag{1}$$

We can see from (1) that P_* appears to be periodic, but we confirm this below by looking at the boundary maps. The map ϵ is the usual augmentation $\epsilon\left(\sum_g \alpha_g g\right) = \sum_g \alpha_g$.

Since P_* is minimal, the cohomology groups $H^i(G) = \mathrm{Ext}^i(k,k)$ are simply

$$\mathrm{Hom}_{kG}(P_i, k) = k^{b_i}.$$

Here, b_i is the $(i+1)$st element in the list returned by `ProjectiveResolution`, so the first element in this list is the dimension of P_0. Thus, the Betti numbers give the ranks of the cohomology groups as well.

To look at the boundary maps, we need some notation. Recall that for G a p-group of size p^n and k a field of characteristic p, which is exactly the situation that we're in in this example, the group algebra kG has a basis

$$\mathcal{B}' = \left\{ x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} \middle| 0 \le a_1, a_2, \dots a_n \le p-1 \right\} \tag{2}$$

where $x_1, x_2, \dots x_n$ is a polycyclic generating set for G. In fact, the fact that $\mathcal{B}'$ is a basis merely expresses the fact the $x_1, x_2, \dots x_n$ is a polycyclic generating set. In the example $G = Q_8$, arranging the $(a_1, a_2, \dots, a_n)$'s in reverse lexicographic order, we have

$$\begin{aligned} \mathcal{B}' &= \left(\begin{array}{cccccccc} 1, & x, & y, & xy, & z, & xz, & yz, & xyz \end{array} \right) \\ &= \left(\begin{array}{cccccccc} 1, & i, & j, & k, & -1, & -i, & -j, & -k \end{array} \right). \end{aligned}$$

However, a more computationally efficient basis of kG is the following.

$$\mathcal{B} = \left\{ (x_1 - 1)^{a_1} (x_2 - 1)^{a_2} \dots (x_n - 1)^{a_n} \middle| 0 \le a_1, a_2, \dots a_n \le p-1 \right\} \tag{3}$$

Let $I = x + 1$, $J = y + 1$, and $K = xy + 1$. Observe that $I^2 = J^2 = z + 1$. Observe also that $K = I + J + IJ$. The element K was included to make the boundary maps below look more symmetric. Then in the example $G = Q_8$ we have

$$\mathcal{B} = \left(\begin{array}{cccccccc} 1, & I, & J, & IJ, & I^2, & I^3, & I^2J, & I^3J \end{array} \right)$$

The boundary maps returned by `BoundaryMaps` are with respect to the basis $\mathcal{B}$.

```
gap> Display(BoundaryMap(C,1));
. 1 . . . . . .
. . 1 . . . . .
gap> Display(BoundaryMap(C,2));
. 1 . . . . . . . . 1 . . . . .
. . 1 . . . . . . 1 1 1 . . . .
gap> Display(BoundaryMap(C,3));
. . 1 . . . . . . 1 1 1 . . . .
gap> Display(BoundaryMap(C,4));
. . . . . . . 1
gap> Display(BoundaryMap(C,5));
. 1 . . . . . .
. . 1 . . . . .
```

Observe first that $\partial_5 = \partial_1$, so we see that P_* is in fact periodic as mentioned above. The matrices for ∂_n give only the image of 1_G from each direct factor of P_n, since the images of the the other elements of P_n are determined by linearity. [1] For example, since

$$\partial_1 : P_1 = kG \oplus kG \to P_0 = kG,$$

the matrix returned above tells us that $\partial_1(1_G, 0) = I$ and $\partial_1(0, 1_G) = J$. Summarizing the information above, we have the following.

[1]Note to users: if the matrices giving the action of kG on itself with respect to $\mathcal{B}$, or the full matrices for the ∂_n's would be useful to users, please let me know. I could include functions to return them, but I hesitate to overload the user with superfluous information.

$$
\partial_n = \begin{cases} \begin{pmatrix} I \\ J \end{pmatrix} & \text{if } n \equiv 1 \pmod 4 \\ \begin{pmatrix} I & J \\ J & K \end{pmatrix} & \text{if } n \equiv 2 \pmod 4 \\ \begin{pmatrix} J & K \end{pmatrix} & \text{if } n \equiv 3 \pmod 4 \\ \begin{pmatrix} I^3 J \end{pmatrix} & \text{if } n \equiv 0 \pmod 4 \end{cases} \qquad (n \geq 1) \tag{4}
$$

The matrices in (4) are meant to be multiplied on the right as usual in GAP.

Now since $H^1(G) = \mathrm{Hom}_{kG}(P_1, k)$, we have a natural basis $\{\eta_1, \eta_2\}$ of $H^1(G)$ where η_1 is the map sending $(1_G, 0) \mapsto 1_k$ and $(0, 1_G) \mapsto 0$ and η_2 is the other way around.

Then the following are chain maps representing η_1 and η_2.

$$
\begin{tikzcd}
P_3 \arrow[r, "(J\ K)"] \arrow[d, "(0\ 1)"'] & P_2 \arrow[r, "\left(\begin{smallmatrix} I & J \\ J & K \end{smallmatrix}\right)"] \arrow[d, "\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)"'] & P_1 \arrow[d, "\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)"'] \arrow[dr, "\eta_1"] & \\
P_2 \arrow[r, "\left(\begin{smallmatrix} I & J \\ J & K \end{smallmatrix}\right)"'] & P_1 \arrow[r, "\left(\begin{smallmatrix} I \\ J \end{smallmatrix}\right)"'] & P_0 \arrow[r, "\epsilon"] & k
\end{tikzcd}
\qquad
\begin{tikzcd}
P_3 \arrow[r, "(J\ K)"] \arrow[d, "(1\ 1)"'] & P_2 \arrow[r, "\left(\begin{smallmatrix} I & J \\ J & K \end{smallmatrix}\right)"] \arrow[d, "\left(\begin{smallmatrix} 0 & 1 \\ 1+J & 1 \end{smallmatrix}\right)"'] & P_1 \arrow[d, "\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)"'] \arrow[dr, "\eta_2"] & \\
P_2 \arrow[r, "\left(\begin{smallmatrix} I & J \\ J & K \end{smallmatrix}\right)"'] & P_1 \arrow[r, "\left(\begin{smallmatrix} I \\ J \end{smallmatrix}\right)"'] & P_0 \arrow[r, "\epsilon"] & k
\end{tikzcd}
\tag{5}
$$

In the rows of the diagrams in (5) we have copies of P_*, while in the columns, we have maps making the diagrams commute. These maps were produced by inspection and by . . . well, let's just say that I used GAP a tiny bit. Fortunately, this is exactly what the CRIME package does for us, as we will see below.

For the purpose of multiplication, the pictures in (5) represent η_1 and η_2, so the composition of the two pictures represents the product, as in the following picture.

$$
\begin{tikzcd}
P_3 \arrow[r] \arrow[d, "(0\ 1)"'] & P_2 \arrow[r] \arrow[d, "\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)"'] & P_1 \arrow[d, "\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)"'] \arrow[dr, "\eta_1"] & \\
P_2 \arrow[r] \arrow[d, "\left(\begin{smallmatrix} 0 & 1 \\ 1+J & 1 \end{smallmatrix}\right)"'] & P_1 \arrow[r] \arrow[d, "\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)"'] \arrow[dr, "\eta_2"] & P_0 \arrow[r, "\epsilon"] & k \\
P_1 \arrow[r] & P_0 \arrow[r, "\epsilon"] & k &
\end{tikzcd}
\tag{6}
$$

From (6), we can see that $\eta_1\eta_2 = \zeta_2$ where $\{\zeta_1, \zeta_2\}$ is the natural basis of $H^2(G)$. This is the map going from P_2 in the top row to k in the bottom, as in the diagrams in (5).

By composing the first diagram with itself, we find that $\eta_1^2 = \zeta_1$. Similarly, by more chain map production and composition, we find that $\eta_2\zeta_2$ is a nonzero element of degree 3, but that no product of elements of degree < 4 produces a nonzero element of degree 4.

Let $\{\xi\}$ be the natural basis of $H^4(G)$. We lift ξ to a chain map.

$$
\begin{tikzcd}
P_8 \arrow[r, "(I^3 J)"] \arrow[d, "1"'] & P_7 \arrow[r, "\left(\begin{smallmatrix} J \\ K \end{smallmatrix}\right)"] \arrow[d, "1"'] & P_6 \arrow[r, "\left(\begin{smallmatrix} I & J \\ J & K \end{smallmatrix}\right)"] \arrow[d, "1"'] & P_5 \arrow[r, "(I\ J)"] \arrow[d, "1"'] & P_4 \arrow[d, "1"] \arrow[dr, "\xi"] & \\
P_4 \arrow[r, "(I^3 J)"'] & P_3 \arrow[r, "\left(\begin{smallmatrix} J \\ K \end{smallmatrix}\right)"'] & P_2 \arrow[r, "\left(\begin{smallmatrix} I & J \\ J & K \end{smallmatrix}\right)"'] & P_1 \arrow[r, "(I\ J)"'] & P_0 \arrow[r, "\epsilon"] & k
\end{tikzcd}
\tag{7}
$$

This time, the production of the chain map is easy because of the periodicity of P_*. From (7), we see that all the elements of degree 4–7 arise as products of ξ with elements of degree 0–3, which in turn are products of η_1 and η_2.

Thus, by recursion, we find that η_1, η_2, and ξ generate the entire ring $H^*(G)$. This is precisely what GAP tells us from the following commands.

```
gap> CohomologyGenerators(C,10);
[ 1, 1, 4 ]
gap> A:=CohomologyRing(C,10);
<algebra of dimension 17 over GF(2)>
gap> LocateGeneratorsInCohomologyRing(C);
[ v.2, v.3, v.7 ]
```

`CohomologyGenerators` merely tells us the degrees of the generators, and they agree with those which we computed above.

The ring returned by `CohomologyRing` has basis `[A.1, A.2, .. A.17]` corresponding with the concatenation of the natural bases of the $H^i(G)$'s. Thus, `A.1` is the identity element, `A.2` and `A.3` correspond with η_1 and η_2, `A.4` and `A.5` correspond with ζ_1 and ζ_2, etc. Observe that $17 = \sum_{i=0}^{10} b_i$ which explains the dimension of A. The true cohomology ring is infinite-dimensional, so that A can be seen as a degree-10-truncation, that is, $A \cong H^*(G)/J_{>10}$ where $J_{>10}$ is the subring of all elements of degree > 10.

The following commands verify the calculations mentioned above.

```
gap> A.2^2;
v.4
gap> A.2*A.3;
v.5
gap> A.3*A.5;
v.6
```

The command `LocateGeneratorsInCohomologyRing` tells us that η_1, η_2, and ξ correspond with `A.2`, `A.3`, and `A.7`, which we had already deduced by degree considerations, but if $\dim H^4(G)$ had been greater than 1, we wouldn't have known which element corresponded with ξ.

Finally, GAP gives us a presentation of $H^*(G)$ with the following command.

```
gap> CohomologyRelators(C,10);
[ [ z, y, x ], [ z^2+z*y+y^2, y^3 ] ]
```

This tells us that

$$H^*(G) \cong k[z,y,x] \big/ \left(z^2 + yz + y^2, y^3\right)$$

is a polynomial ring in the variables z, y and x, modulo the ideal generated by $z^2 + yz + y^2$ and y^3.