Observations on Factoring Using the GNFS

How Do I Factor - GNFS

1. Polynomial Selection
2. Sieving
3. Combine

How Do I Factor - GNFS

1. Polynomial Selection
2. Sieving
3. Combine

1. f(x) & g(x) of degree d, e
2. irreducible over rationals
3. interpreted mod n have common root mod m

How Do I Factor - GNFS

1. Polynomial Selection
2. Sieving
3. Combine

1. f(x) & g(x) of degree d, e
2. irreducible over rationals
3. interpreted mod n have common root mod m

1. Millions of pairs a,b
2. Such that $b^d \cdot f(a/b)$ & $b^e \cdot g(a/b)$ factor 'prettily' (are smooth)
3. Via Lattice Sieving

How Do I Factor - GNFS

1. Polynomial Selection
2. Sieving
3. Combine

1. f(x) & g(x) of degree d, e
2. irreducible over rationals
3. interpreted mod n have common root mod m

1. Millions of pairs a,b
2. Such that $b^d \cdot f(a/b)$ & $b^e \cdot g(a/b)$ factor 'prettily' (are smooth)
3. Via Lattice Sieving

How Do I Factor - GNFS

1. Polynomial Selection
2. Sieving
3. Combine

1. f(x) & g(x) of degree d, e
2. irreducible over rationals
3. interpreted mod n have common root mod m

1. Millions of pairs a,b
2. Such that $b^d \cdot f(a/b)$ & $b^e \cdot g(a/b)$ factor 'prettily' (are smooth)
3. Via Lattice Sieving

1. Filter Relations & Build Matrix
2. Linear Algebra using Lanczos
3. "Square Root Phase"

How Do I Factor - GNFS

1. Polynomial Selection
2. Sieving
3. Combine

Slow & Unparallelizable

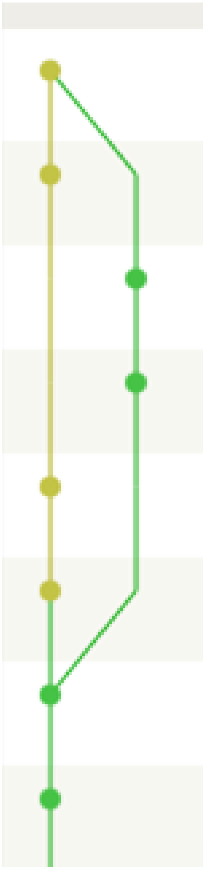
512 Bit ~8 Core-Days
768 Bit ~155 Core-Years*

1. f(x) & g(x) of degree d, e
2. irreducible over rationals
3. interpreted mod n have common root mod m

1. Millions of pairs a,b
2. Such that $b^d \cdot f(a/b)$ & $b^e \cdot g(a/b)$ factor 'prettily' (are smooth)
3. Via Lattice Sieving

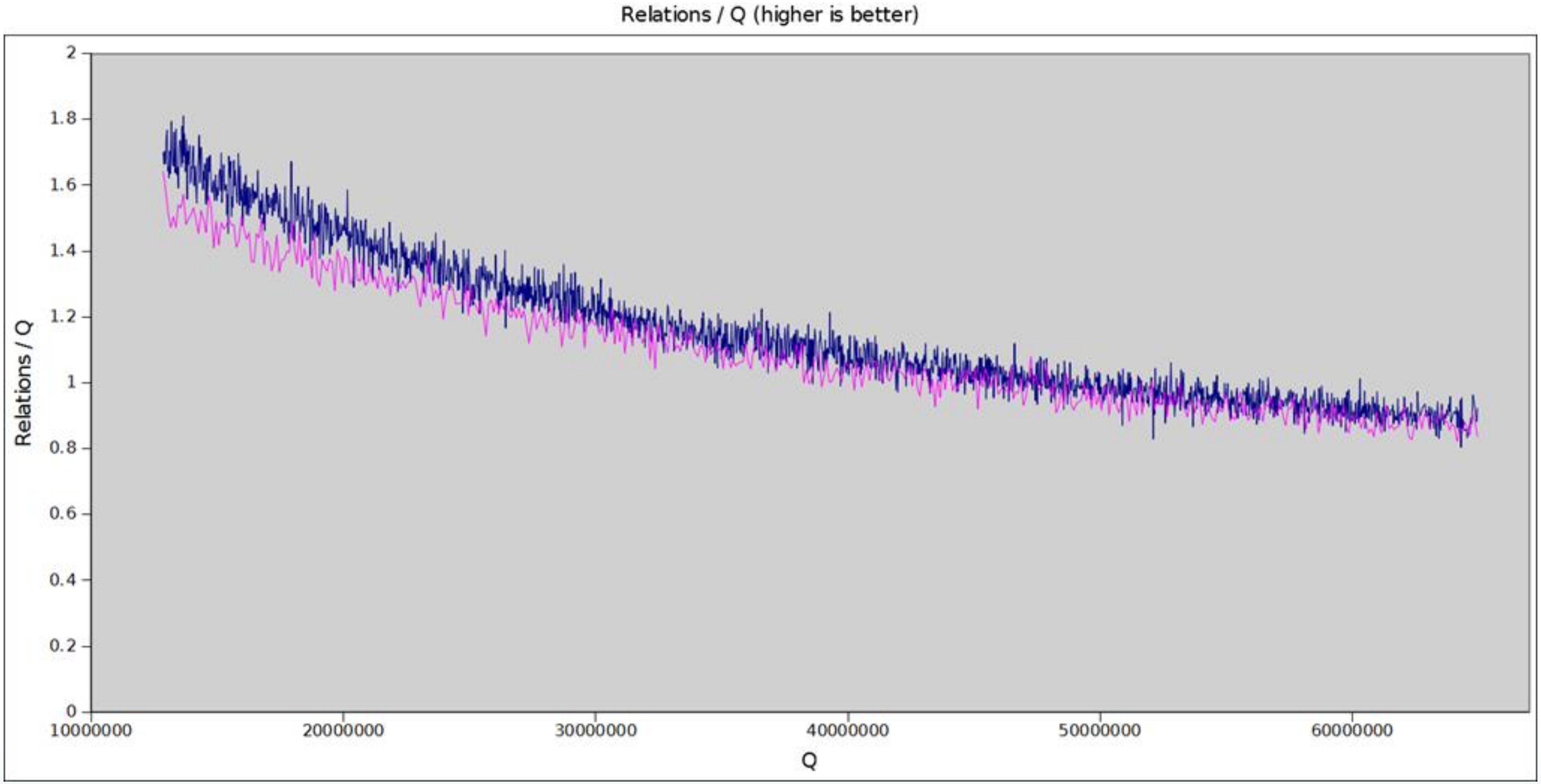
1. Filter Relations & Build Matrix
2. Linear Algebra using Lanczos
3. "Square Root Phase"

Some Details on Factoring

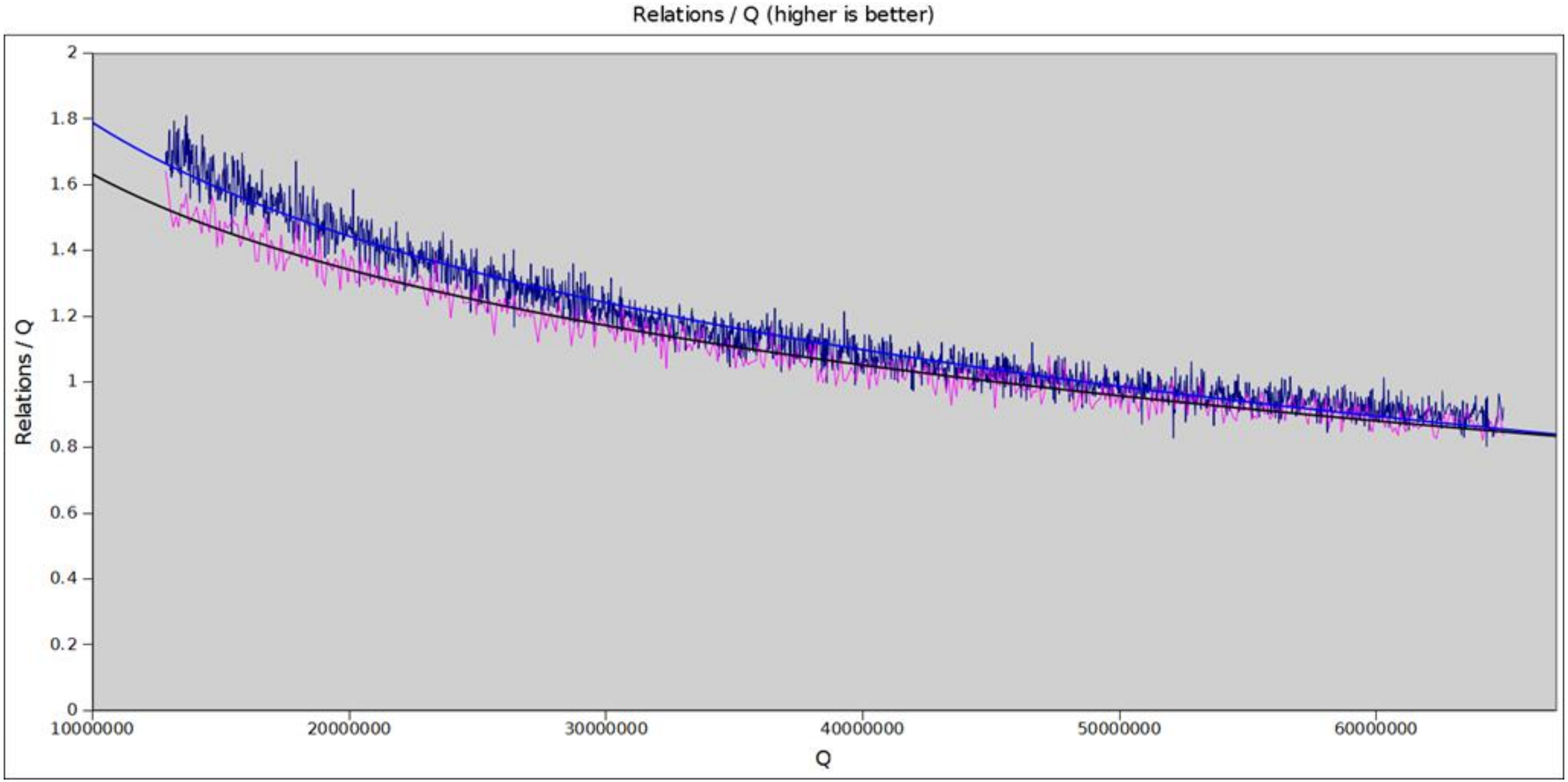


- Polynomial Selection
- Siever Comparisons
- Oversieving

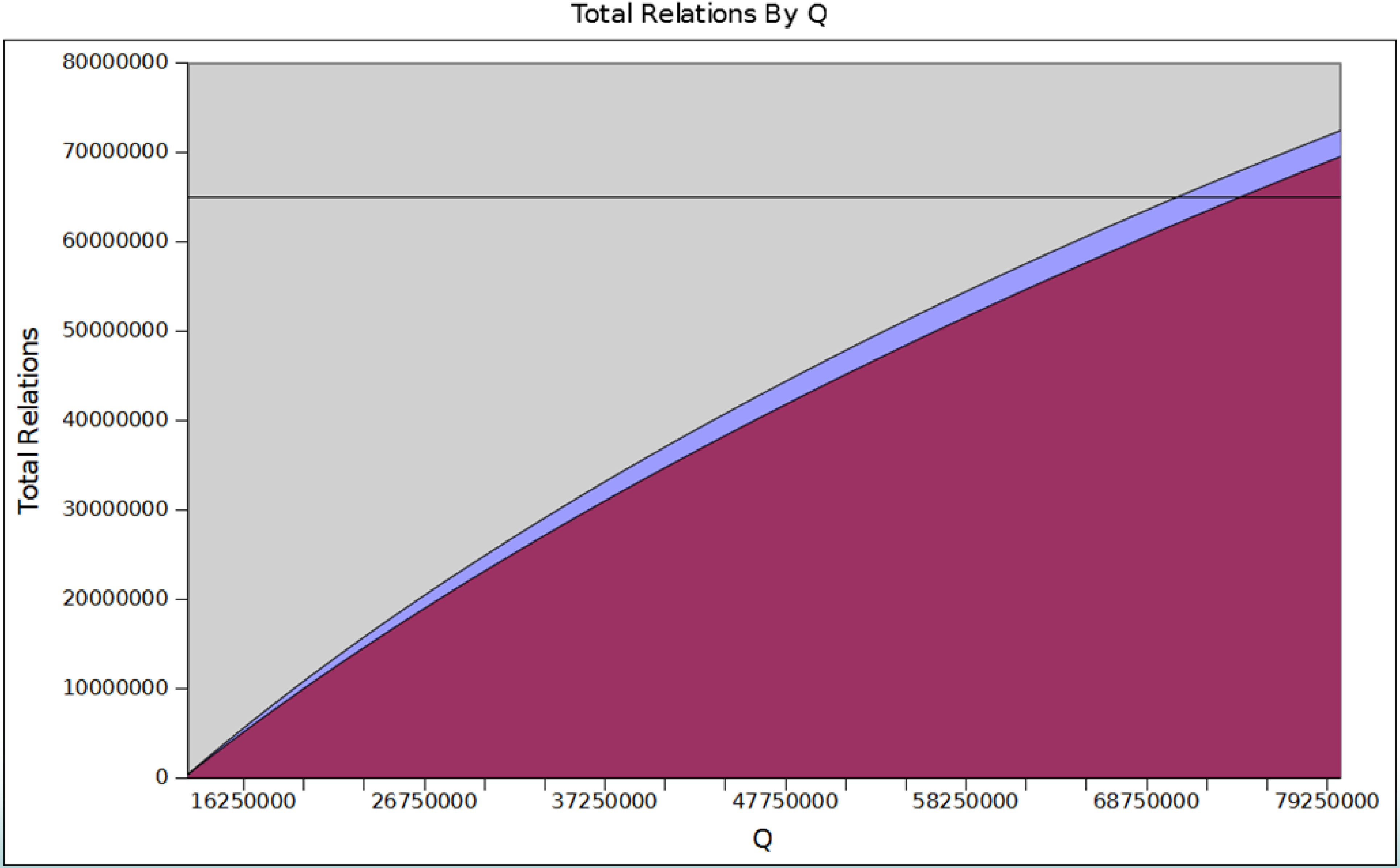
Misconceptions about Polynomials



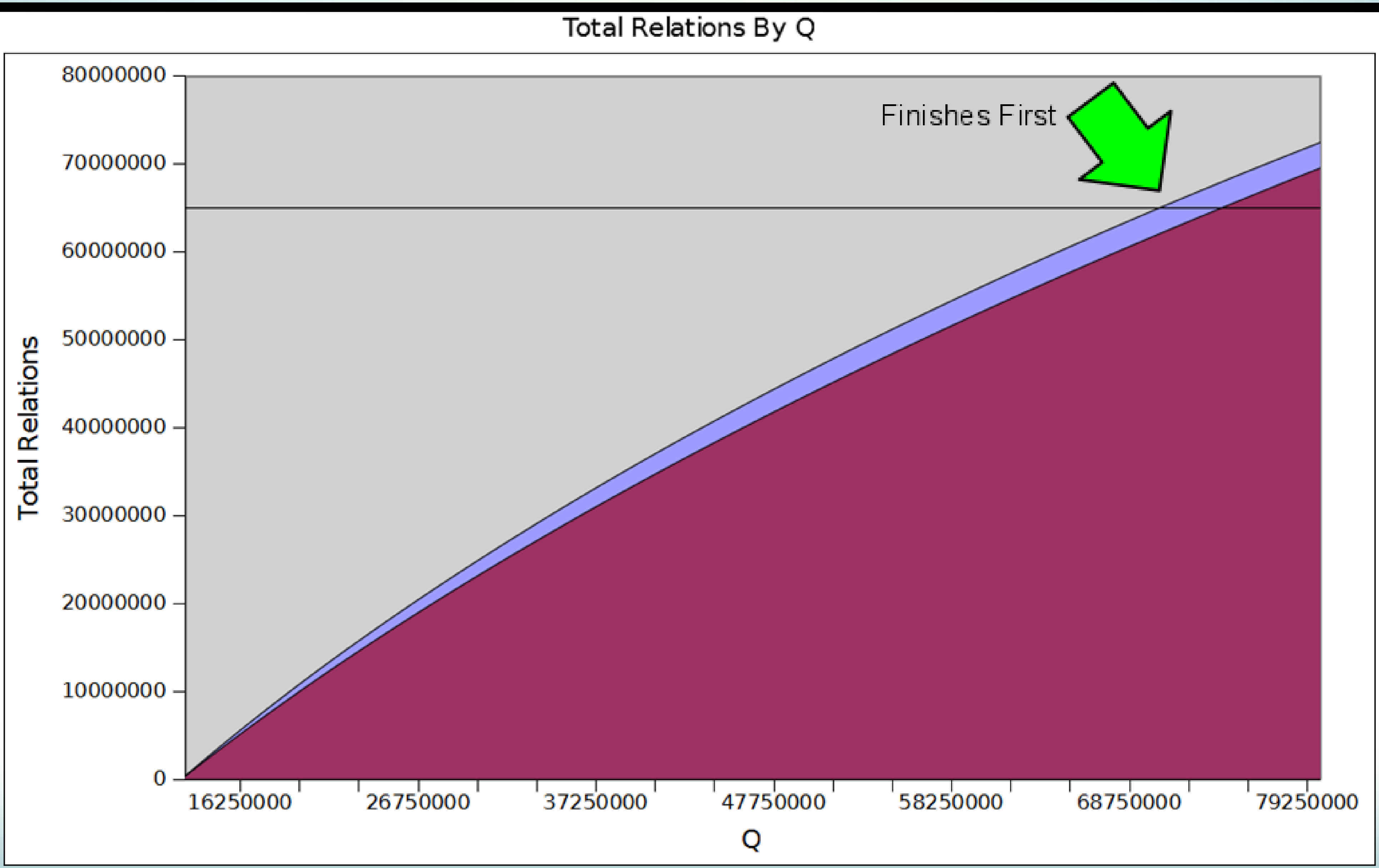
Misconceptions about Polynomials



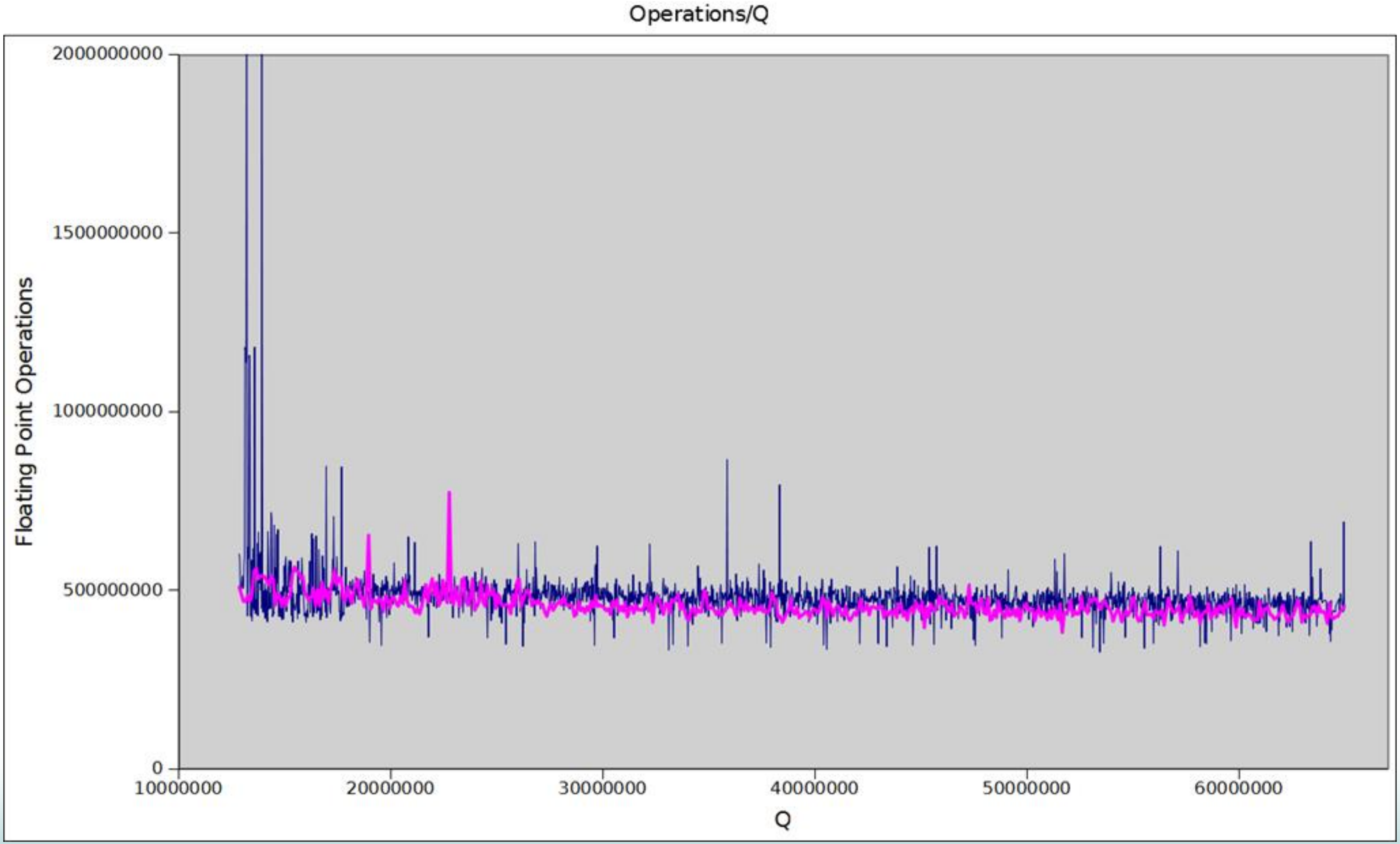
Misconceptions about Polynomials



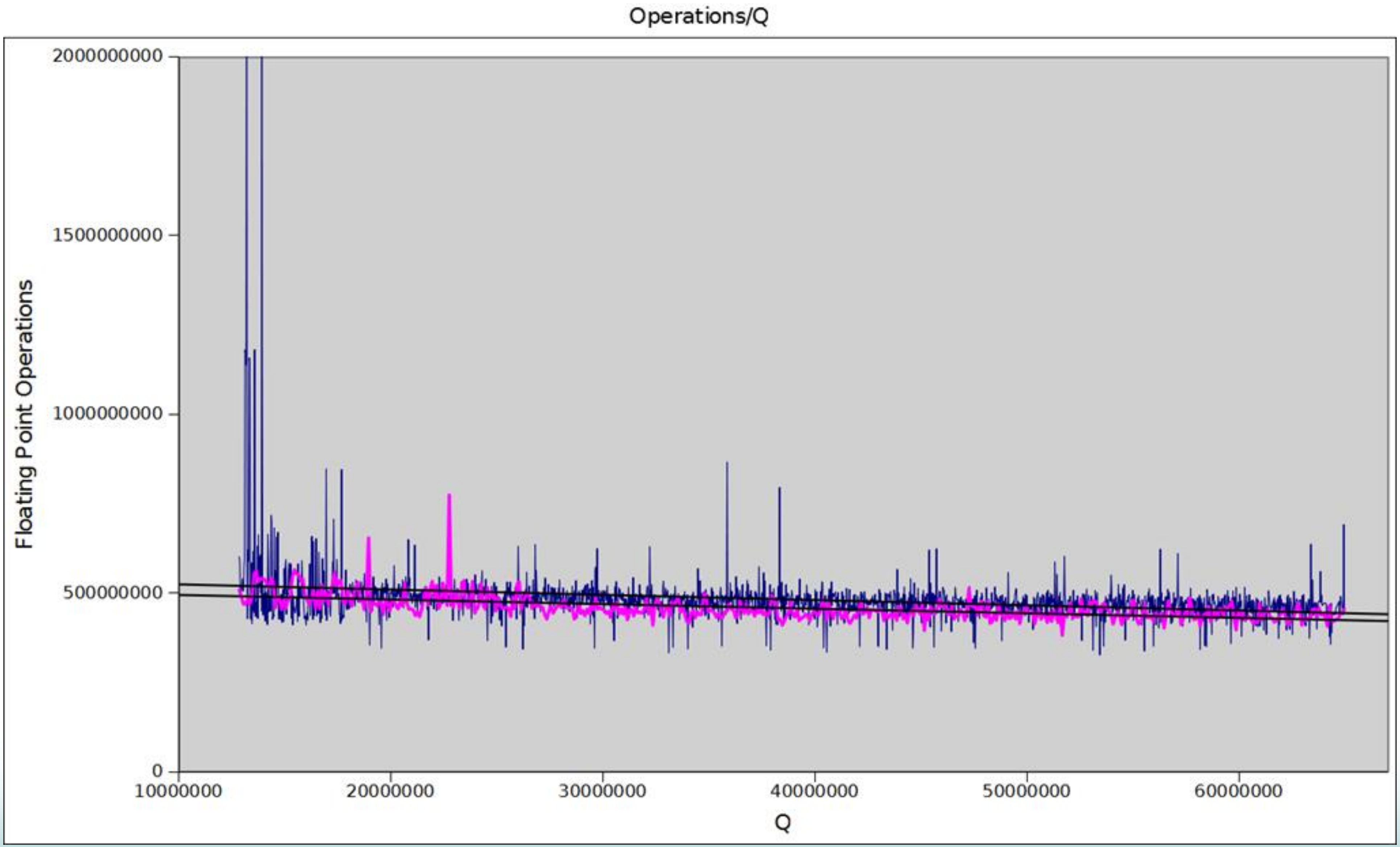
Misconceptions about Polynomials



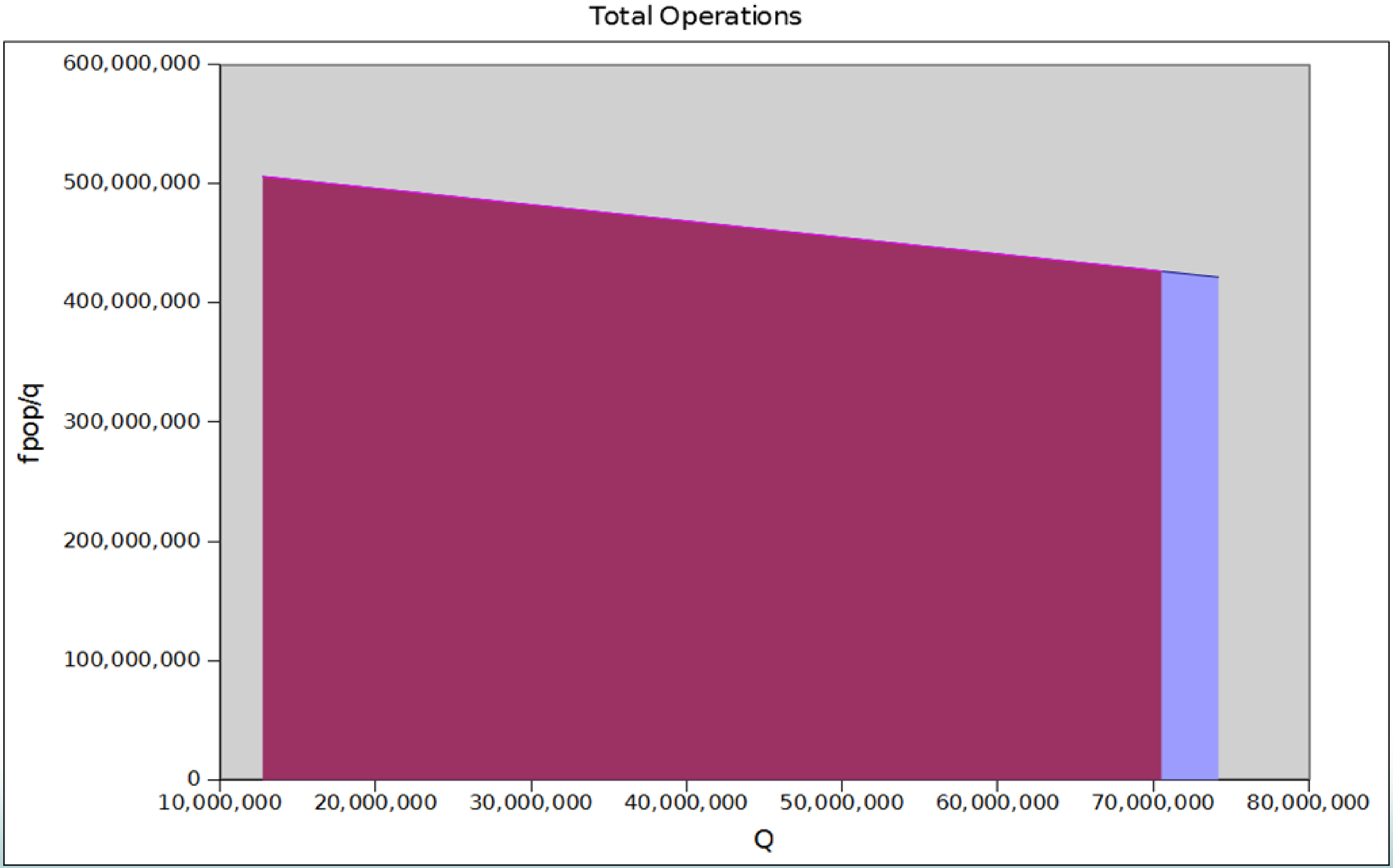
Misconceptions about Polynomials



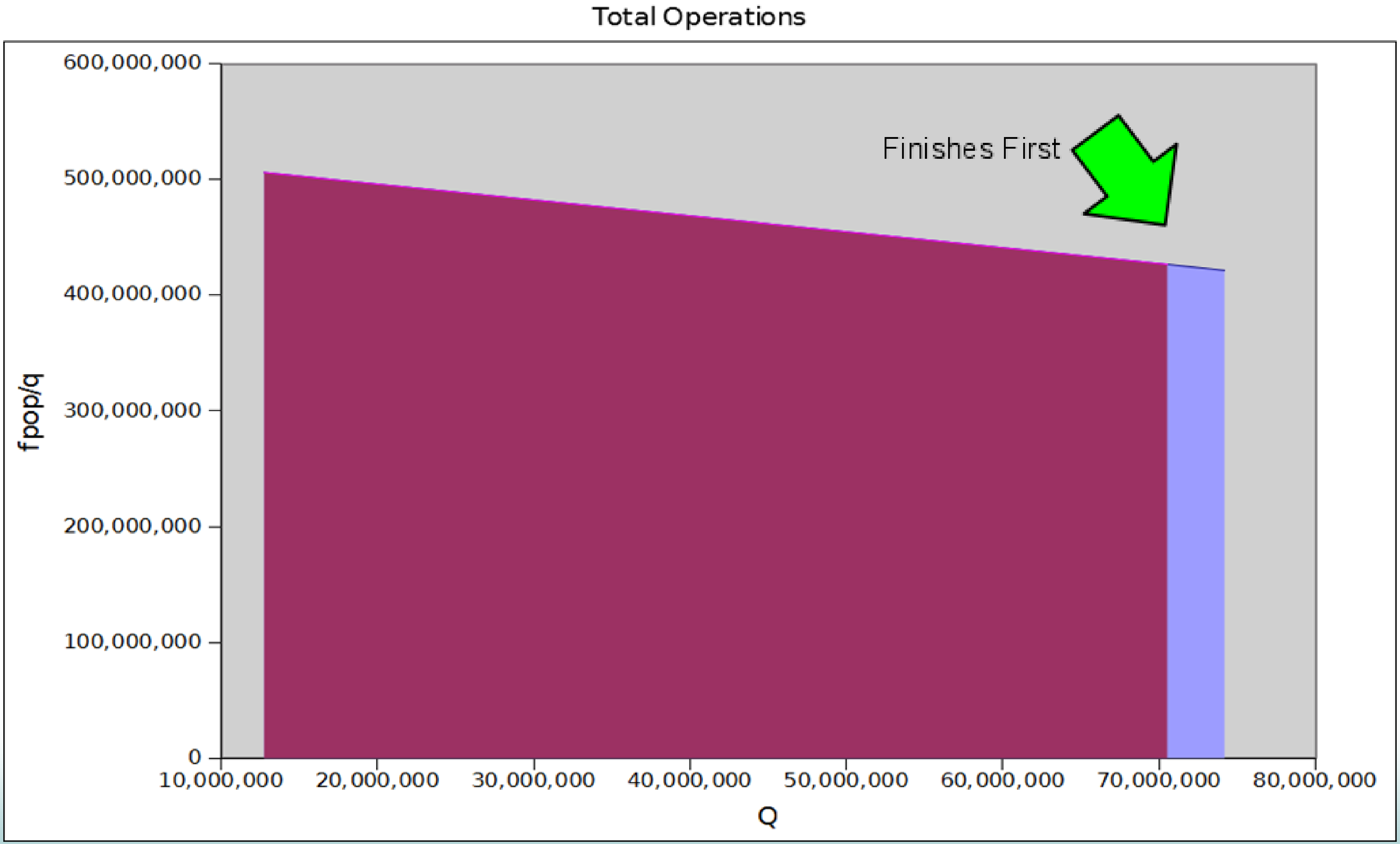
Misconceptions about Polynomials



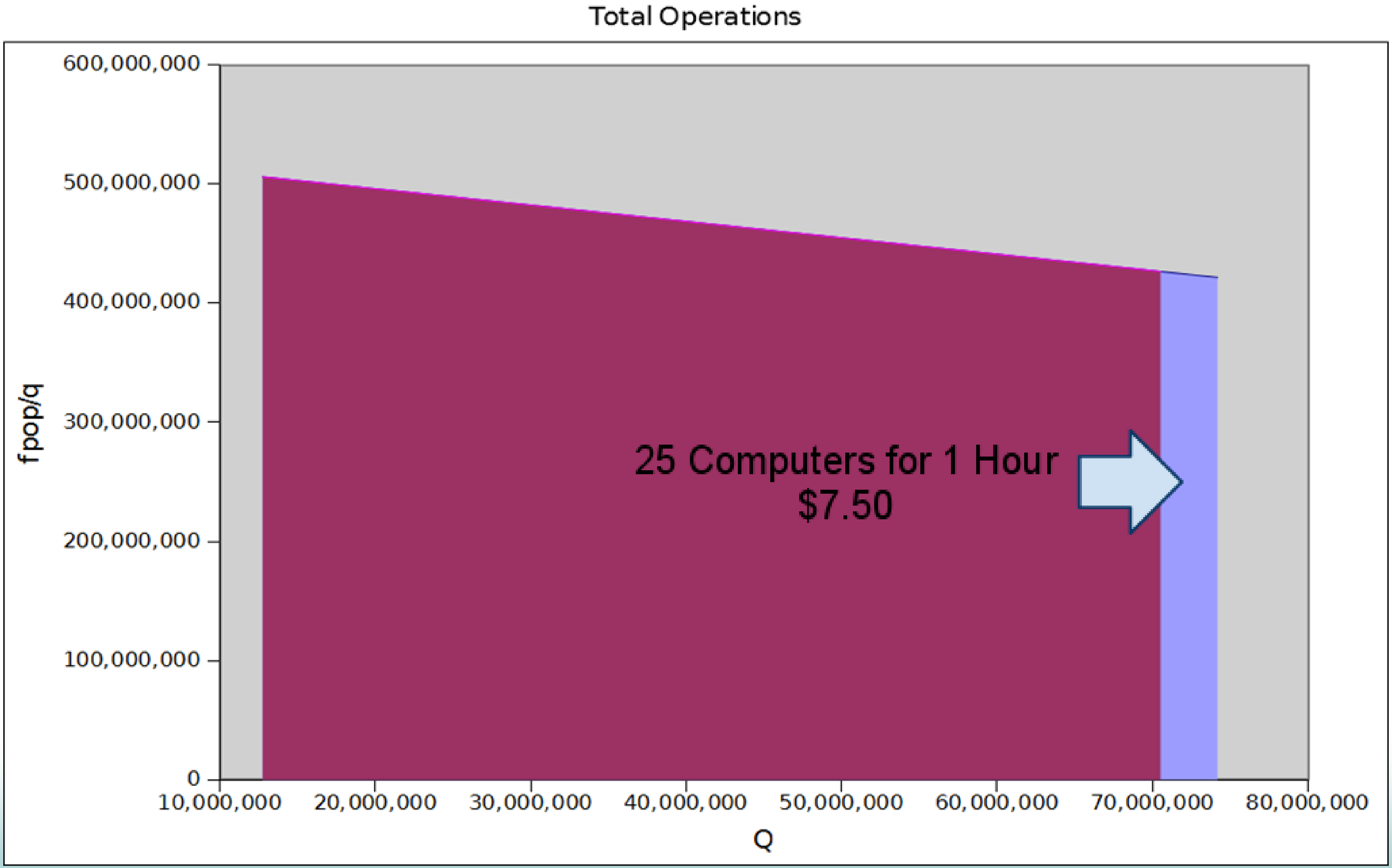
Misconceptions about Polynomials



Misconceptions about Polynomials



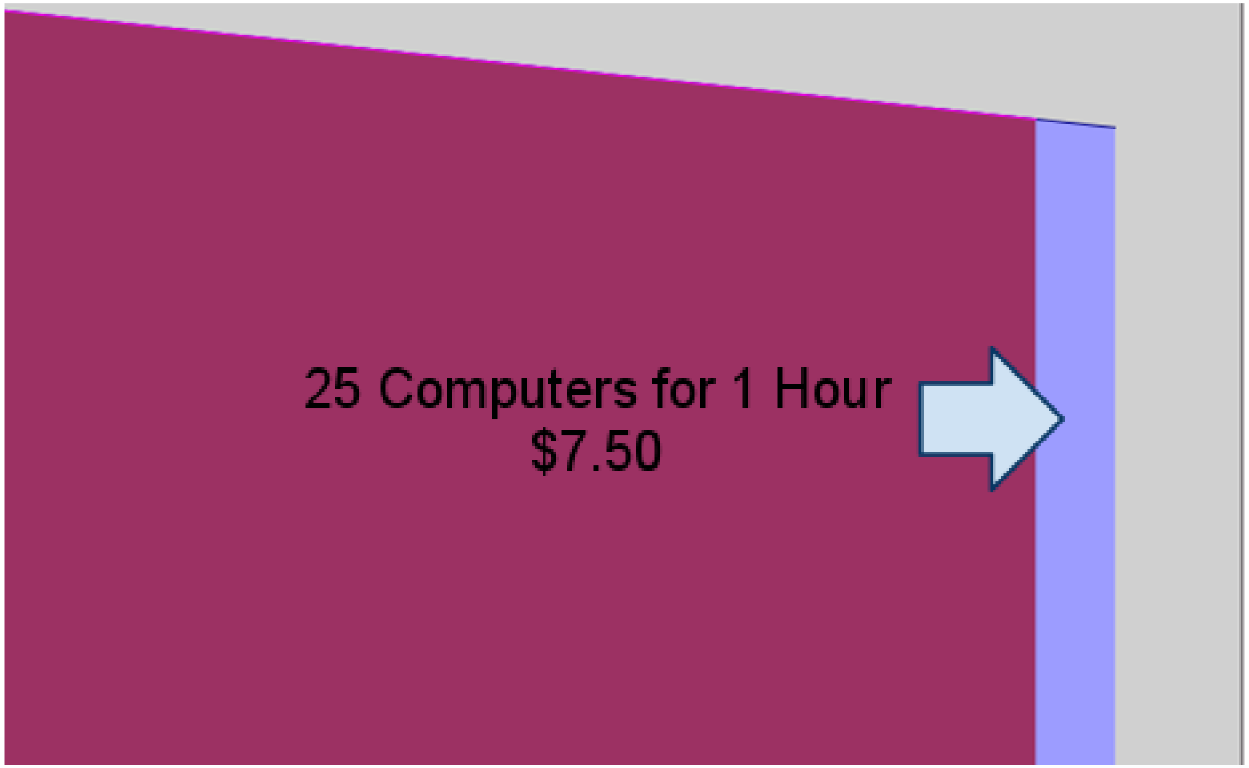
Misconceptions about Polynomials



25 Computers for 1 Hour
$7.50

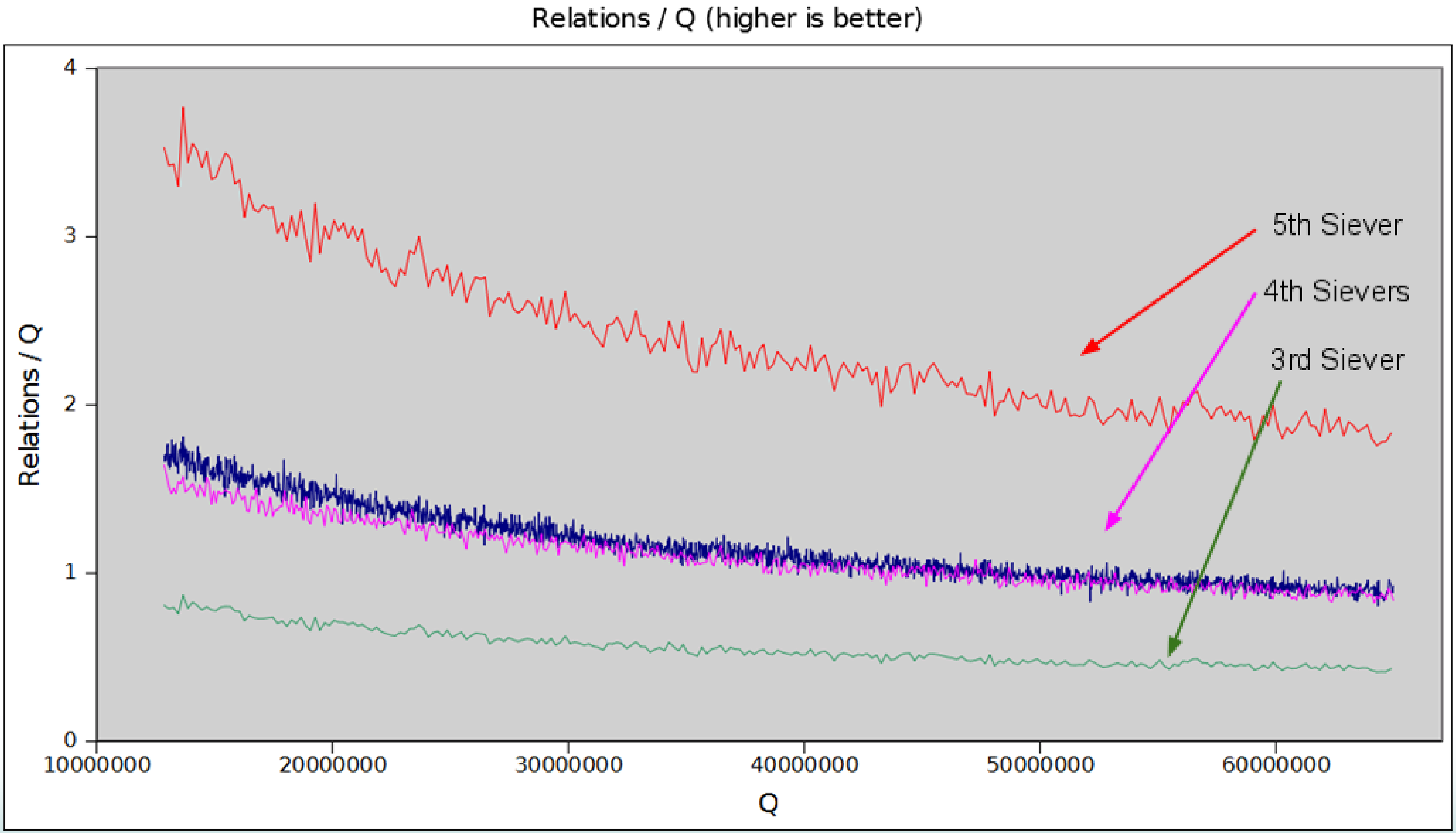
Misconceptions about Polynomials

If time is more valuable to you than (a relatively little) money it is in your best interest to take the first polynomial you get and sieve with that, rather than doing another poly-selection run.

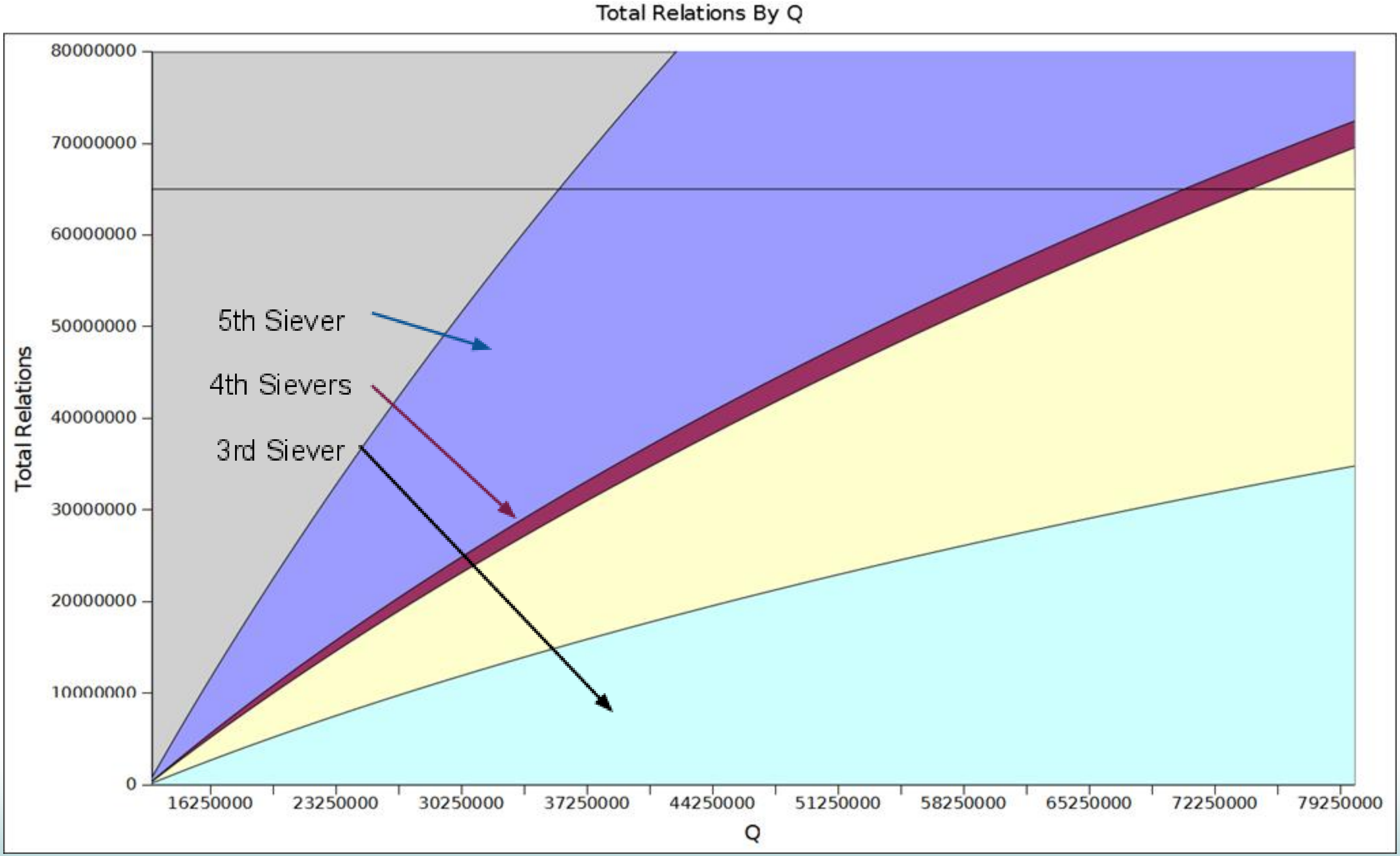


(this advice is only
for 512-bit semiprimes.)

Siever Comparisons



Siever Comparisons

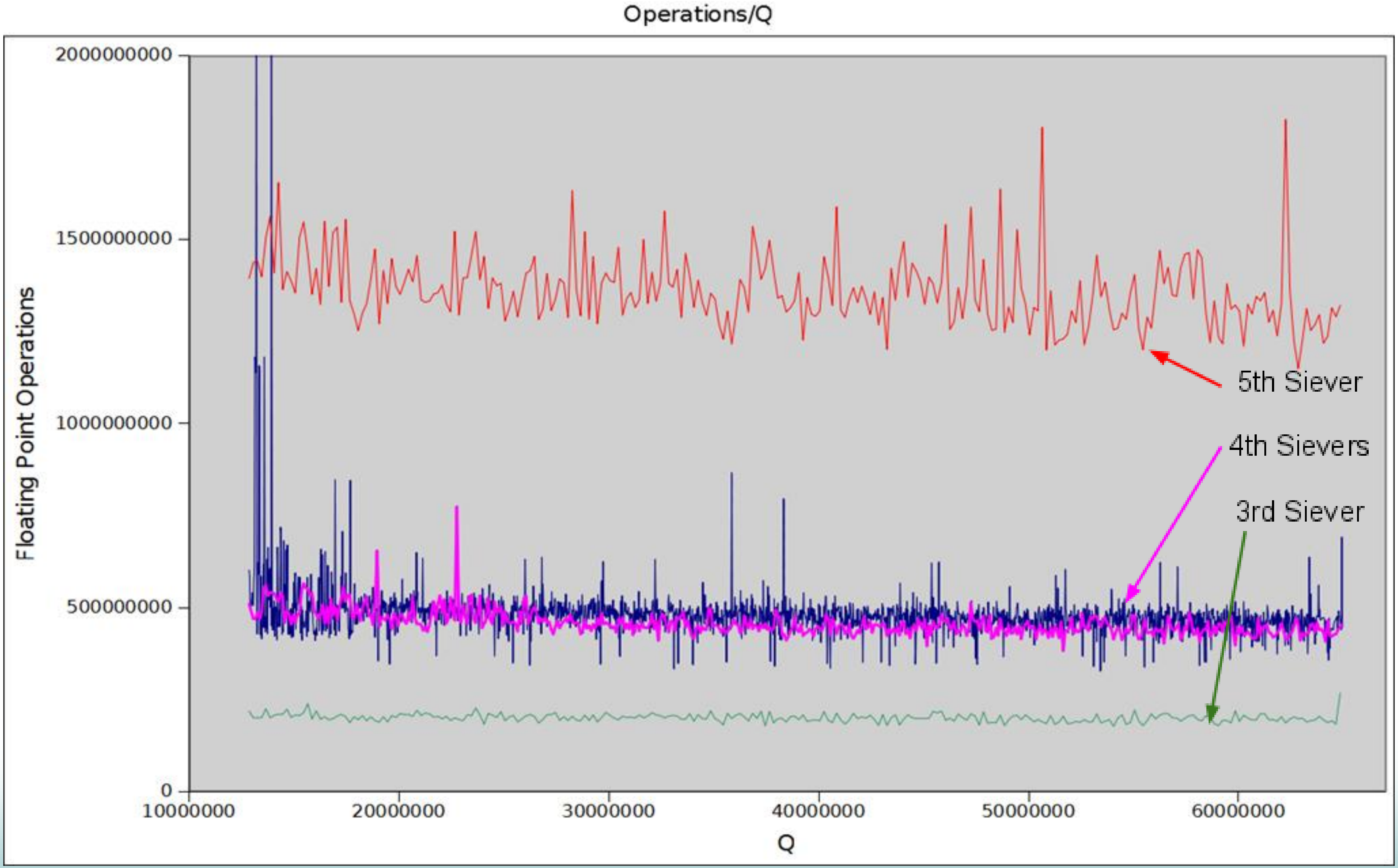


5th Siever

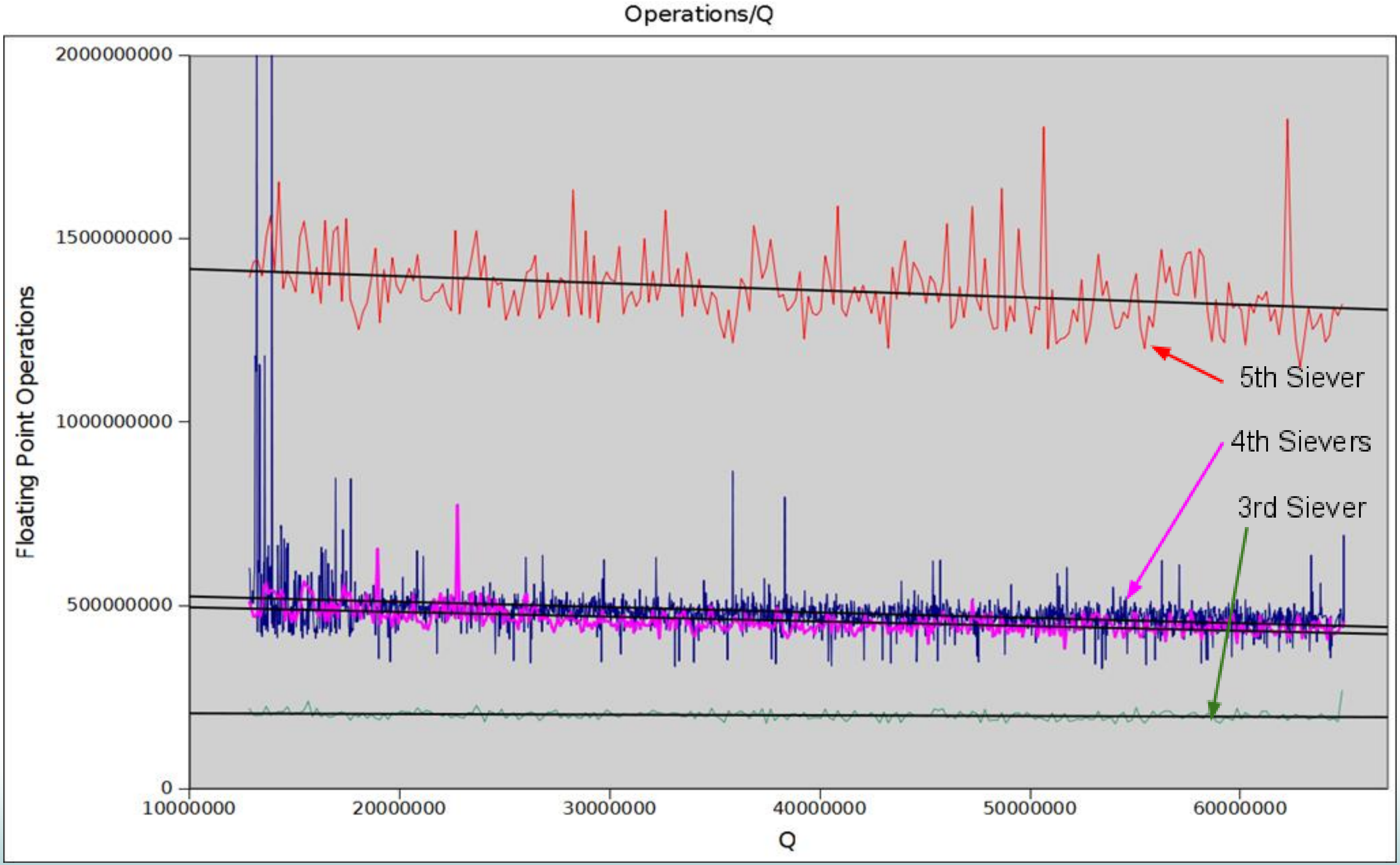
4th Sievers

3rd Siever

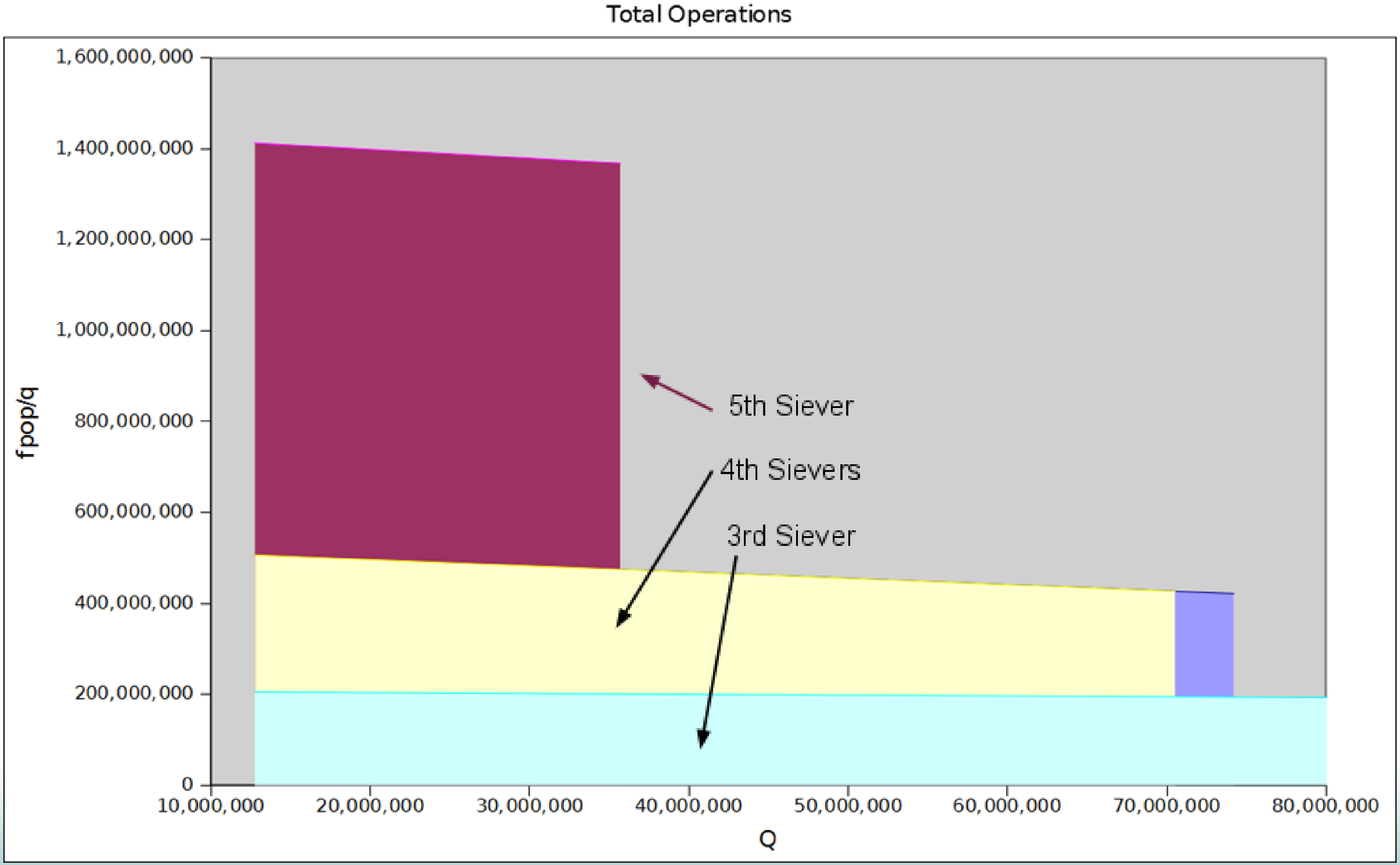
Siever Comparisons



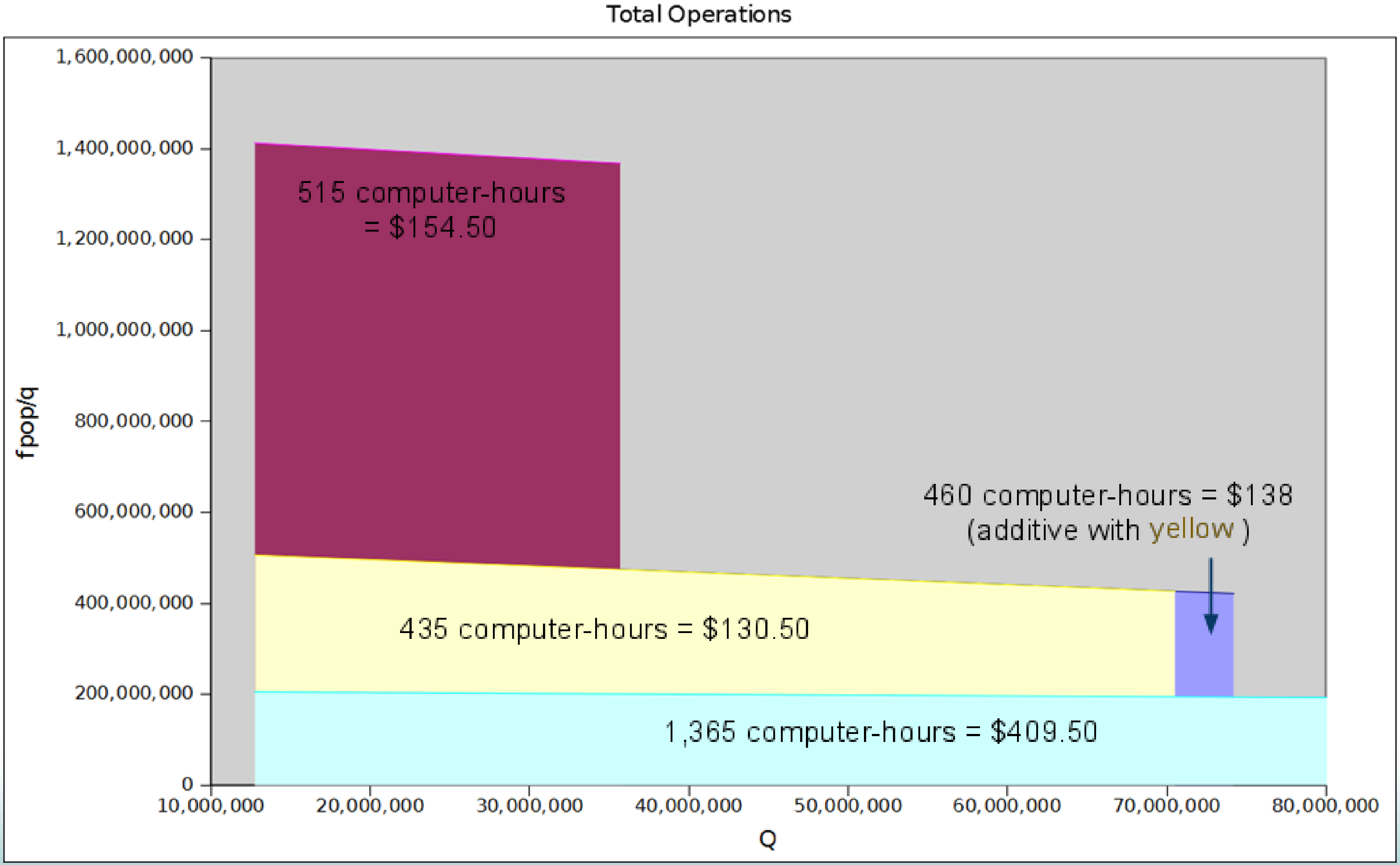
Siever Comparisons



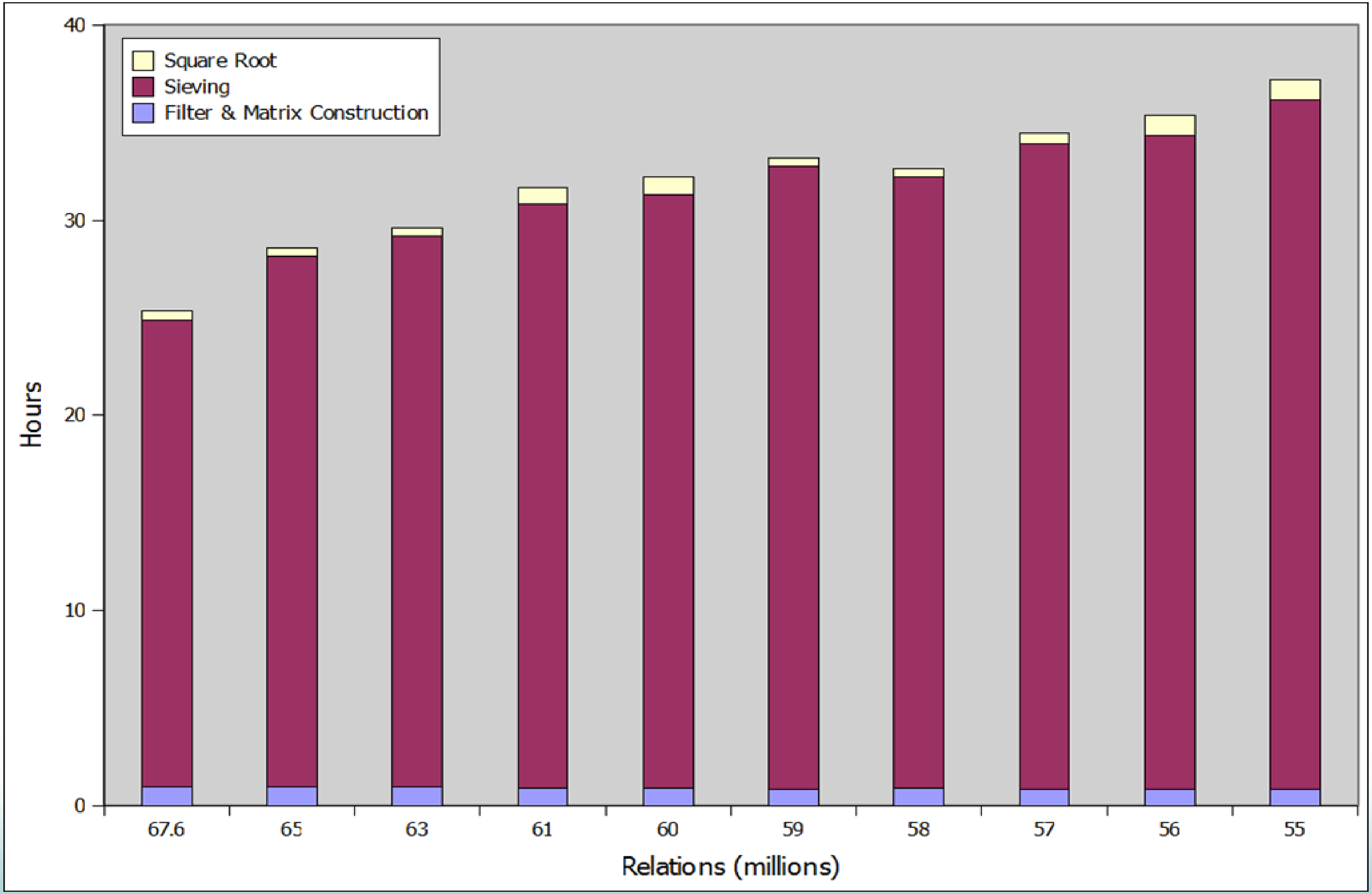
Siever Comparisons



Siever Comparisons



Oversieving



Obligatory Ending Slide

Fin

Thanks:

- GDS
- NYSec
- MersenneForum & jasonp

Tom Ritter
http://ritter.vg
(encrypted mail preferred)

Big Ups To:

- jasonp

http://www.gdssecurity.com/
https://github.com/GDSSecurity/cloud-and-control