ElGamal Experiments Report

Lucas Perin

May 2020

1 Introduction

Brett's questions:

For a collection of primes p (in millions), define a handful of primitive elements g (preferably first five smallest and 10 additional spanning over the entire range). For each g and with $2 \le z \le 15$, plot $\Delta_l = \lambda(z) -$ lower-bound and Δ_u upper-bound $-\lambda(z)$.Repeat experiment with the following restrictions:

1. plot only when q is even;
2. plot only when q is odd;
3. plot only when g is even;
4. plot only when g is odd.

In Theorem 8, we have that the occurrence of some arbitrary t-tuple in the ElGamal sequence is bounded as

$$\left\lfloor \frac{g}{v} \right\rfloor^{t-1} \left\lfloor \frac{q}{v} \right\rfloor \le \lambda(z) \le \left\lceil \frac{g}{v} \right\rceil^{t-1} \left(\left\lfloor \frac{q}{v} \right\rfloor + 1 \right).$$

We plot these bounds with the following code:

```
def tuple_bound(p, v, g, t):
    """
    Bounds defined in Theorem 8 for t-tuples
    """
    q = floor(p/pow(g,t-1))
    lower = pow(floor(g/v),t-1)*floor(q/v)
    upper = pow(ceil(g/v),t-1)*(floor(q/v)+1)
    return lower, upper
```

1.1 Expected bound explosion!

We could probably stop plotting when (or let it happen a bit):

For the upper bound:

$$g > \sqrt[t-1]{p}$$

$$t > \log_g p$$

for the lower bound:

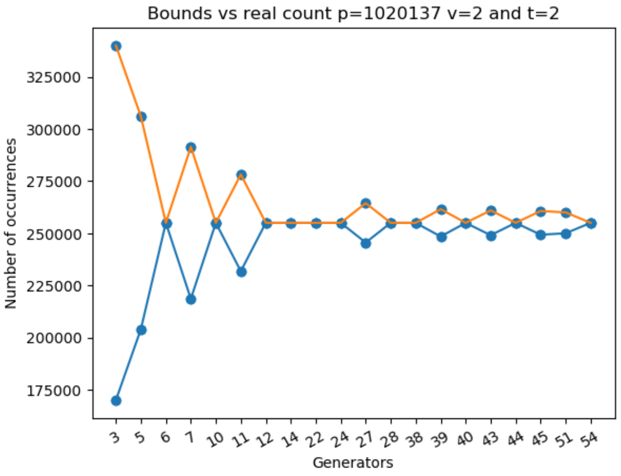
$$v > q$$

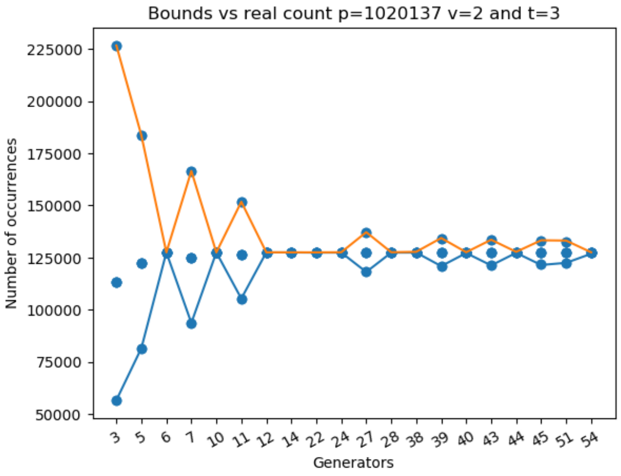
$$v > g$$

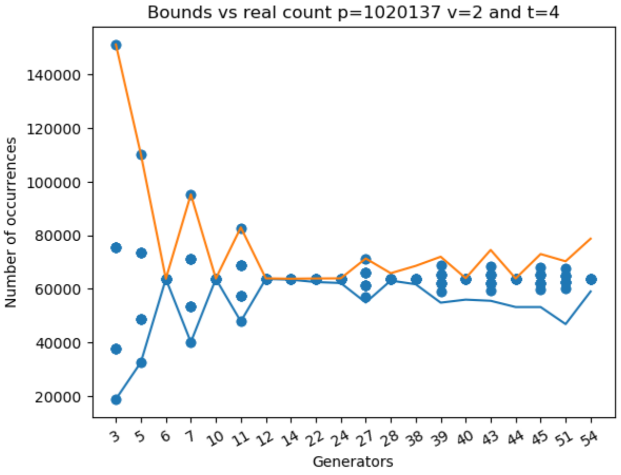
2 First Evaluating t-tuple bounds for $v = 2$

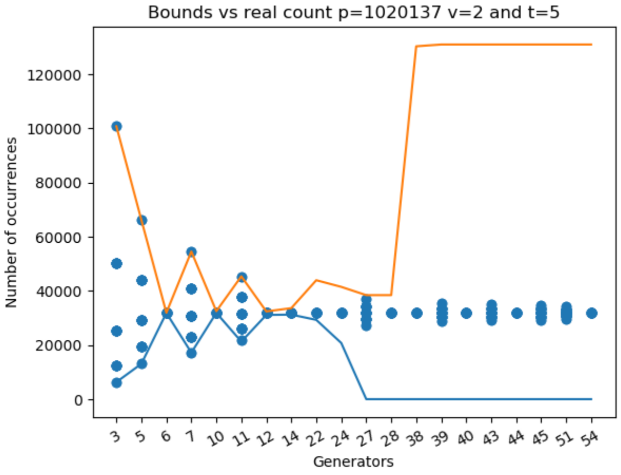
In this section, we first investigated real counts and expected count with the bounds, by drawing a line over the plot. The line is truncated when the upper bound exceeds 1.3 times the largest actual count of the entire plot. This is clear in the figures when t grows. The experiments that follow do not use Δ_l or Δ_u.

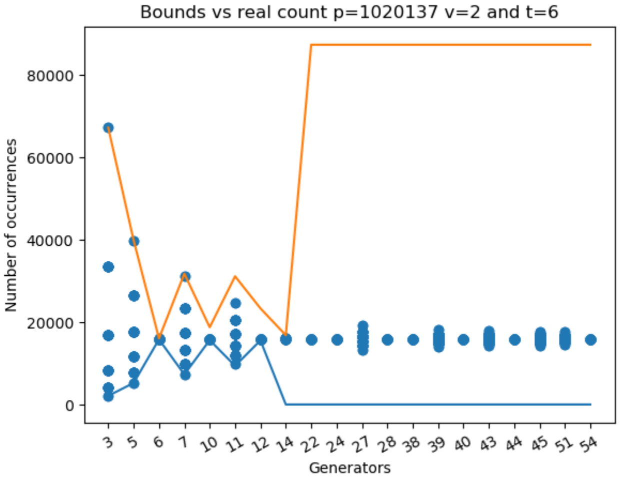
2.1 Plotting all for each prime individually

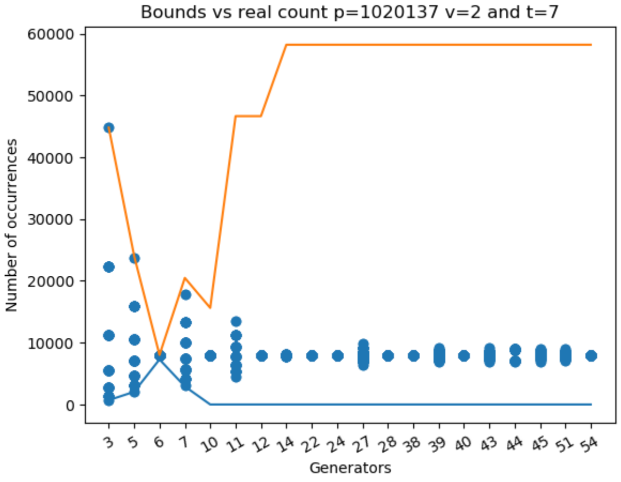




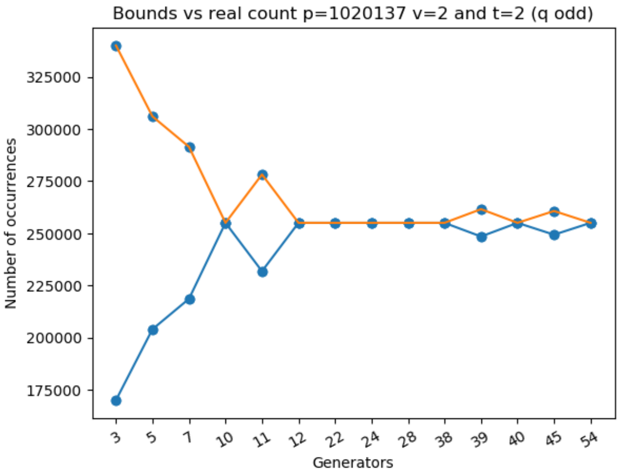


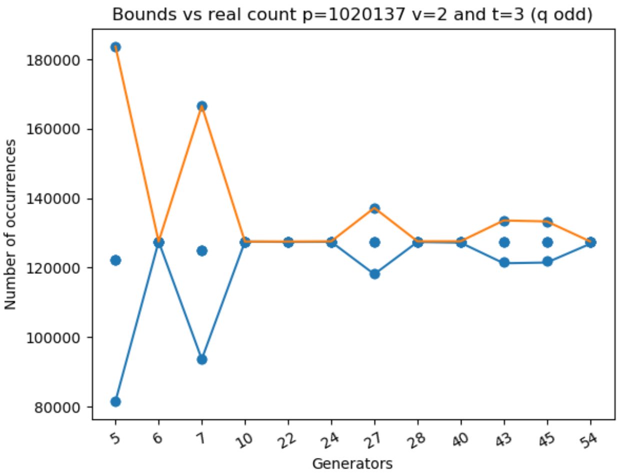


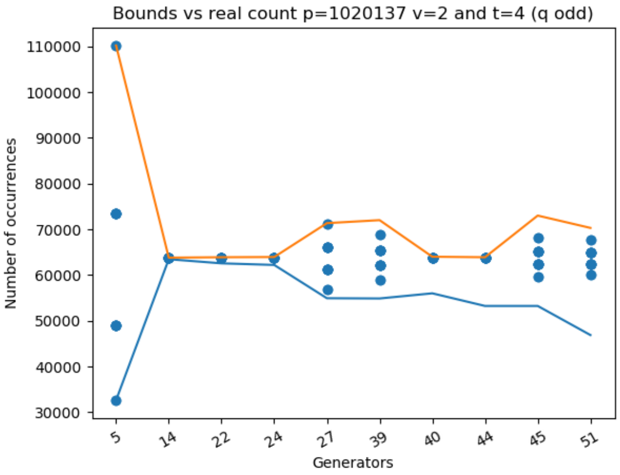


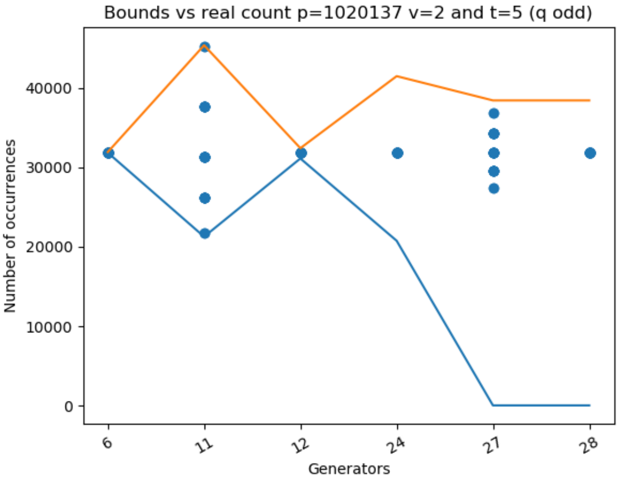


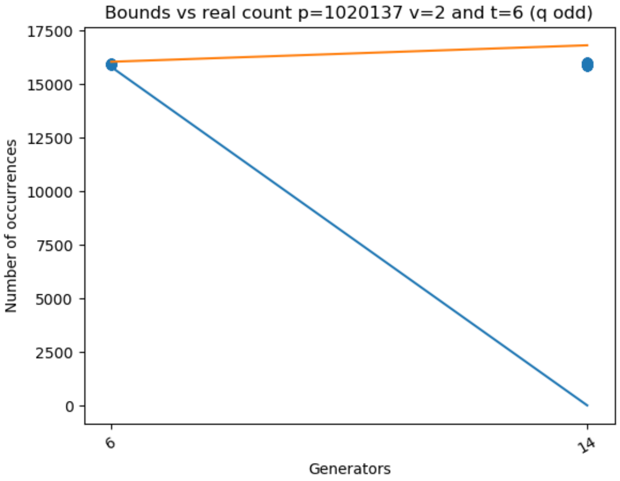
2.2 Plotting when q is odd for each prime individually

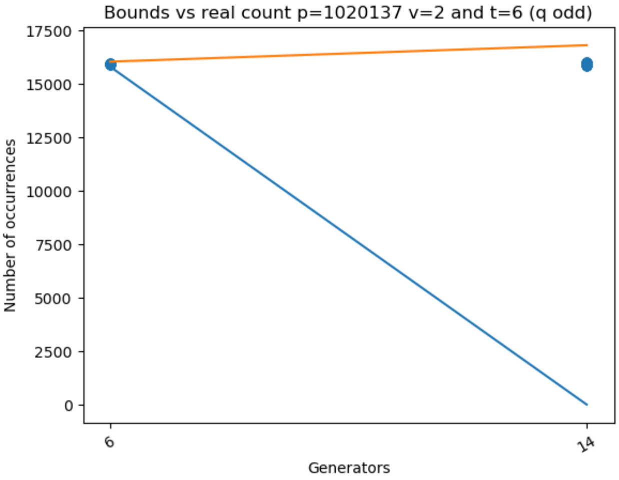




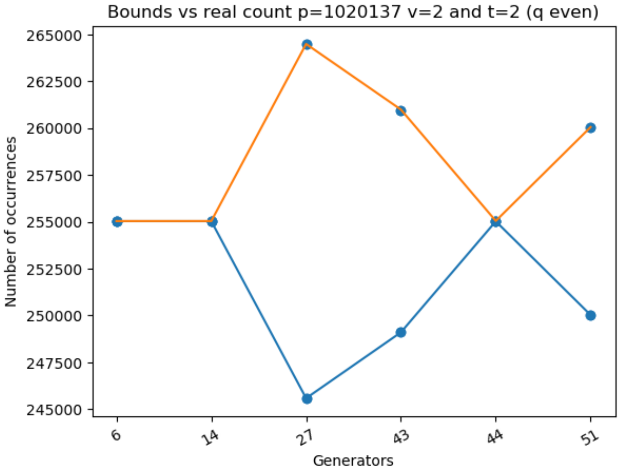


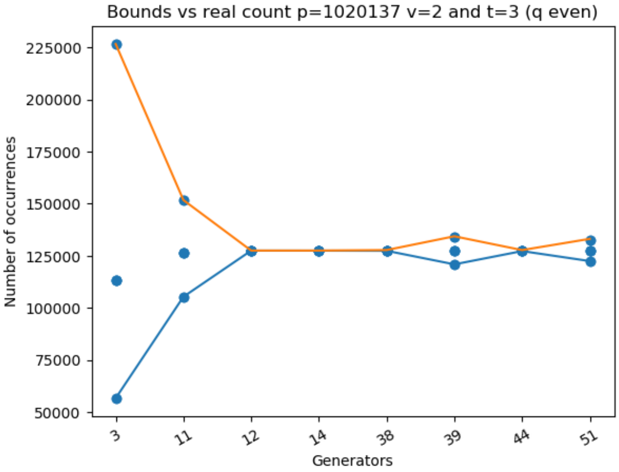


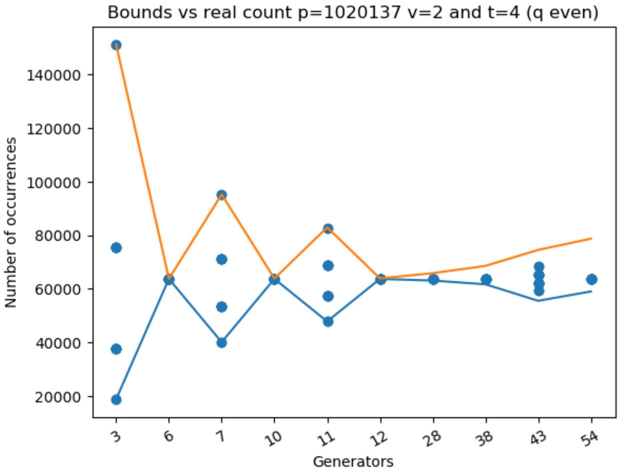


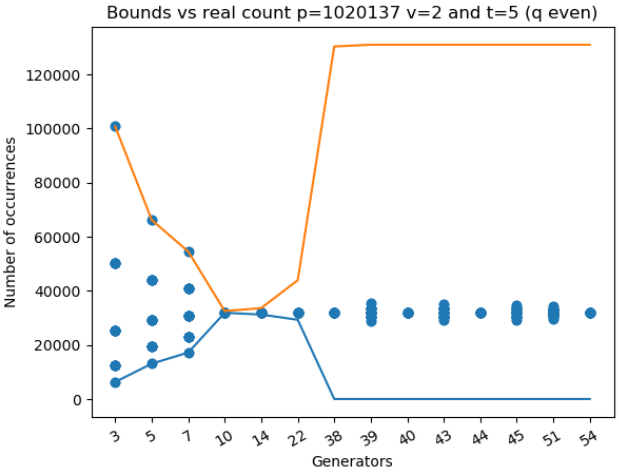


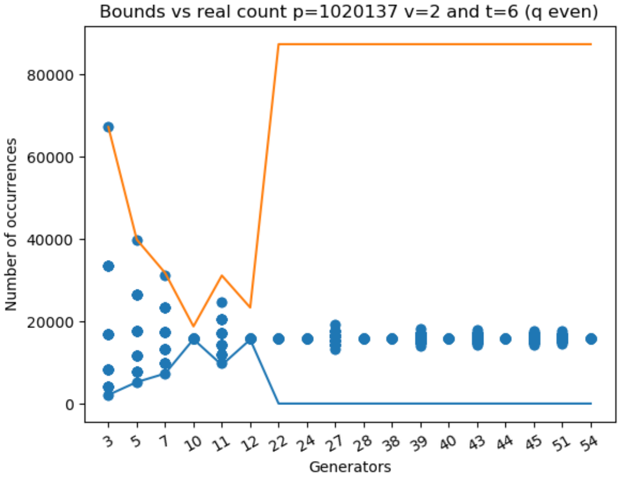
2.3 Plotting when q is even for each prime individually

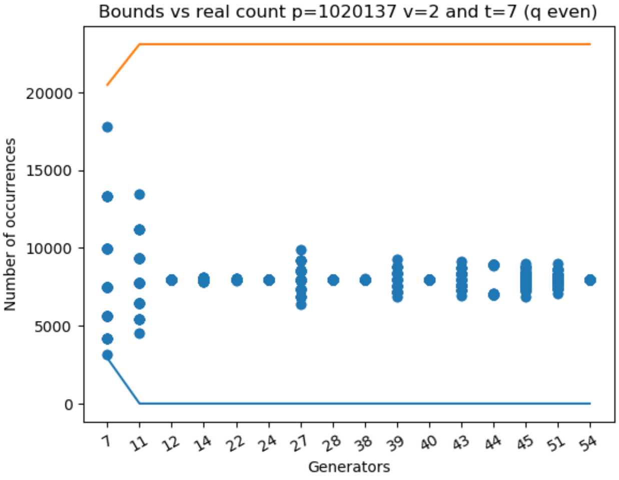




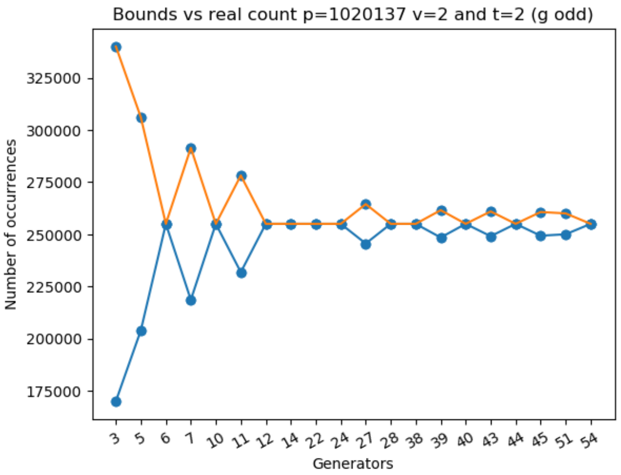


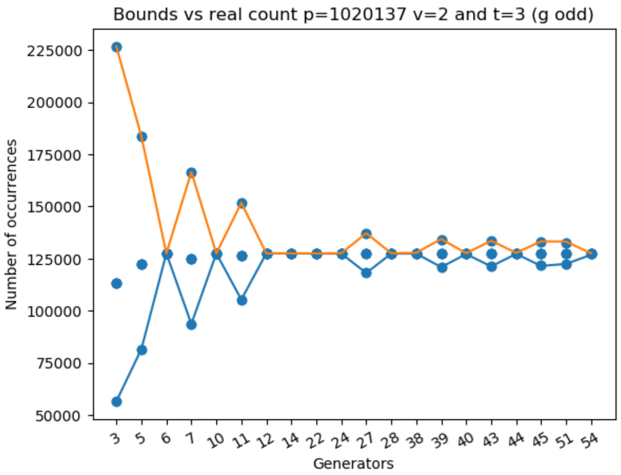


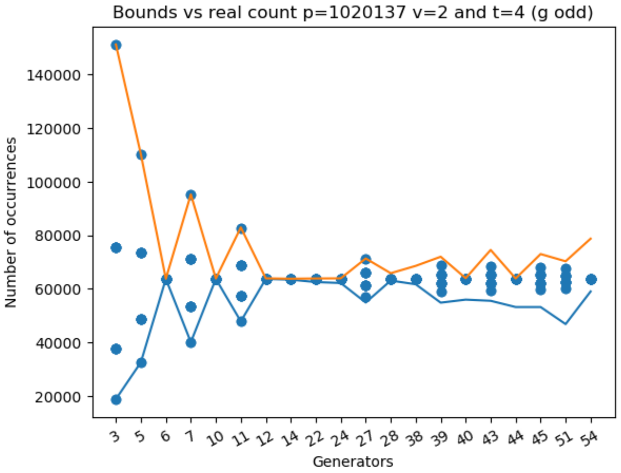


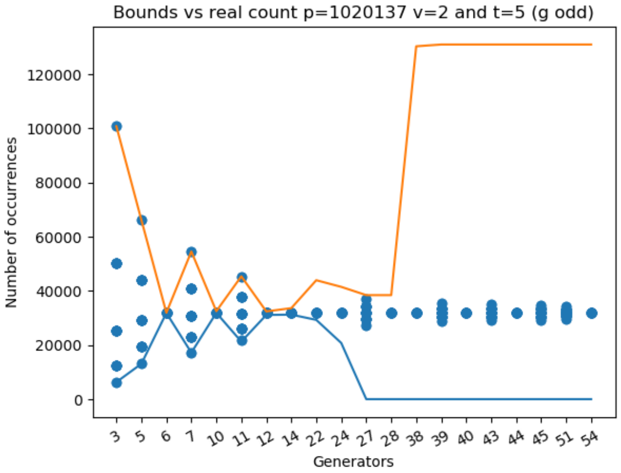


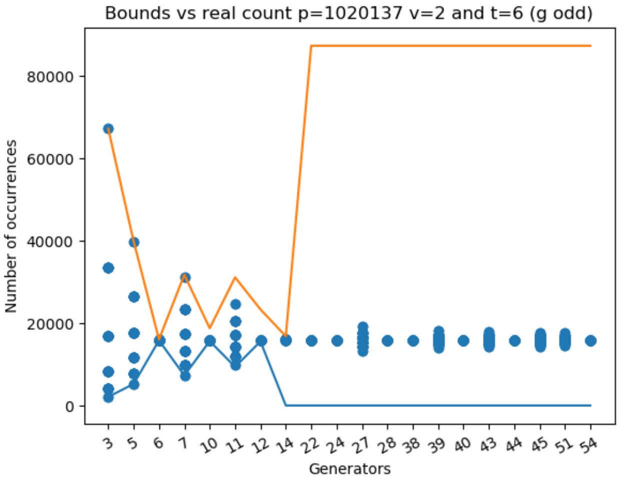
2.4 Plotting when g is odd for each prime individually

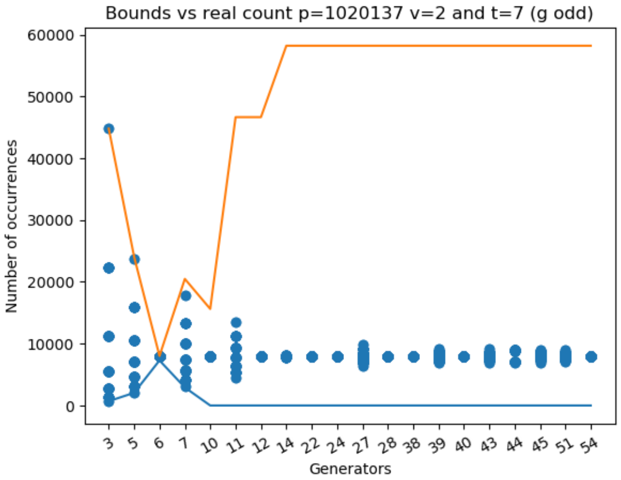




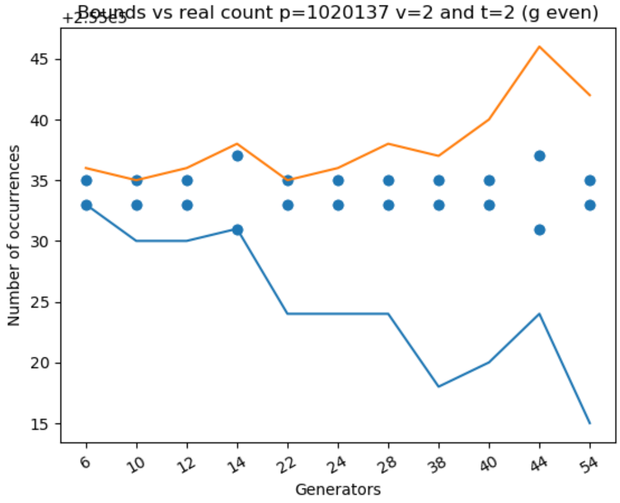


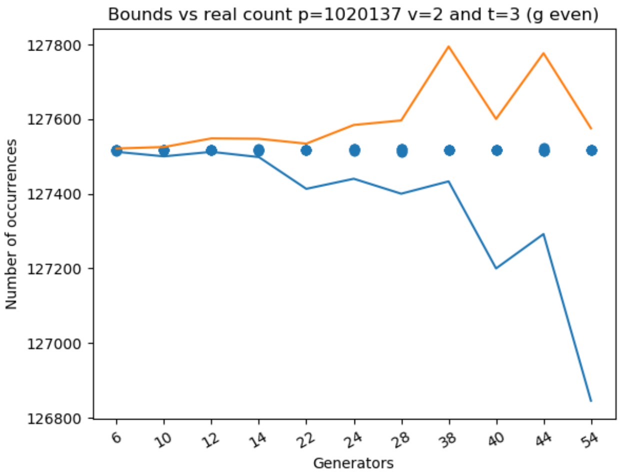


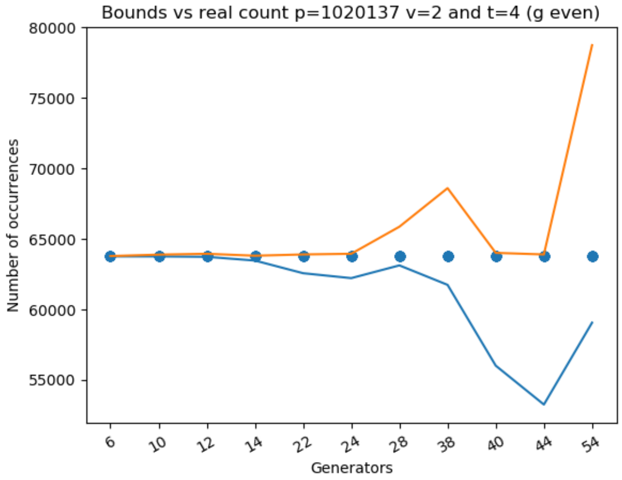


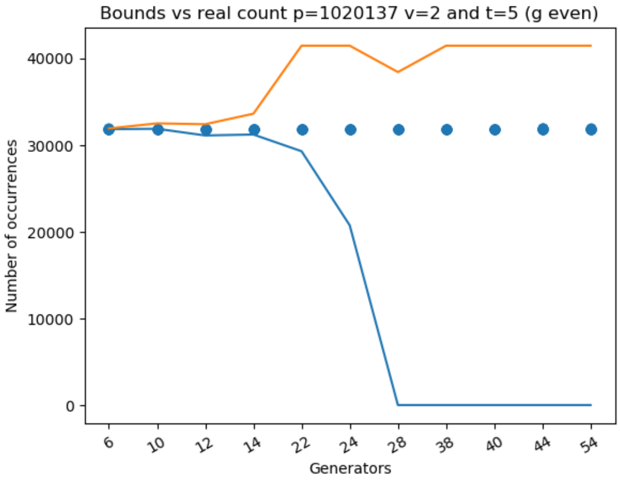


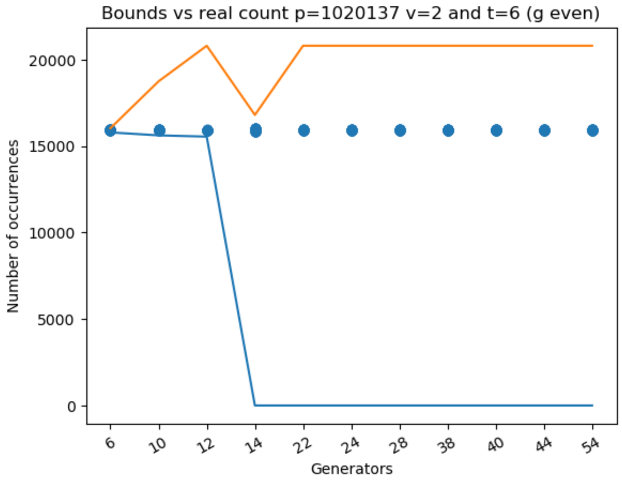
2.5 Plotting when g is even for each prime individually

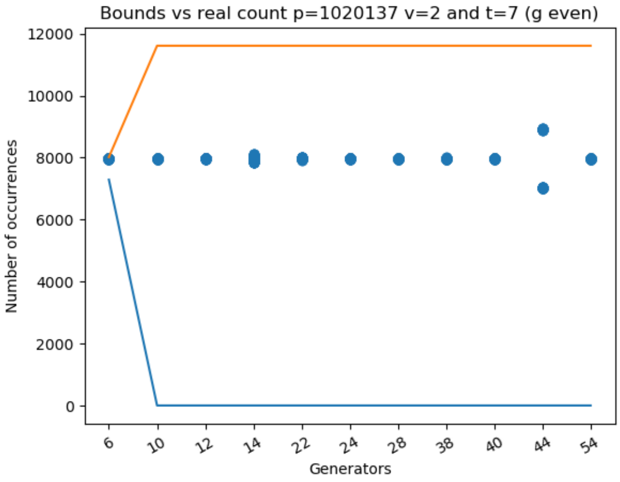






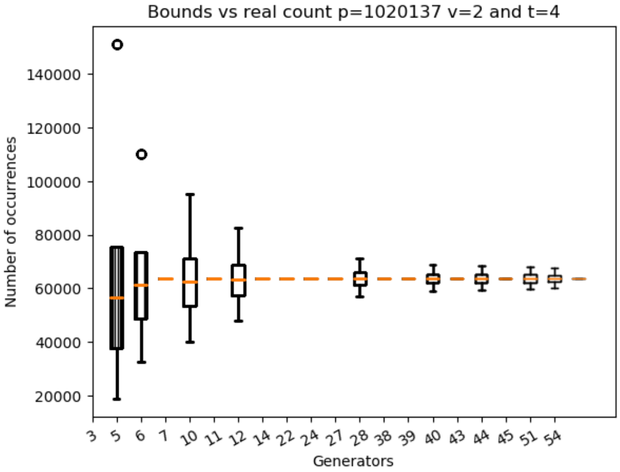


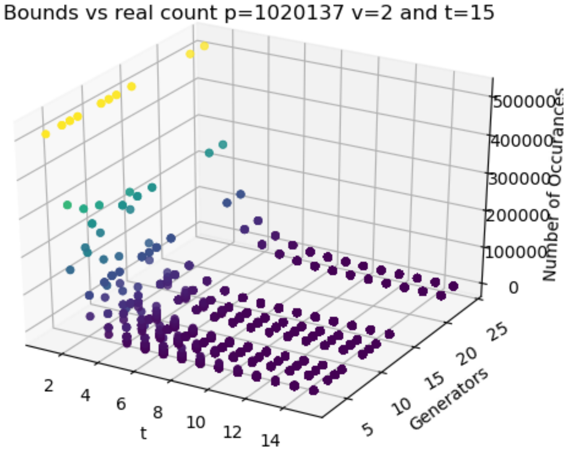




2.6 Box and 3d plots

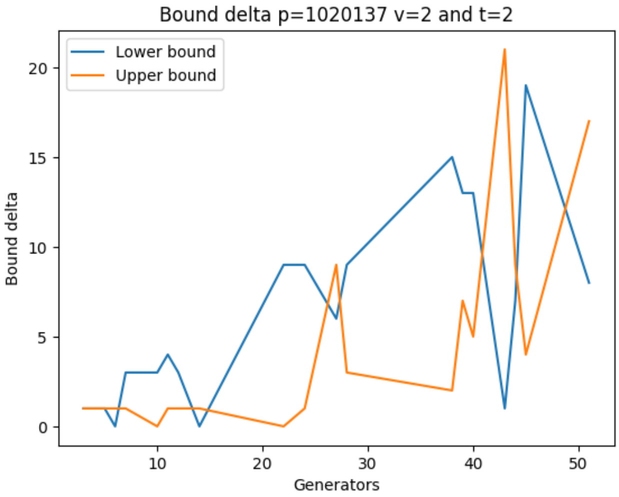
We may try to compose a set of experiments for the same prime all in one plot as shown below, using 3d plots. The tricky part is that the plotted data will have to be the delta mentioned in the first page — namely, the distance of the bounds to original count. The main issue with this is that for each pair $(x, y) = (t, \lambda)$ we will have to plot two dots, one for the lower bound and one for the upper bound. Essentially, one dot may end up on top of each other or too far away, making it hard to read. I will investigate further.

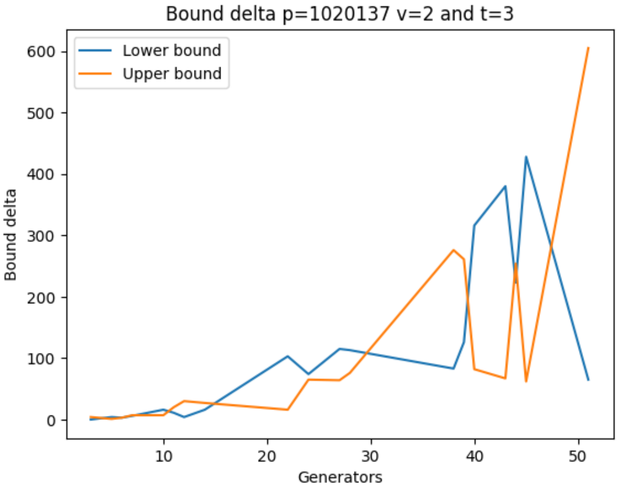


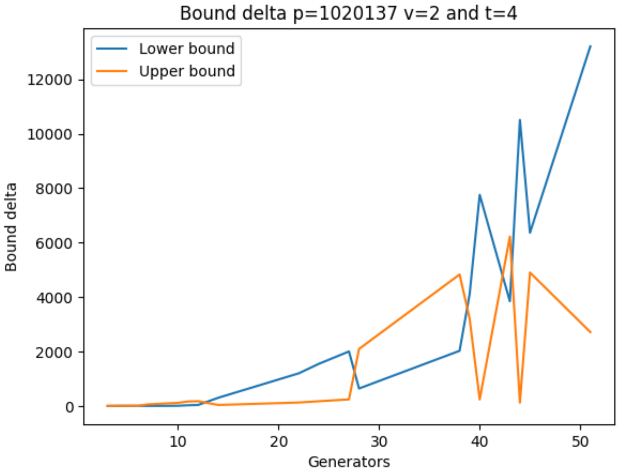


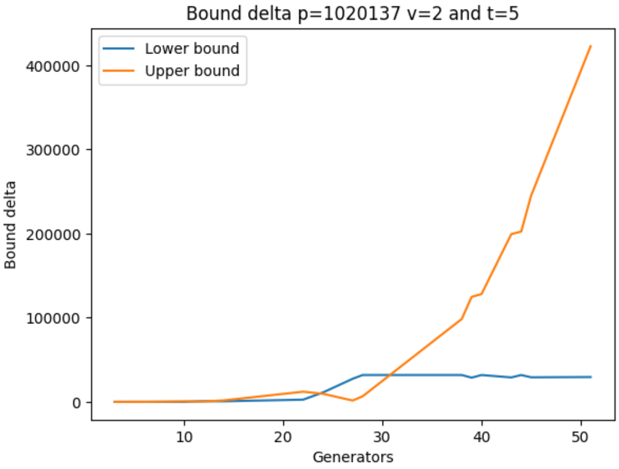
3 Delta plots

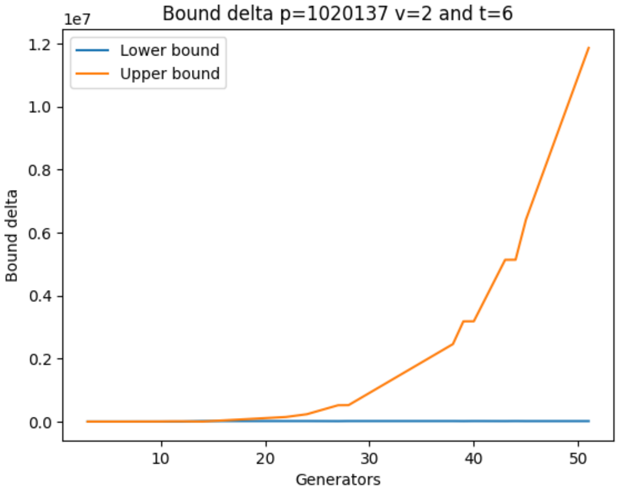
In the following, we show how the bounds have a tendency to “explode” for some specific set of parameters.

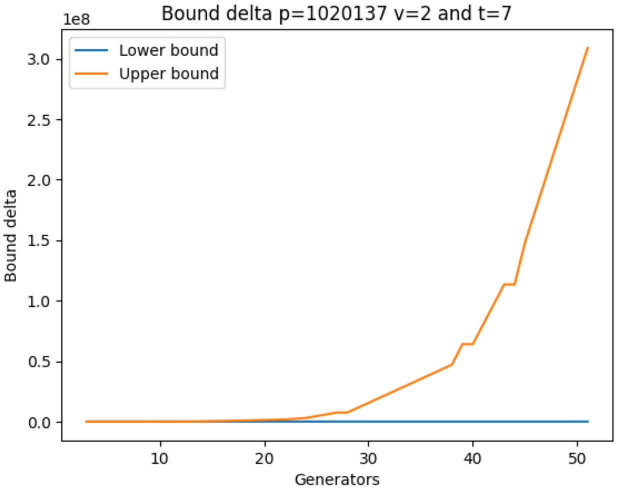






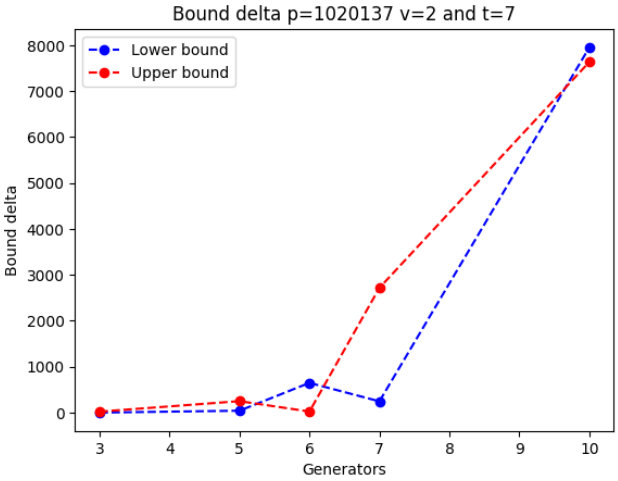


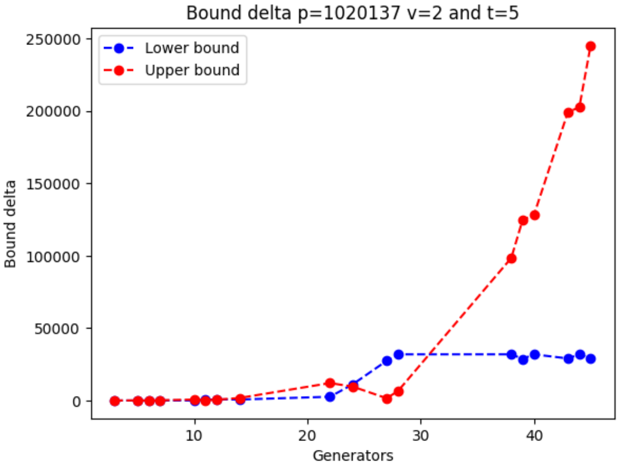




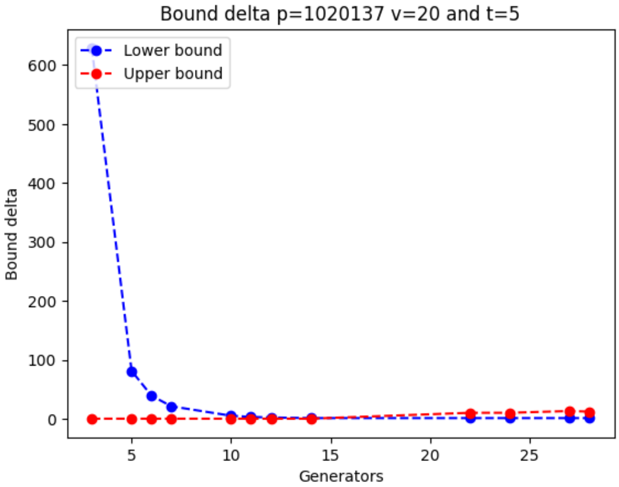
3.1 Tight delta plots

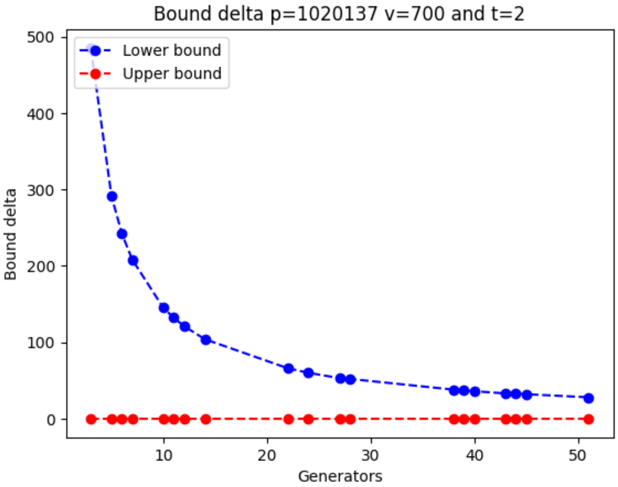
Now, we present plots for parameter sets where the bounds are tight, that is, close to the actual count. We do this by considering only parameters such that, for small v, $g < \lfloor \sqrt[t-1]{p} \rfloor$ and $t < \lfloor log_g p \rfloor$. For example, let $(t, p, v) = (7, 1020137, 2)$, then we are we have that the bound explodes when $g \geq 10$. The same happens if we set $t = 5$ for $g >= 31$.


Bound delta p=1020137 v=2 and t=7

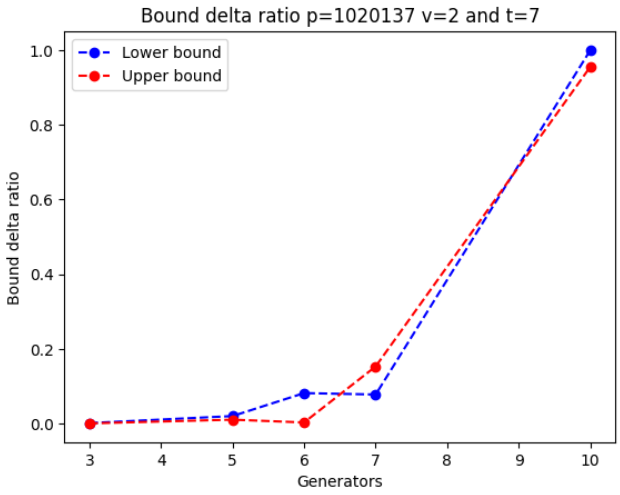

Bound delta p=1020137 v=2 and t=5

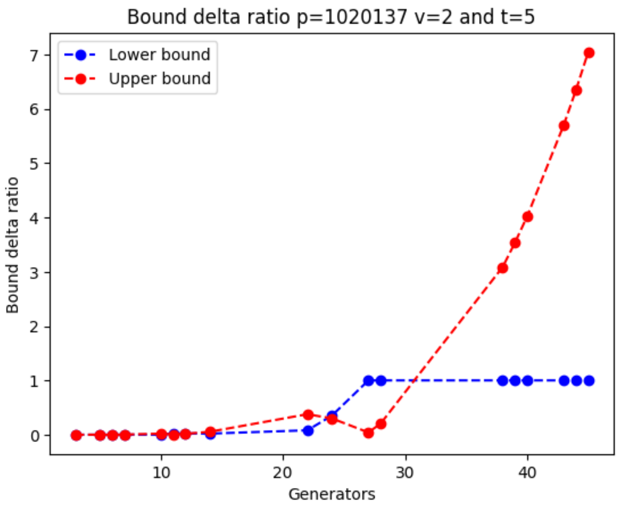
As it shows in the examples, these parameter constraints do not correlate to the explosion of the lower bound necessarily. Clearly, since the lower bound cannot be less than zero, eventually it will be stable. However, we do expect it *NOT* to be tight when $v > q$ or $v > g$. While the first requires v to be large when p grows, the second is may occur eventually (even as p grows) for small value v. Observe the following display of this behaviour.

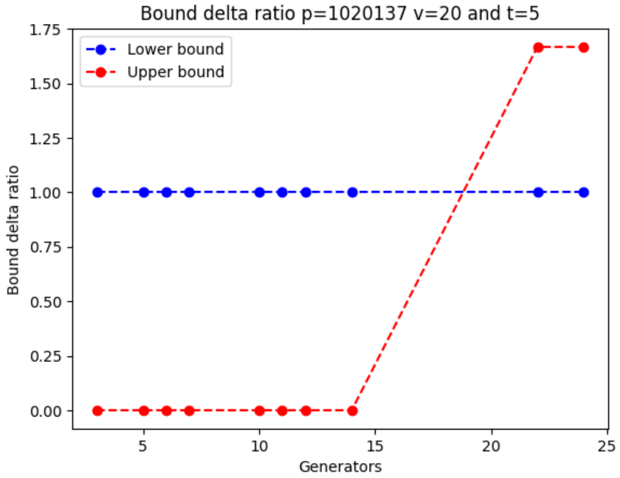

Bound delta p=1020137 v=20 and t=5

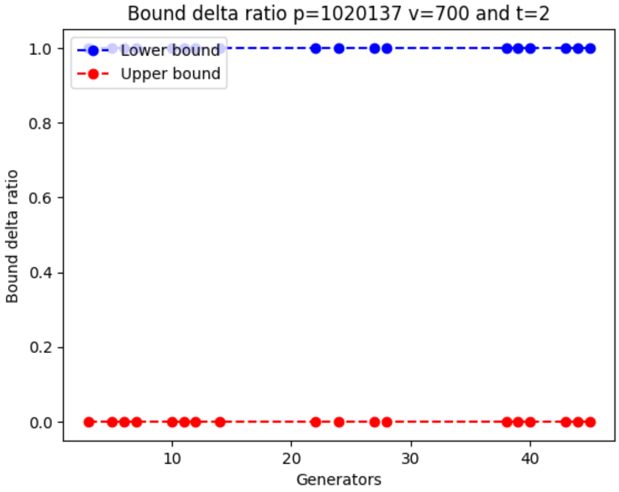

Bound delta p=1020137 v=700 and t=2

We also remark that the numbering on the y axis makes it difficult to actually understand how tight the bound is. One would always consider the Δ close to zero to be tight, and zero to be exact. But when $\lambda(z)$ varies in range of hundreds of thousands, looking at Δ in range of thousands is not so bad. Let us look at the same examples but using a ratio value.









Brett and Daniel. These last two plots are weird. What happens here is that the lower bound is zero but the actual count is not. Let Δ_l denote the difference of actual count and the lower bound, namely $\min(\lambda(z)) - lb$, then I compute the ratio as follows:

$$\Delta_l^r = \frac{\min(\lambda(z)) - lb/}{\min(\lambda(z))} = 1 - \frac{lb}{\min(\lambda(z)}$$

and for the upper bound Δ_u

$$\Delta_u^r = \frac{ub - \max(\lambda(z))}{\max(\lambda(z))} = \frac{ub}{\max(\lambda(z))} - 1$$

This means that this ratio is bad when it comes to show the lower bound. Any tips?