Mathematical Formula Manipulation from a User's Point of View

Arjeh M. Cohen
Centre for Mathematics and Computer Science
P.O. Box 4079, 1009 AB Amsterdam, The Netherlands
Department of Mathematics, University of Utrecht
Budapestlaan 6, 3584 CD Utrecht, The Netherlands

I discuss two applications from my own experience of the use of computer algebra software packages to mathematics. The first is concerned with finding a closed formula for an expression I came across in finite geometry, the second deals with compiling and solving a set of polynomial equations in order to establish the existence of a particular finite subgroup of the complex Lie group of type E_6.

Software packages for mathematics are becoming more widely available and very useful to pure mathematicians. Although we should not expect them to essentially change the way mathematical research is being conducted, they allow the mathematician to verify conjectures more thoroughly, to dismiss routine calculations to machine work and to compute more effectively than is possible by hand. I expect that computer algebra systems will play an important role in many stages of mathematical research, such as 1° testing (instances of) hypotheses and helping in developing them, and 2° proving explicit results that are of calculational nature, but too tedious and complicated to be performed by hand. Below I present an example of each type, taken from my own work. Both have been worked out in MAPLE. For other interesting examples, composed by someone with more experience than I have, see [4]. My first example illustrates how a computer algebra software system can be of use in finding a closed formula for an expression determined by recursion, the second how an existence proof can be given for a subgroup of a Lie group that has hitherto not been established otherwise.

1. Finding a closed formula

Before going into the example itself, let me display the strategy by a completely trivial example: suppose we wish to find a closed formula for the geometric progression

$$1 + x + x^2 + \cdots + x^n .$$

If we refer to this expression as $geom(x,n)$, it will be clear that it is given by the following MAPLE procedure:

```
# recursion for geom
geom := proc(x, n)
        if n < 0 then 0
        else geom(x, n—1)+x^n fi
end:
```

Now imagine that via some trial and error we have come to the conclusion that, for $x \neq 1$, the following closed formula

$$\frac{1 - x^{n+1}}{1 - x}$$

is a suitable candidate for *geom*(x,n). Denote it by *geomapp*(x,n) (the suffix *app* to remind us that we are still dealing with an approximation at this stage). The following procedure computes it.

```
#  the hypothesised closed formula
 geomapp := proc (x,n)
                  (1 - x^(n+1))/(1 - x)
 end:
```

So far, there is hardly a noticeable difference with ordinary computer programs. In ordinary languages a check of the following nature would be performed :

```
for i to 2 do print (geomapp (2,i)); print(geom(2,i))
od;
```

giving output '3 3 7 7'. Now symbolic computation manifests itself through the presence of the variable x: the command

```
geom(x,3);
```

and the command

```
normal(geomapp(x,3));
```

both yield

$$1 + x + x^2 + x^3 .$$

Of course there are limitations; the command

```
geom(x,n);
```

triggers the response

```
Error, (in geom) cannot evaluate boolean
```

We now come to the actual example based on the same idea. The analog of *geom* is a recursively defined formula, called $a(n,m,j,l,k,e)$, counting objects from a certain finite geometry (a polar space) determined by the parameters n

and e, in a certain position (determined by the parameters j, k, and l) with respect to a given object (specified by the parameter m). The footnote[1] contains a more detailed description for the interested reader (those not familiar with finite geometry are well advised to skip it.) Further geometric details are to be found in [1].

Elementary properties of the underlying geometric object (polar spaces), make it clear that $a(n,m,j,l,k,e)$ satisfies the properties laid down in the recursive procedure below. These properties determine $a(n,m,j,k,l,e)$ uniquely. Before giving the procedure, we introduce two auxiliary functions, namely $gaussq(n,k)$ and $polargaussq(n,k,e)$. [They represent the number of k-dimensional linear subspaces of the vector space of dimension n over the field with q elements and singular subspaces of rank $k+1$ of the polar space with parameters n, e, respectively.] They are given by the following closed formulae:

$$gaussq(n,k)=\prod_{i=1}^{k}\frac{q^{n-i+1}-1}{q^i-1}\ ,$$

$$polargaussq(n,k,e)=gaussq(n,k)\cdot\prod_{i=0}^{k-1}(q^{n+e-i-1}+1)\ .$$

In MAPLE language, for the q-Binomial coefficient *gaussq*:

```
gaussq := proc(n,k)
local answ, kk;
answ := 1;
if (k > n) then answ := 0 fi;
if k <= n then
        for kk to k do
                answ := answ*(q^(n - kk + 1) - 1)/(q^kk - 1);
        od
fi;
answ
end:
```

and, for the 'polar variation' *polargaussq*:

1. The *polar space* of a quadric of rank n is an incidence system derived from a nondegenerate quadratic form on a vector space V of Witt index n. A point of this incidence system is a 1-dimensional subspace contained in V on which the quadratic form vanishes; more generally, a singular subspace of the polar space (of rank m) is an $m+1$-dimensional subspace of V on which the form vanishes identically. We shall be concerned with the case where the ambient vector space V is finite, whence defined over a finite field of order, say q. Then the dimension of V is either $2n$ or $2n+1$. Let e be 0 or 1 depending on whether V has even or odd dimension. (The reason for incorporating e is that there are more polar spaces, left out of the present discussion for the sake of exposition, see [loc cit].) Now let x be a fixed singular subspace of our polar space of dimension m. Then $a(n,m,j,l,k,e)$ stands for the number of $(k+l+j)$-dimensional spaces y with

$$\dim(x\cap y)=j \quad \text{and} \quad \dim(x^{\perp}\cap y)=j+l,$$

where $\perp$ denotes the usual orthogonal space in V with respect to the given quadratic form.

```
polargaussq := proc(n,k,e)
local answ, ii;
answ := 1;
if (k > n) then answ := 0 fi;
if k <= n then
        for ii from 0 to k-1 do
            answ:= answ*(q^(n + e - ii - 1) + 1)
        od
fi;
answ*gaussq(n,k)
end:
```

Now we are in a position to describe - using MAPLE - the function *a* as determined from geometric observations.

```
# the recursive approach
a := proc (n,m,j,l,k,e)
local ii,jj,answ;
# in the following cases there are no objects as required:
if m>n or j>m or l+m>n or j+k+l>n then answ := 0
else
  # reduction to the case j=0
  if (m>=j) and (j>0) then answ := a(n - j,m - j,0,l,k,e)*gaussq(m,j) fi;
  # a trivial case:
  if j=0 and k=0 and l=0 then answ := 1 fi;
  # reduction ot the case where k=0
  if j=0 and l>0 and k>0 then answ := a(n,m,0,l,0,e)*a(n - l,m,0,0,k,e) fi;
  # a case in which a closed formula can be given:
  if j=0 and l>0 and k=0 then answ := polargaussq(n - m,l,e)*q^(l*m) fi;
  # the remaining case in which we only the answer by excluding many other
  # cases, which are known by recursion:
  if j=0 and l=0 and k>0 then
        answ := polargaussq(n,k,e);
        for ii to k do
            answ := normal(answ - a(n,m,ii,0,k - ii,e))
        od;
        for ii from 0 to k do
            for jj from 1 to k - ii do
                answ := normal(answ - a(n,m,ii,jj,k - ii - jj,e))
            od;
        od;
  fi;
  normal(answ)
  end:
```

Going over the reductions and experimenting a little interactively, I got the

following candidate for a closed formula, to which I will refer as *aapp*(n,m,j,l,k,e):

```
aapp := proc(n,m,j,l,k,e)
local answw;
answ := gaussq(m,j)*polargaussq(n - m,l,e)*q^(l*(m - j));
answ := answ*gaussq(m - j,k)*q^((2*(n - l) - j - m+e - 1)*k - k*(k - 1)/2);
normal(answ)
end:
```

Running a few instances gives strong indications that we are on the right track:

```
  a(1,2,3,4,5,6);
                              0
>
  aapp(1,2,3,4,5,6);
                              0
>
  a(12,3,1,1,1,1);
   20   2              8    7    6    5    4    3    2              9
  q   (q  + q + 1) (q  + q  + q  + q  + q  + q  + q  + q + 1) (q  + 1) (q + 1)
>
  aapp(12,3,1,1,1,1);
   20   2              8    7    6    5    4    3    2              9
  q   (q  + q + 1) (q  + q  + q  + q  + q  + q  + q  + q + 1) (q  + 1) (q + 1)
>
  a(6,2,1,1,1,0);
                        7          3    2          3
                       q  (q + 1) (q  + q  + q + 1) (q  + 1)
>
  aapp(6,2,1,1,1,0);
                        7          3    2          3
                       q  (q + 1) (q  + q  + q + 1) (q  + 1)
>
  aapp(5,2,1,0,1,1);
                              7
                             q  (q + 1)
>
  a(5,2,1,0,1,1);
                              7
                             q  (q + 1)
```

Thus, a good hypothetical formula has been found much quicker than by conventional methods. Now it is not too hard to provide a proof that the formula given in *aapp* is the right one, i.e., that

$$a(n,m,j,l,k,e)=$$
$$gaussq(m,j)\cdot polargaussq(n-m,l,e)\cdot$$
$$gaussq(m-j,k)\cdot q^{l(m-j)+((2(n-l)-j-m+e-1)k-k(k-1)/2)}.$$

In fact, such a proof can be found in [loc cit].

2. Solving a set of polynomial equations to embed a finite group in $E_6(\mathbb{C})$

We shall now be concerned with a proof of a mathematical fact that seems to be hard to establish without a lot of computation:

The fractional linear group $L=L(2,19)$ over the field $\mathbb{Z}/19\mathbb{Z}$ of 19 elements of order 3420 embeds in the complex Lie group E of type E_6.

In [2], it turns out that L is one of the few nonabelian finite simple groups for which an embedding in E exists. The discussion below reports on the construction given in [loc cit]. For 'easier' (e.g. nilpotent) groups, there are criteria that make it relatively straightforward to decide whether or not they are subgroups of E. The strategy of the construction of an embedding of L in E is to first construct an embedding of an easier group (namely the one of order 171 generated by the elements u and t given below), and next to search for a suitable element (in fact the element w below) in E such that the easier group together with w generate the required group L. At this second stage, straightforward numerical work enables us to find w as a 27 by 27 matrix whose entries are polynomials with 6 indeterminates. From there on, we make essential use of the features of a computer algebra package to find appropriate values for the indeterminates, which upon substitution in the entries of w, turn w into the required element of E.

To embed L, we use the observation that L is the unique nontrivial group generated by two elements u and w satisfying the following relations

$$u^{19}=w^2=1,$$
$$(uw)^3=(u^2w)^{19}=1.$$

Using the well-known presentation of $L=L(2,19)$ as the set of pairs $\{a, -a\}$ ofnonsingular 2 by 2 - matrices a, the elements u and w of L correspond to

$$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \text{ and } \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \text{ respectively.}$$

The complex Lie group E of type E_6 is regarded as a set of 27 by 27 matrices. To be precise E will be taken to be the set of all invertible 27 by 27 matrices preserving the cubic form F on $\mathbb{C}^{27}$ given by

$$F(x_a)_{1\leqslant a\leqslant 27}=\det(x_{ij}^{(1)})+\det(x_{ij}^{(2)})+\det(x_{ij}^{(3)})-\operatorname{trace}(x_{ij}^{(1)})(x_{ij}^{(2)})(x_{ij}^{(3)}),$$

where $x_{jk}^{(i)}$ $(1\leqslant i,j,k\leqslant 3)$ stands for x_a with $a=i+3(j-1)+9(k-1)$. Details will appear in joint work with D.B. Wales [loc cit]. Rather than in the complex Lie group, we shall embed L in a finite counterpart of E, namely the

so-called nonsplit central extension $\bar{E}$ of the Chevalley group $E_6(6841)$. This greatly simplifies the amount of computations needed. This group $\bar{E}$ can be viewed just as E, the only difference being that, instead of taking the complex numbers, we now take as scalars $\mathbb{Z}/6841\mathbb{Z}$, the field of integers modulo 6841. (The form F, defined over the integers, gives rise to a well-defined form on $\mathbb{Z}/6841\mathbb{Z}$). This is allowed because of the more general observation that, if H is a finite group whose order is not divisible by the prime number p, and G a Chevalley group such that H embeds in $G(\mathbb{Z}/p\mathbb{Z})$ (the group defined over the field of order p), then H embeds in the complex Lie group $G(\mathbb{C})$. [*Proof* (as worked out in joint work with R.L. Griess): since the kernel of the natural morphism $G(\mathbb{Z}/p^n\mathbb{Z}) \to G(\mathbb{Z}/p^{n-1}\mathbb{Z})$ is a p-group, there is a subgroup isomorphic to H in the inverse image of a subgroup of $G(\mathbb{Z}/p^n\mathbb{Z})$ isomorphic to H; it follows that H can be embedded in

$$\lim_{\leftarrow} G(\mathbb{Z}/p^n\mathbb{Z}) \cong G(\lim_{\leftarrow}(\mathbb{Z}/p^n\mathbb{Z})) = G(\mathbb{Z}_p),$$

where $\mathbb{Z}_p$ denotes the ring of p-adic integers, and, using that $\mathbb{Z}_p$ embeds in $\mathbb{C}$, we obtain a group embedding of $G(\mathbb{Z}_p)$ in $G(\mathbb{C})$, leading to the required embedding of H in $G(\mathbb{C})$]. Using the theory of Lie groups, it is not hard to find the right choice for u (up to conjugacy) in $\bar{E}$. We get

$u =$

2128 663 3618 173 775 1715 6494 644 2836 2925 1813 3817 4276 5981 4782 4505 2059 4303 2688 3237 2396 6379 4992 2357 6156 5553 971
1329 4988 1690 1493 956 3225 2192 3519 4326 6305 73 1772 6822 2586 6236 6543 5914 5388 3421 4782 2784 5560 2655 5169 5972 1932 1323
6557 5659 4988 1067 64 685 6290 5973 2793 6301 5504 935 731 4755 6118 827 6041 1313 3495 6715 3832 6639 829 2968 3738 2787 1105
3162 5583 1133 5990 3103 4385 6212 3416 2997 4932 76 561 1271 3673 5986 5630 687 6791 2844 2924 3884 6226 914 2348 4334 4242 5644
4836 2520 1081 681 4988 2813 6233 5850 1385 4423 4478 1839 5467 4749 1746 2572 2178 2731 28 340 248 4445 2266 3525 5708 459 6514
270 5603 5885 4979 4331 6612 6631 2479 4361 2688 188 43 6387 4671 3690 636 2746 4352 3744 3007 2846 6053 2952 6773 70 2799 2370
6579 3238 5669 5685 6634 1815 5 6110 1793 6478 1414 6813 1537 3972 6146 2645 6614 5743 834 1979 2598 109 1860 5902 4768 4891 585
34 1157 5068 4233 2201 5964 4163 4988 3915 2957 3067 1110 1172 0 6226 3024 2019 4938 5033 5265 1805 1882 561 5874 2784 6634 6331
11107 2917 4456 4310 2085 2124 1763 4999 3364 3511 5936 1181 2999 6339 4389 1173 1330 2216 4683 2178 11 2742 447 431 605 3327 3077
6993 6717 4821 5233 5626 5088 3849 5957 2338 5990 835 869 1651 994 4227 237 1944 5523 2329 254 2608 2523 2107 5470 2585 613 4193
2420 121 3778 262 1906 5469 872 3718 5618 2302 163 874 1554 4271 4449 2671 75 1997 2306 4235 1077 2354 5456 397 6617 5124 4941
5303 6355 3857 6188 4966 6161 6802 2268 5725 6234 4559 4988 6595 4740 2021 6197 1238 6834 207 2899 2353 4699 1843 3020 124 6581 4269
65 3183 2678 599 1506 4366 4984 551 5085 1381 4698 1070 5 3240 2104 380 2892 5001 3069 5086 3420 4084 6217 2941 2609 5648 4872
90 924 5713 5552 3791 4196 3839 6748 5353 4739 2242 5809 6060 522 3885 6598 1858 2560 3712 6265 119 4769 4622 3997 5416 3443 3558
6348 3737 6697 1396 6513 205 6016 1407 4079 2500 4539 2731 4063 37 5156 332 1372 4550 4626 2269 2271 3535 1493 792 1345 4480 414
5343 202 1281 4442 2505 886 6490 1538 2420 4473 2545 6807 5388 1685 1735 2128 6104 4448 1900 5726 3777 3856 3142 4693 478 3216 194
3512 3668 1226 4611 5101 867 6478 2929 3084 669 5510 3557 5311 1014 4794 5019 597 4328 6182 4108 2899 6838 620 5855 6249 4825 3419
218 2357 6801 5253 4100 5384 6619 2583 2779 6434 5837 3189 2214 2820 2946 586 5180 4820 6608 291 5471 1626 3850 794 1250 2499 3696
4793 5436 6384 786 39 5740 3148 4005 6357 3508 789 608 160 2000 5822 5043 6759 2307 5 2653 119 5017 1166 2967 110 6627 3309
3122 1378 4270 3290 2403 6541 5406 4034 2857 2631 75 5084 4548 6358 2065 1236 5622 4709 5545 2972 6795 2361 1614 2336 5079 3247 705
6222 5772 5256 884 662 2677 4749 4268 4884 3425 3112 2902 1405 977 5956 4640 1045 5104 3658 3403 4988 6066 1912 4135 1842 3544 4065
6315 6014 298 5184 619 149 3062 3547 5839 2434 2960 5941 3906 3196 4522 5137 1953 1590 2298 179 2005 2128 286 6541 249 54 544
5910 5811 115 4717 5962 561 4768 2964 3042 2583 6125 5004 4736 0 6803 6056 4409 4041 2178 2079 3560 3952 2613 2220 4199 5974 2105
6327 1906 3830 6072 539 5004 444 4577 4152 2909 2402 4620 1602 4382 6778 4046 3169 4037 5886 4327 5066 3040 2312 3196 3327 5487 4771
6285 607 6160 3922 5774 5810 3705 4520 3140 2995 3660 536 2 632 4329 6268 5914 3823 2630 1456 971 2609 5965 442 5990 2557 5830
5969 3173 2220 588 4151 2185 5517 6342 2113 2277 6212 3913 3130 3623 4408 2993 6766 5449 3062 174 917 1832 3626 3828 3237 2538 332
284 3800 6763 331 1773 5608 141 2376 3422 3951 1643 6309 3486 4121 5394 5353 5177 4002 3274 64 6037 3353 926 1771 4255 1506 6780

As a matter of fact, we have given u in such a way that the element t of L corresponding to the 2 by 2 matrices

$$\pm \begin{bmatrix} 2 & 0 \\ 0 & 10 \end{bmatrix}$$

over $\mathbb{Z}/19\mathbb{Z}$ has diagonal shape on $(\mathbb{Z}/6841\mathbb{Z})^{27}$ with respect to a very special basis, namely a basis for a maximal torus of $\overline{E}$. [This has been achieved by means of elaborate t-eigenspace computations in the same software package; we do not discuss them here as they are of a numerical nature.] This implies that w has a pretty shape: its 27 rows are:

$[1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

$[0,0,264ze/a,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

$[0,596a/ze,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,863a^2b,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,0,0,2079abze,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,0,0,1263ybae+5854xyaz+987az,0,0,0,0,0,0,0,0,$
$987xaz+5578bae,0,0,0,0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,6705a,0,0,0,0,0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,5142ez,0,0,0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,0,0,987ybae+915xyaz+5926az,0,0,0,0,0,0,0,0,$
$5926xaz+5854bae,0,0,0,0,0,0,0]$

$[0,0,0,1086/(a^2b),0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

$[0,0,0,0,0,6840(3609eb+6236xz)/(zeab),0,0,$
$4(808yeb+1559z+5282xyz)/(zeab),0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

$[0,0,0,0,4202/(baze),0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,6839a(2321xz+956eb)/(ze),0,0,$
$2a(2321z+4520xyz+5885yeb)/(ze),0,0,0,0,0,0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,(3418yeb+2155xyz+4686z)/(ab),0,0,0,0,0,0,0,0,$
$6840,(3418eb+2155xz)/(ab),0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2806/(ab),0,0,0,0,0]$

$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,6837(432eb+47xz)/(zeb),0,0,$
$4(47z+6794xyz+6409yeb)/(zeb)]$

$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,5(6410yeb+349xyz+6492z)/(ba),0,0,0,0,0,0,0,0,$
$6836(6410eb+349xz)/(ba),0,0,0,0]$

$[0,0,0,0,0,0,3672/a,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$

$[0,0,0,0,0,6840(5321eb+360,9xz)/(abze),0,0,$

$$9(929yeb+401z+6440xyz)/(abze),0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$$

$$[0,0,0,0,0,0,0,6233/(ze),0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]$$

$$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1553ba,0,0,0,0,0,0,0,0,0,0,0]$$

$$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,6833a(239xz+214eb)/(ze),0,0,$$

$$8a(239z+6602xyz+6627yeb)/(ze),0,0,0,0,0,0,0,0,0]$$

$$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1466xyz+5375z+6379yeb,0,0,0,0,0,0,0,0,$$

$$5375xz+462eb,0,]$$

$$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0]$$

$$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,6839(745eb+864xz)/(zeb),0,0,$$

$$144(12z+6829xyz+2365yeb)/(zeb)]$$

$$[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,949xyz+5892z+5375yeb,0,0,0,0,0,0,0,0,$$

$$5892xz+1466eb,0]$$

for certain $a,b,e,z,x,y \in \mathbb{Z}/6841\mathbb{Z}$. At this stage, we know that each nonzero choice of a,b,e,z,x,y leads to an element of E. But which choice leads to a matrix w satisfying the required relations? This problem is solved by use of the character that the group L must have when it atcs as a subgroup of E on $\mathbb{C}^{27}$. From Lie group theory, we know it must be the character $9_a + 18_c$ (up to algebraic conjugacy) in the notation of the ATLAS [3]. Taking values modulo 6841, this determines the trace of the matrix $u^i w$ for each i ($0 \leqslant i \leqslant 18$).

For $i=0$, equating trace $(u^i w)$ to this value gives the identity $3=3$ (rows 1,13, and 25 contribute 1 each), but for $i=1$, it gives:

$$3989a+6490ez+3961a^2b+4521abze+2974a^2be+$$

$$8123a^2bze+1847xaz+1324xz^2ae+3891a^3bz+6460bae+$$

$$435aez+6326xa^2z+4231xz^2a^2be+184a^3b^2e+28a^2bz^2e+$$

$$1182z^2ae+128a^2be^2z^2+1693yb^2a^3e^2z+4316a^3z^2be+4011xa^3z^2be+$$

$$338az+2525xya^3z^2be+4436ye^2abz+5659xyz^2ae+6508e^2abz+$$

$$4559e^2b^2a^2z+6225ye^2b^2a^2z+6813xyz^2a^2be+2493a^3b^2ez+1278a^3b^2e^2z+$$

$$1019a^4b^2ez+2855a^3bez+2504ybae+1245a^3b^2z^2e^2+2080yba^2e+$$

$$1613a^3b+2950a^3xybz+6503xyaz+2199xya^2z+2638e^2z^2ba+$$

$$4642a^2z+4193a^3xbz+2392a^3yb^2e$$

$$=0.$$

In the subsequent 17 equations, i.e., those for $i=2,\cdots,18$, the same monomials occur. To exploit this phenomenon, I used Gauss elimination. Here is the

key routine (Ron Sommeling introduced me to MAPLE with a first version of it):

```
# read a standard routine for extracting coefficients of terms in a
   polynomial:
readlib(coeftayl):
p:= 6841:
# the key routine depending on the number t of the equation selected
# the polynomial preserve representing the pivoting term
gauss := proc(t,preserve)
local aa,bb,ci,ee,zz,xx,yy,i,cb;
aa := degree(t,a):   bb := degree(t,b):   ee := degree(t,e):
zz := degree(t,z):   xx := degree(t,x):   yy := degree(t,y):
cb := coeftayl(eqs[preserve], [a,b,e,z,x,y]=[0,0,0,0,0,0],
                              [aa,bb,ee,zz,xx,yy]) mod p;

if cb = 0 then print('error   cb = 0')
else     for i to 19 do
                        if i < > preserve then
                              ci:= coeftayl(eqs[i],
                                    [a,b,e,z,x,y]=[0,0,0,0,0,0],
                                    [aa,bb,ee,zz,xx,yy]) mod p;
                              eqs[i]:=
                                    (cb*eqs[i]-ci*eqs[preserve])
                                    mod p
                        fi
                  od
   fi;
   end:
```

The crucial MAPLE session consisted of running repeatedly and interactively the routine *gauss* with 'hand picked' row numbers t and monomials *preserve* in order to decrease the number of monomials in each equation (this number is 43 in the above equation for $i=1$). This resulted in fairly simple equations, which by use of standard commands in MAPLE, enabled me to find the following solution: $a=1492$; $b=631$; $e=2146$; $x=4372$; $y=1744$; $z=818$. Finally, a check that

$$w^2=(uw)^3=(u^2w)^{19}=1$$

established that the elements u and w generate a subgroup of $\bar{E}$ isomorphic to L. The point to be made here is that the computations were too cumbersome to be done by hand. Note that, apart from verification of the relations on u and w, all that is actually needed for the proof that L embeds in $\bar{E}$ is to verify that the 27 by 27 matrices over $\mathbb{Z}/6841\mathbb{Z}$ found for u and w (i.e., the one obtained by substuting the values for a,b,e,x,y,z in the matrix for w whose rows are given above) indeed preserve the form F (that is, the version over $\mathbb{Z}/6841\mathbb{Z}$); this is straightforward, but extremely tedious to verify by hand.

References

1. A.E. Brouwer, A.M. Cohen, A. Neumaier (1988). *Distance Regular Graphs,* Ergebnisse, Springer, Berlin (to appear).
2. A.M. Cohen, D.B. Wales (1988). *Finite Subgroups of $F_4(\mathbb{C})$ and $E_6(\mathbb{C})$,* in preparation.
3. J.H. Conway, R.T. Curtis, S.P. Norton, R.P. Parker, R.A. Wilson (1985). *Atlas of Finite Groups,* Clarendon Press, Oxford.
4. A.M. Odlyzko (1985). Applications of symbolic mathematics to mathematics. R. Pavelle (ed.). *Applications of Computer Algebra,* Kluwer, Dordrecht, 95-111.