A.V.Isogenies, a library for computing isogenies between abelian varieties

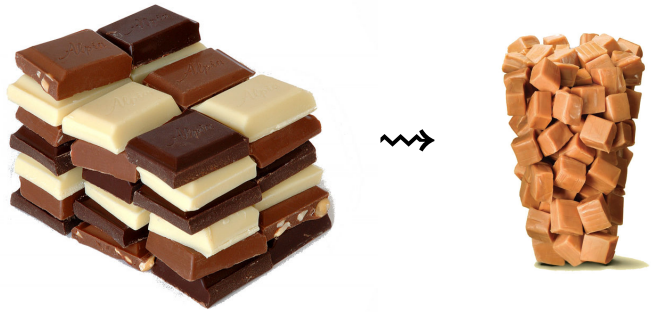
Gaetan Bisson Romain Cosset Damien Robert

CARAMEL group
LORIA, Nancy, France

s/CACAO/CARAMEL/g

Who are these people?

s/CACAO/CARAMEL/g



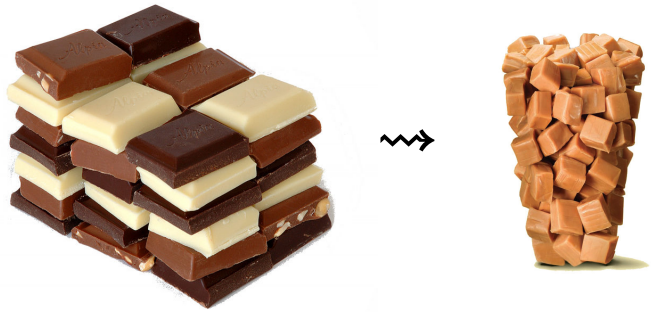
Who are these people?

SERIOUS PEOPLE

Jérémie D.
Pierrick G.
Emmanuel T.
Paul Z.

→ ECC'11

s/CACAO/CARAMEL/g

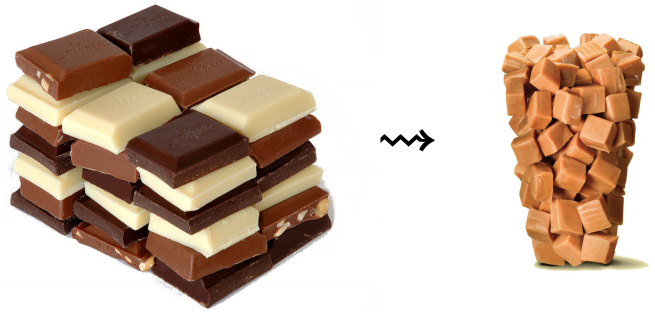


Who are these people?

SERIOUS PEOPLE	YOUNG GUYS
Jérémie D.	Gaetan B.
Pierrick G.	Romain C.
Emmanuel T.	Nicolas E.
Paul Z.	Damien R.

→ ECC'11

s/CACAO/CARAMEL/g



Who are these people?

SERIOUS PEOPLE	YOUNG GUYS
Jérémie D.	Gaetan B.
Pierrick G.	Romain C.
Emmanuel T.	~~Nicolas E.~~
Paul Z.	Damien R.

→ ECC'11

The way *they* code

```
    d[5],Q[999                  ]={0};main(N                  C,A,
  (;i--;e=scanf("%"           "d",d+i));for(A               R,a,
 ++i<A          ;++Q[        i*i%          A],R=           M,E,
R:i);             for(;i   --;)             for(M          L,i=
--;N              +=!M*Q   [E%A             ],e+=          5,e,
+E*E-            R*L*      L%A)            %A])          ){for
  E=i,L=M,a=4;a;C=             i*E+R*M*L,L=(M*E           =*d;
    %A,E=C%A+a                  --[d]);printf           i[Q]?
                                                        =A;M
                                                        Q[(A
                                                         for(
                                                         +i*L)
                                                          ("%d"
                                                           "\n",
                                                            (e+N*
                                                              N)/2
                                                              -A);}
```

The way *they* code

```
    d[5],Q[999
  (;i--;e=scanf("%"
 ++i<A          ;++Q[
R:i);             for(;i
--;N              +=!M*Q
+E*E-            R*L*
  E=i,L=M,a=4;a;C=
    %A,E=C%A+a
```

```
     ]={0};main(N
  "d",d+i));for(A
 i*i%          A],R=
--;)            for(M
[E%A            ],e+=
 L%A)           %A])
  i*E+R*M*L,L=(M*E
   --[d]);printf
```

```
      C,A,
    R,a,
  M,E,
 L,i=
5,e,
){for
=*d;
i[Q]?
=A;M
Q[(A
 for(
 +i*L)
  ("%d"
   "\n",
    (e+N*
      N)/2
      -A);}
```

≈ 250 glyphs

The way *they* code

counts points on Jacobians of genus-two curves

```
    d[5],Q[999                  ]={0};main(N                    C,A,
  (;i--;e=scanf("%"           "d",d+i));for(A                  R,a,
 ++i<A          ;++Q[        i*i%          A],R=              M,E,
R:i);             for(;i   --;)             for(M             L,i=
--;N              +=!M*Q  [E%A              ],e+=            5,e,
+E*E-            R*L*     L%A)             %A])           ){for
  E=i,L=M,a=4;a;C=            i*E+R*M*L,L=(M*E             =*d;
    %A,E=C%A+a                 --[d]);printf             i[Q]?
                                                        =A;M
                                                        Q[(A
                                                         for(
                                                         +i*L)
                                                          ("%d"
                                                           "\n",
                                                            (e+N*
                                                              N)/2
                                                              -A);}
```

≈ 250 glyphs

The way *they* code

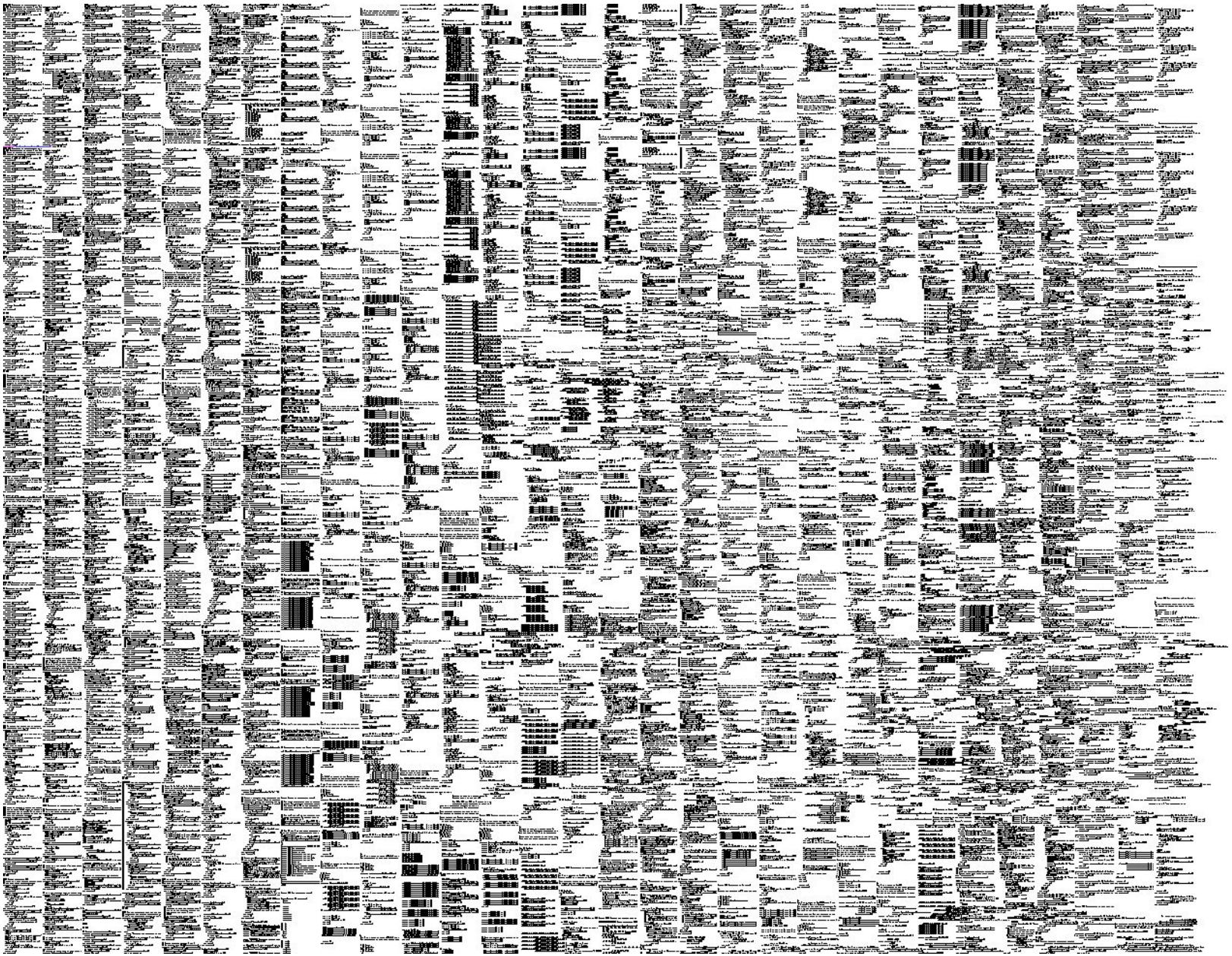
counts points on Jacobians of genus-two curves

```
    d[5],Q[999                    ]={0};main(N                      C,A,
  (;i--;e=scanf("%"             "d",d+i));for(A                   R,a,
 ++i<A          ;++Q[          i*i%          A],R=                M,E,
R:i);             for(;i     --;)             for(M               L,i=
--;N              +=!M*Q   [E%A              ],e+=                5,e,
+E*E-             R*L*      L%A)             %A])              ){for
  E=i,L=M,a=4;a;C=              i*E+R*M*L,L=(M*E                 =*d;
    %A,E=C%A+a                   --[d]);printf                i[Q]?
                                                              =A;M
                                                              Q[(A
                                                               for(
                                                               +i*L)
                                                                ("%d"
                                                                 "\n",
                                                                  (e+N*
                                                                    N)/2
                                                                    -A);}
```

≈ 250 glyphs

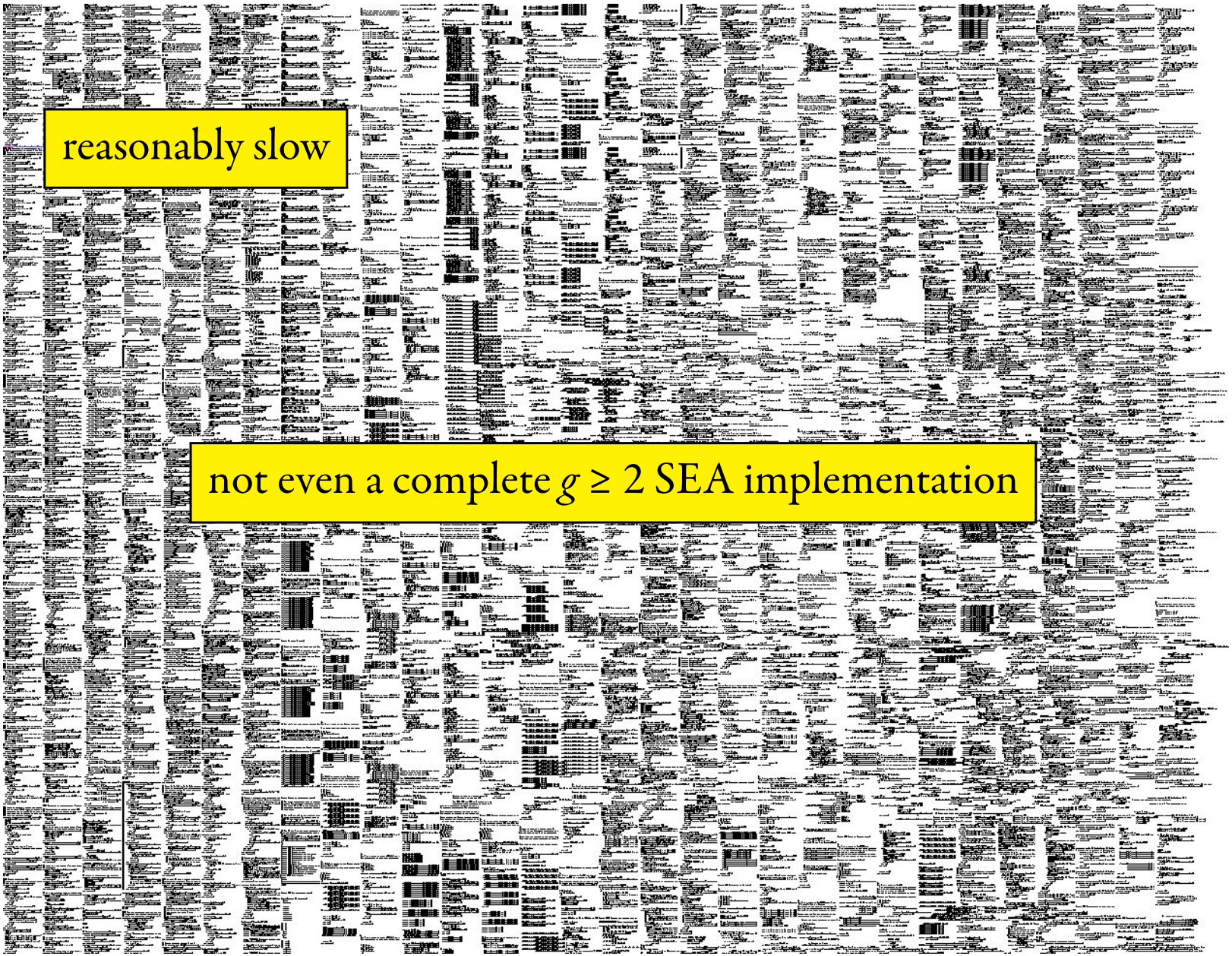
reasonably fast

The way *we* code

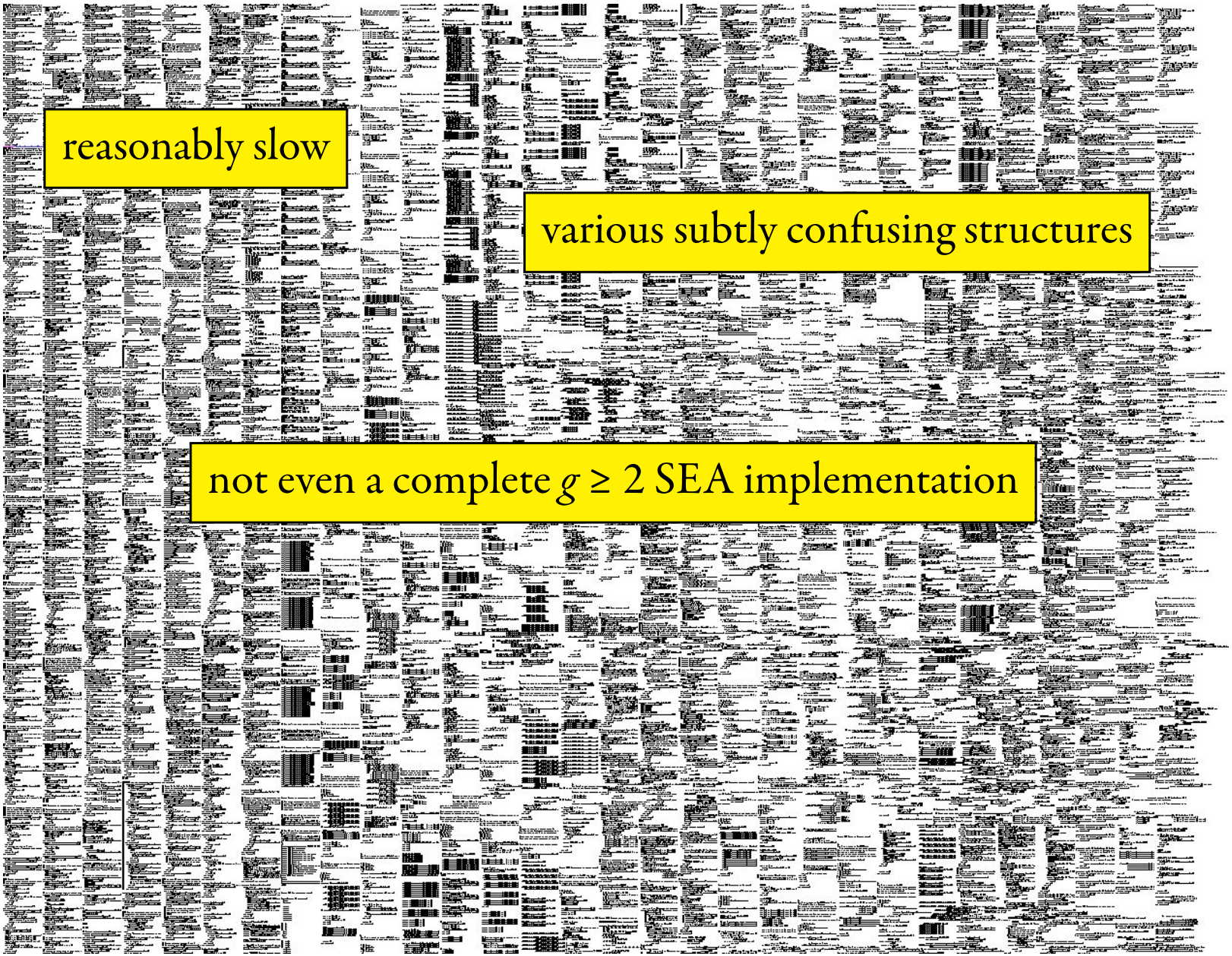


The way *we* code

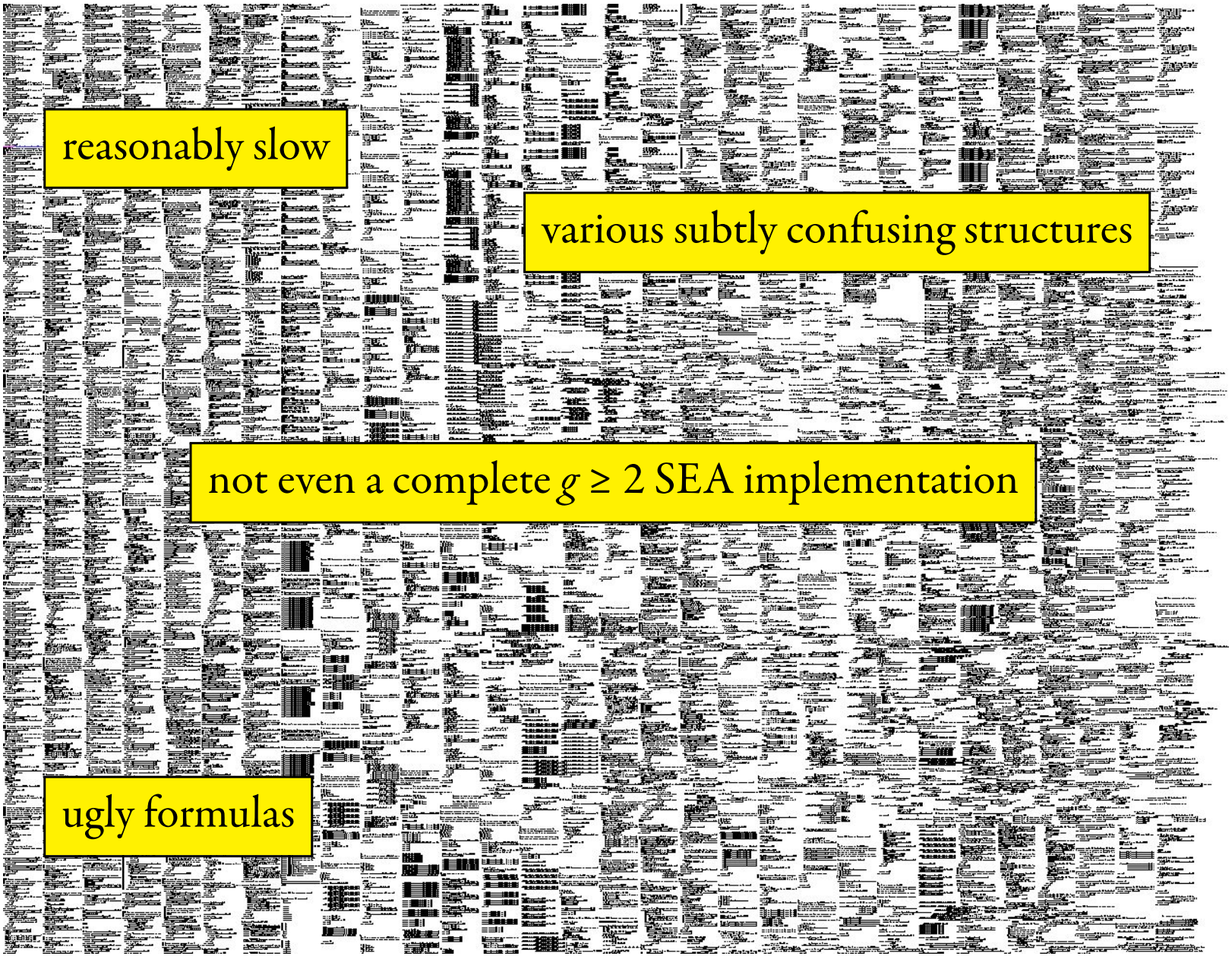
The way *we* code



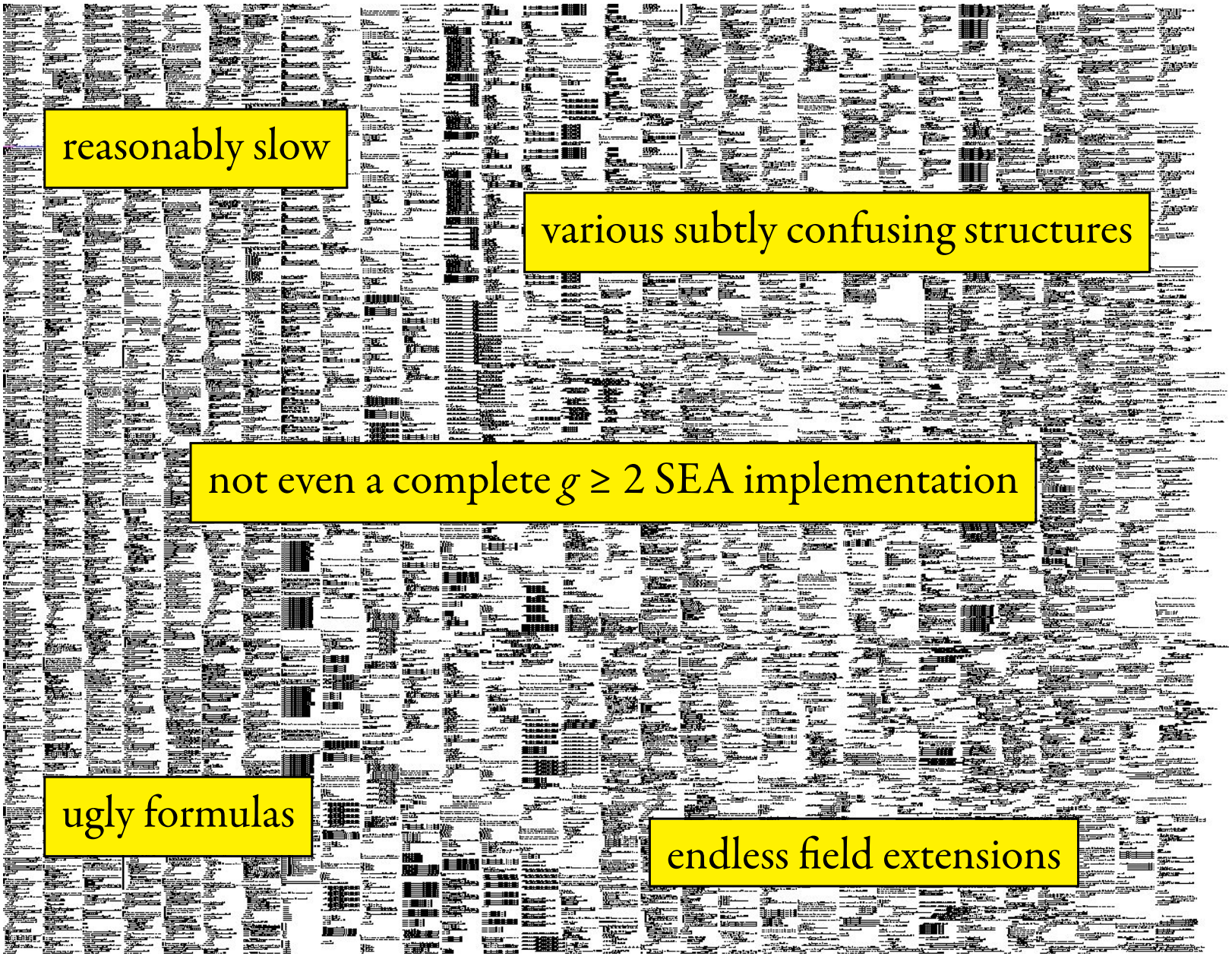
The way *we* code



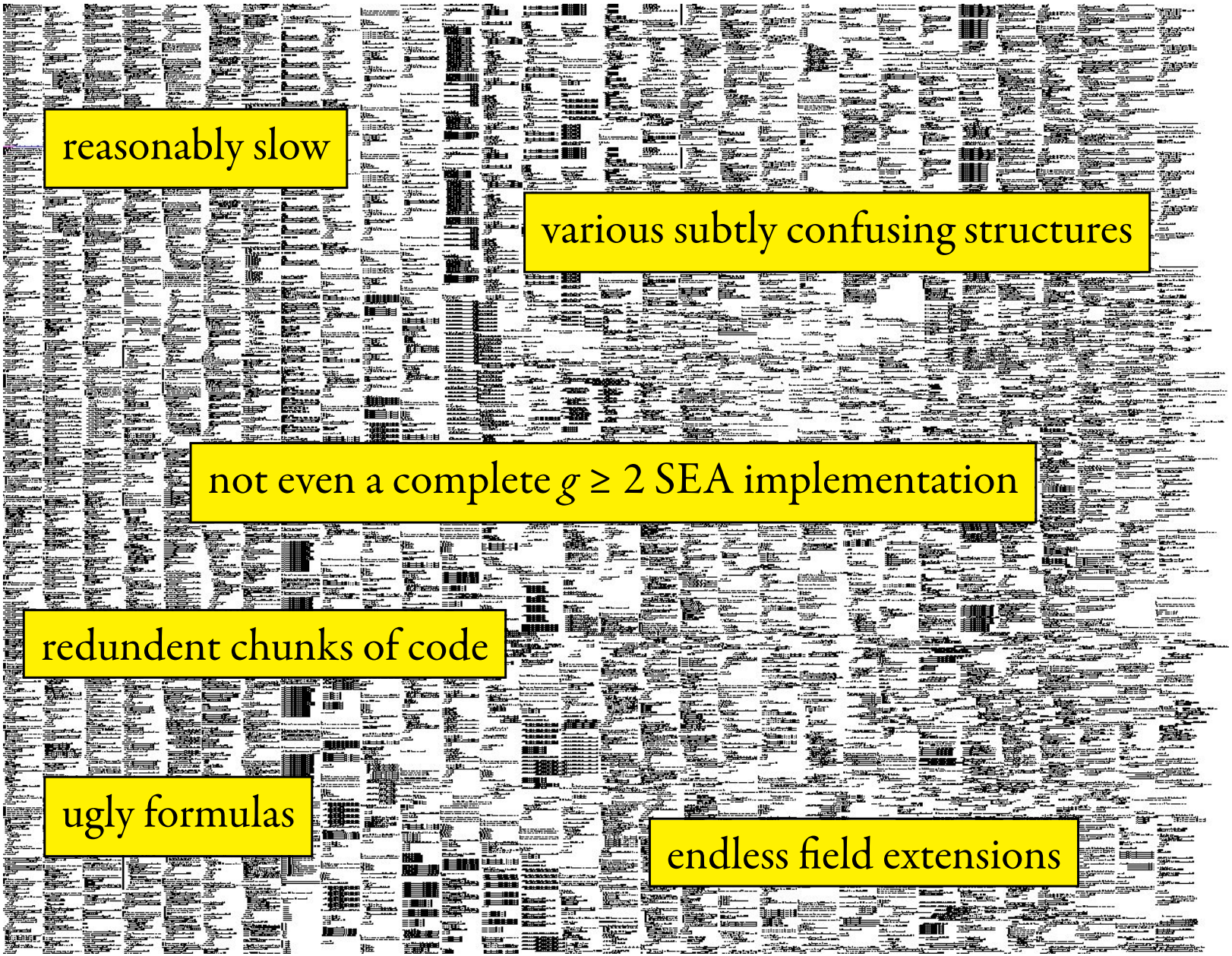
The way *we* code



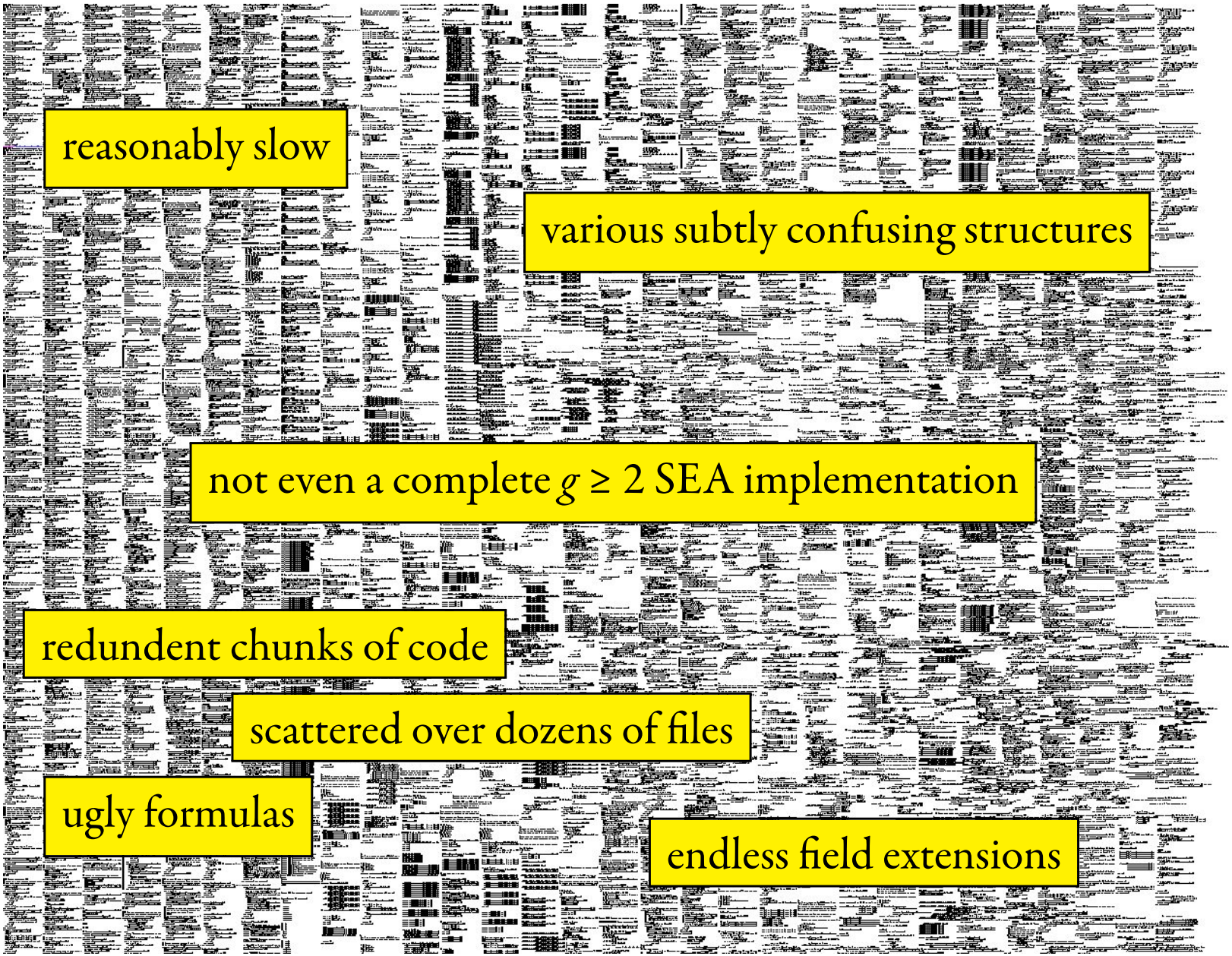
The way *we* code



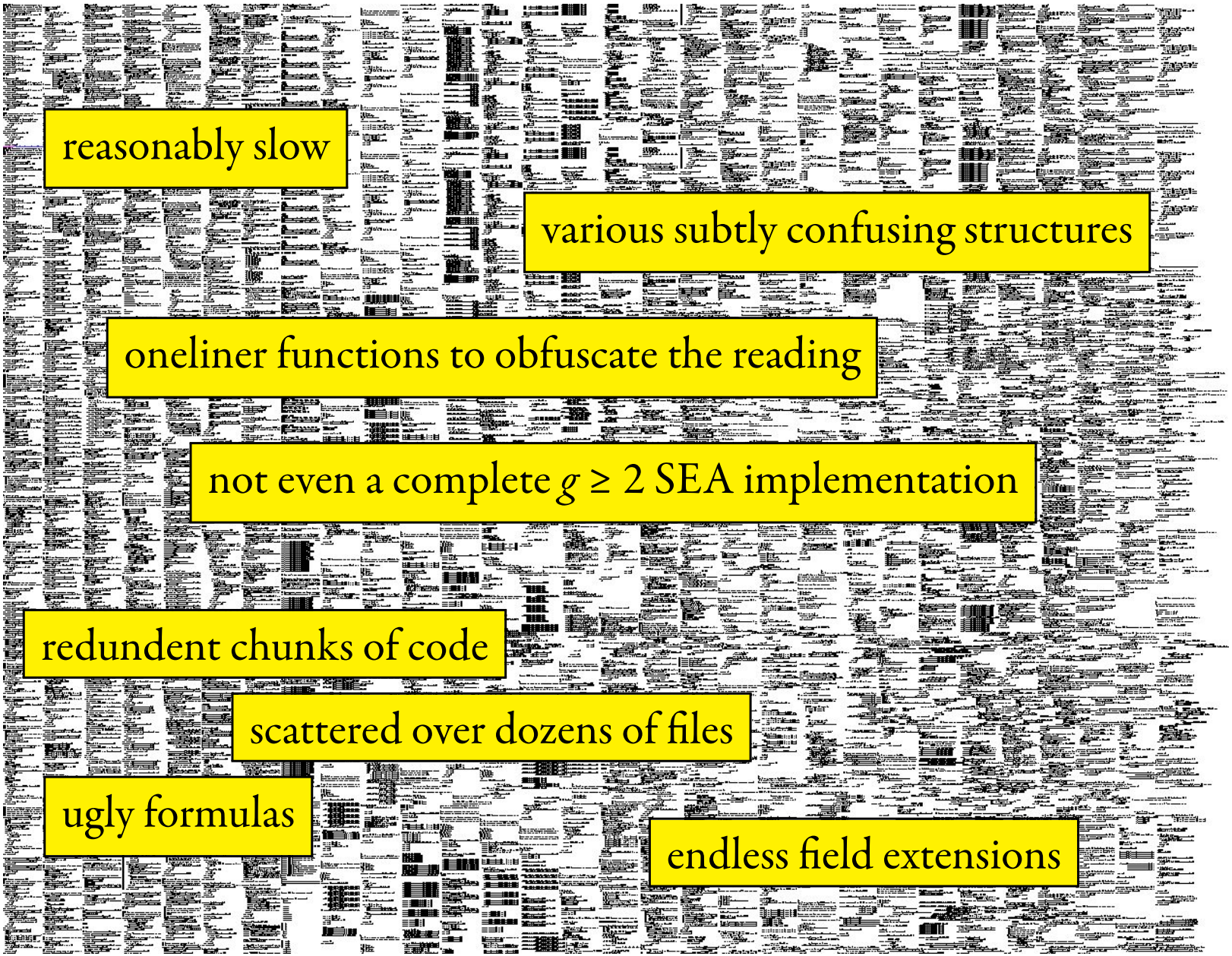
The way *we* code



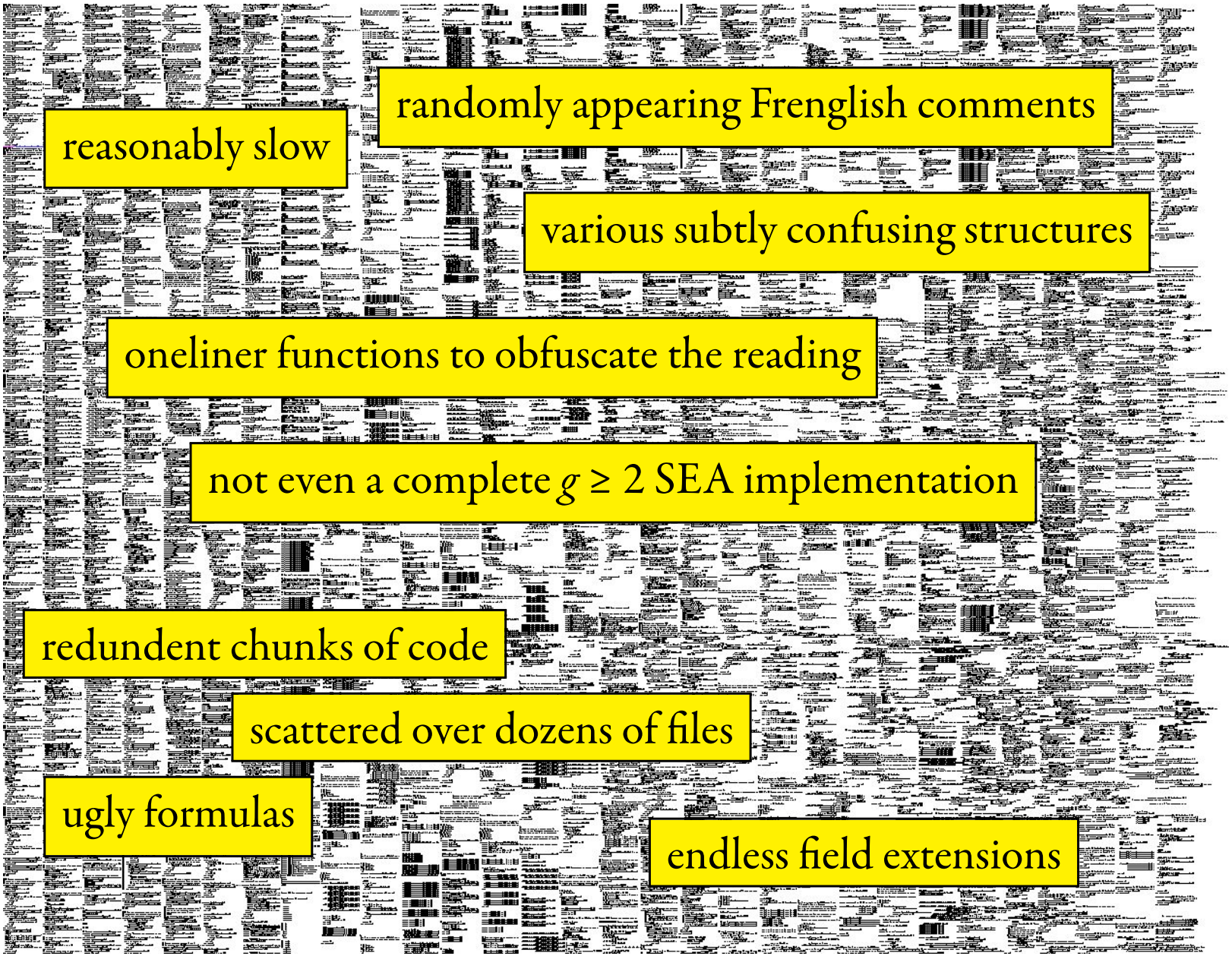
The way *we* code



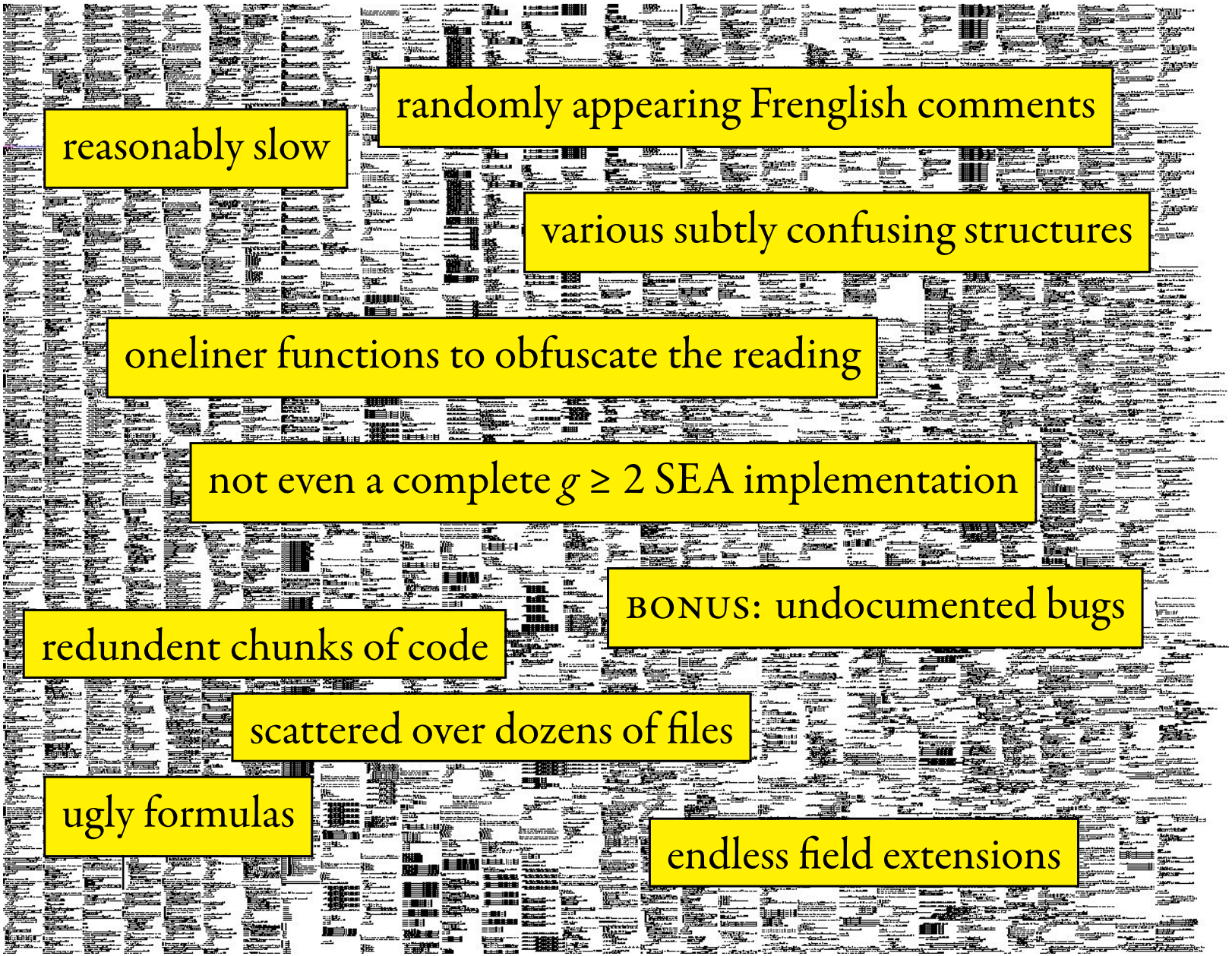
The way *we* code



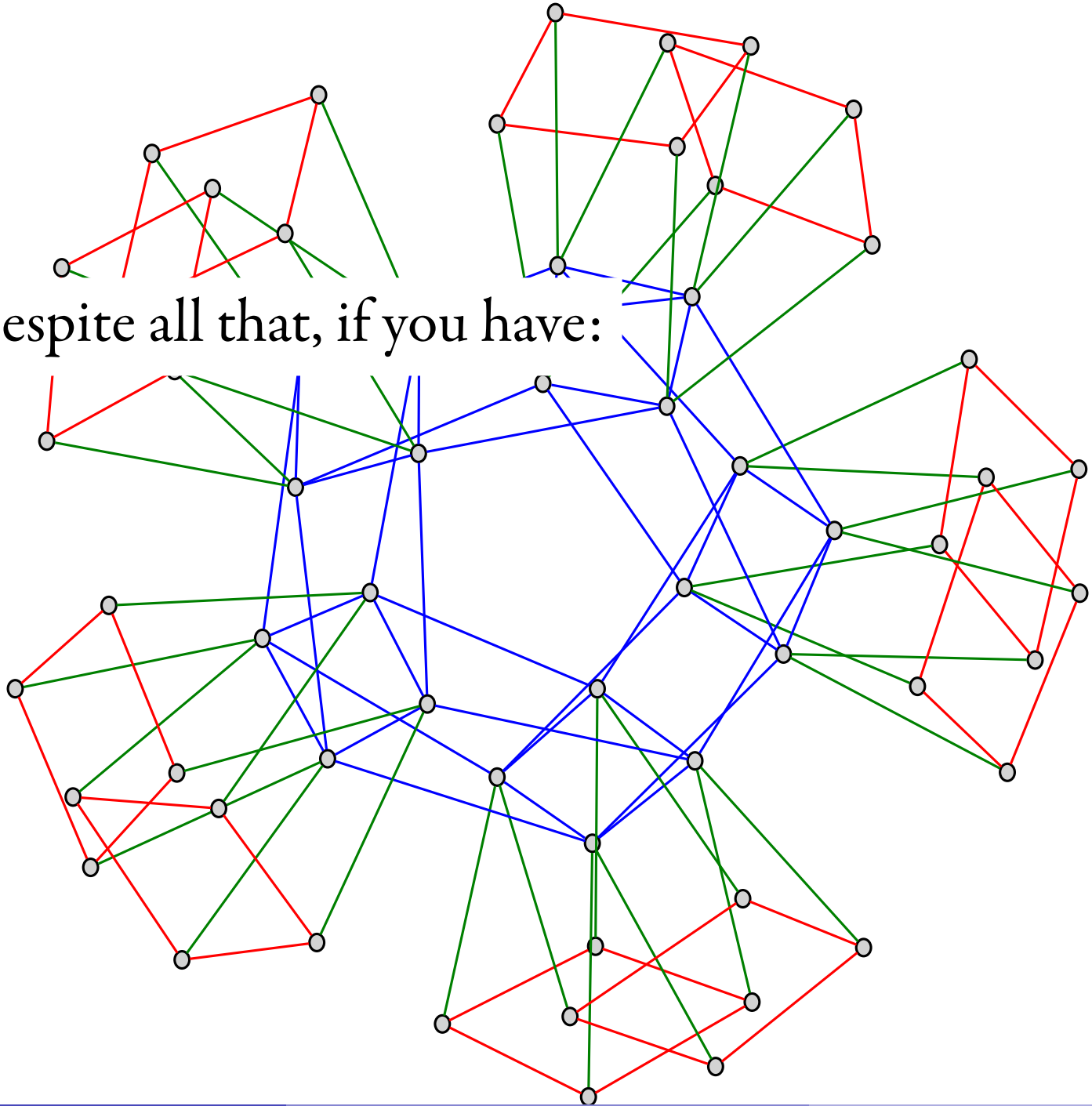
The way *we* code

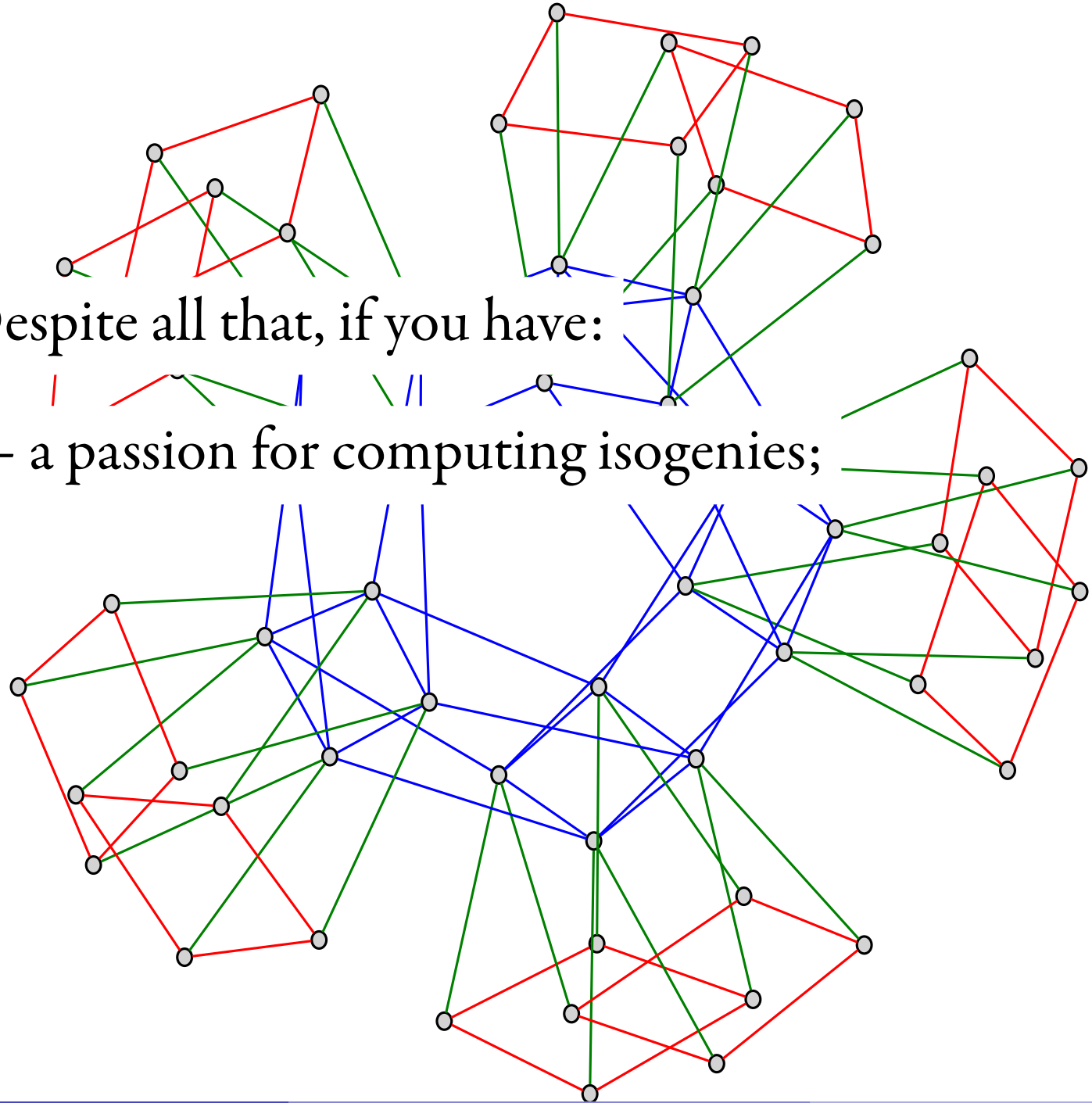


The way *we* code



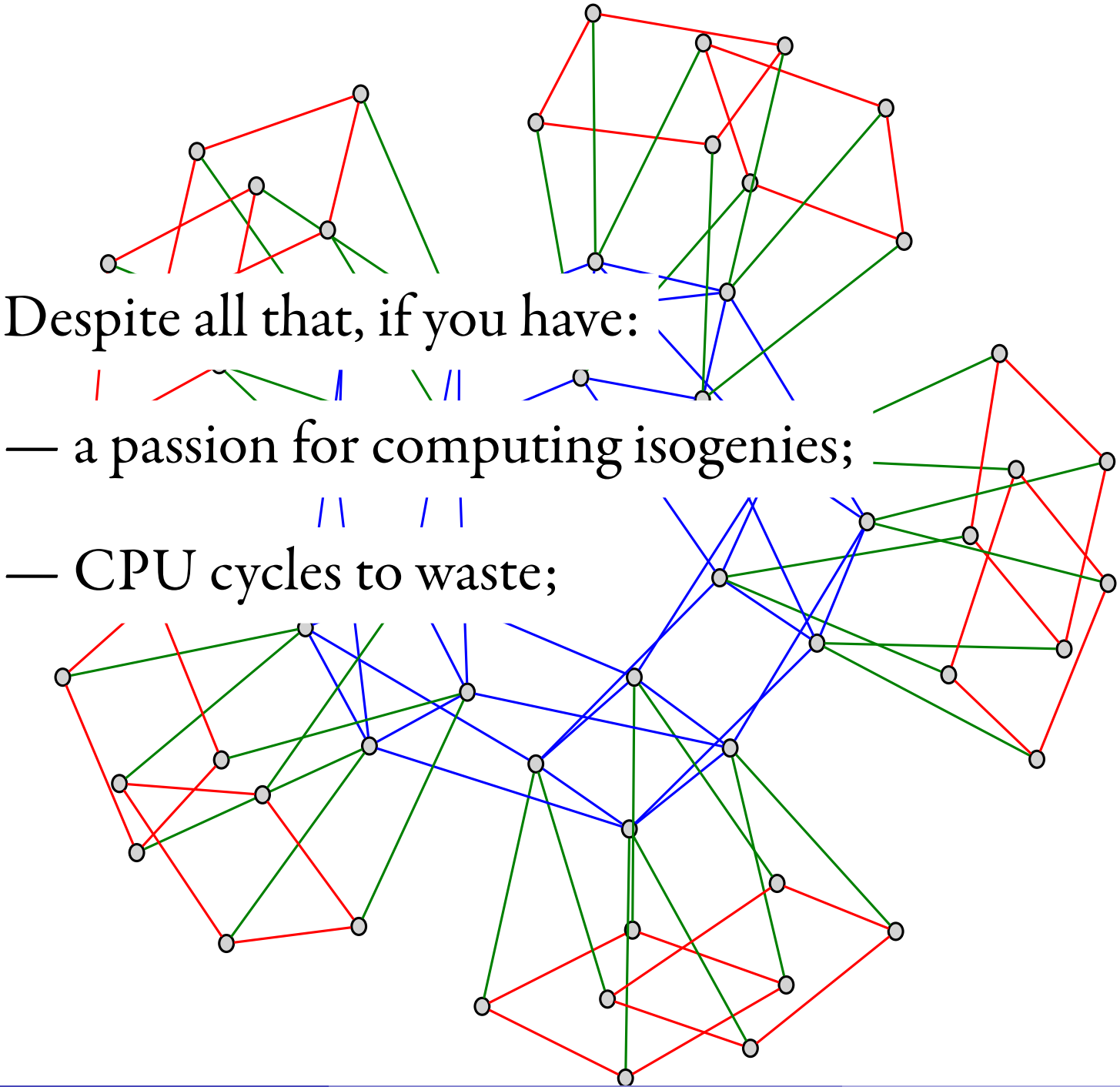
Despite all that, if you have:





Despite all that, if you have:

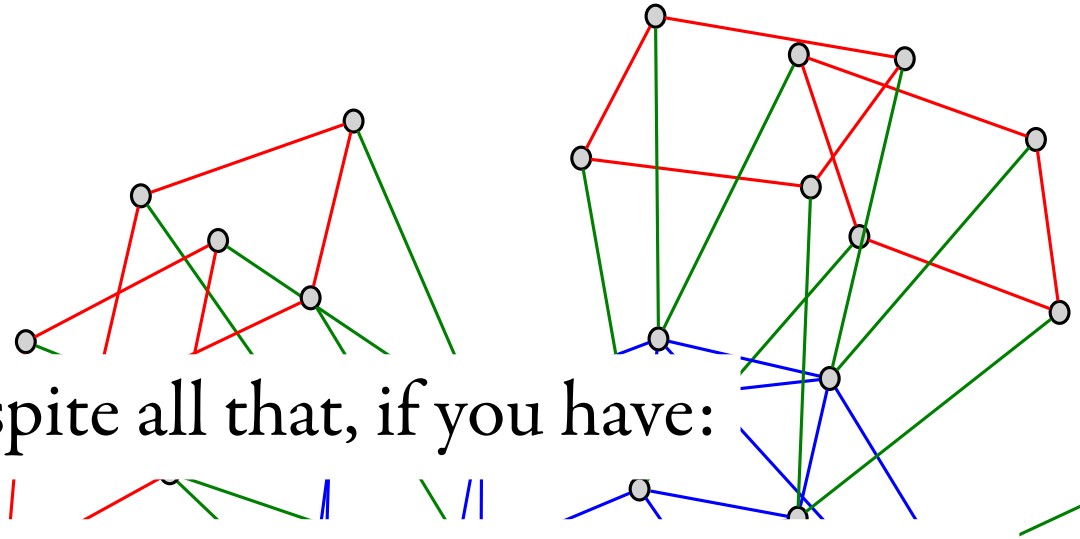
— a passion for computing isogenies;



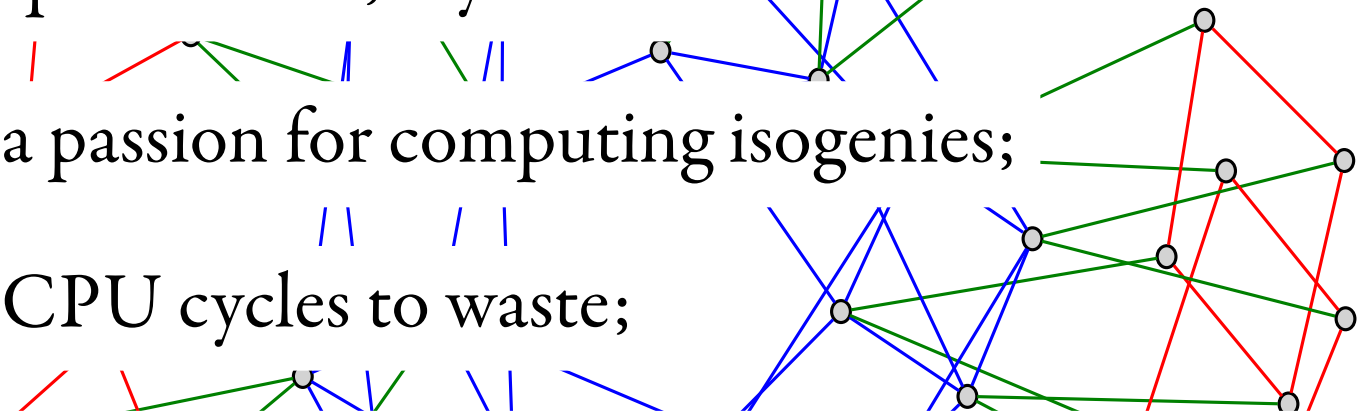
Despite all that, if you have:

— a passion for computing isogenies;

— CPU cycles to waste;



Despite all that, if you have:



— a passion for computing isogenies;

— CPU cycles to waste;

drop us an email and get an LGPL'ed library for free!