Large near-optimal Golomb rulers, a computational search for the verification of Erdos conjecture on Sidon sets

Apostolos Dimitromanolakis

joint work with Apostolos Dollas (Technical University of Crete)

Definition of a Golomb ruler

- Golomb ruler: a set of positive integers (marks) $a_1 < a_2 < \ldots < a_n$ such that all the positive differences $a_i - a_j$, $i > j$ are distinct.
- Goal: minimize the maximum difference $a_i - a_j$, the length of the ruler. Usually the first mark is placed in position 0.

- This ruler measures distances 1,2,3,4,5,7,8,9,10,11 and has length 11.
- $G(n)$ is defined as the minimum length of a ruler with n marks (an optimal ruler).
- No closed form solution exists for $G(n)$.

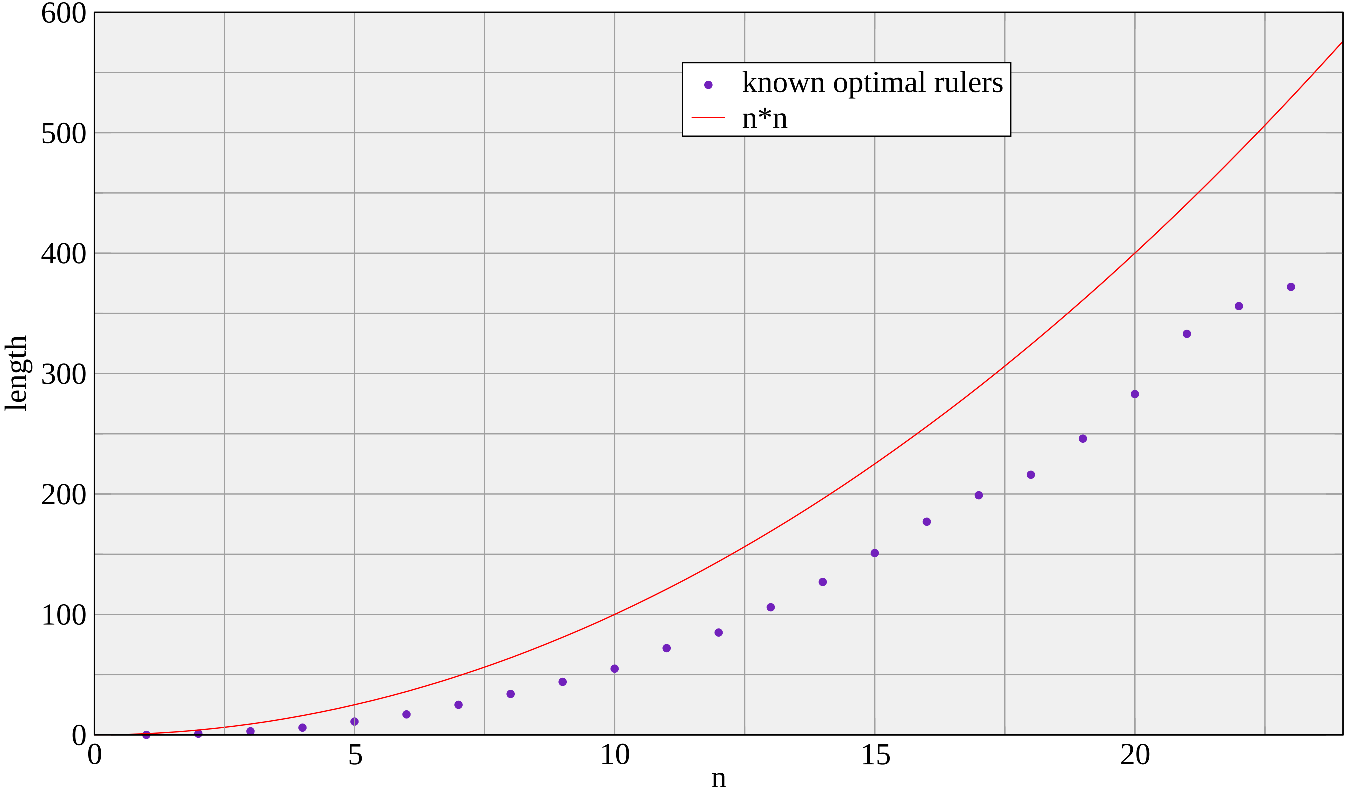
Applications of Golomb rulers

- Radio-frequency allocation for avoiding third-order interference (Babock 1953)
- Generating C.S.O.C. (convolutional self-orthogonal codes) (Robinson 1967)
- Linear telescope arrays in radioastronomy for maximization of useful observations (Blum 1974)
- Sensor placement in crystallography etc.

Near-optimal Golomb rulers

- No algorithm for finding optimal Golomb rulers exists apart from exhaustive (exponential in the number of marks).
- Up to now optimal Golomb rulers are known for up to 23 marks (applications need a lot more!).
- To find the 23-mark ruler, 25000 computers were used in a distributed effort for several months (co-ordinated by distributed.net / project OGR).
- Not possible to apply exhaustive search for a large number of marks.
- Near-optimal rulers: a ruler whose length is close to optimal (in our context this means length less than n^2)

Length of known optimal rulers



Sidon sets

Definition:

A Sidon set (or B_2 sequence) is a subset $a_1, a_2, \ldots, a_n$ of $\{1, 2, \ldots, n\}$ such that the sums $a_i + a_j$ are all different.

- $F_2(d)$: maximum number of elements that can be selected from $\{1,2,\ldots,d\}$ and form a Sidon set.

Known limits for $F_2(d)$

➠ Upper bounds

- Trivial: $F_2(d) \leqslant \sqrt{2}\, d^{1/2}$.
- Erdős 1941: $F_2(d) < d^{1/2} + O(d^{1/4})$
- Lindstrom 1969: $F_2(d) < d^{1/2} + d^{1/4} + 1$

➠ Lower bounds

- much harder (usually one has to exhibit an actual ruler to prove)
- Constructions prove that $F_2(d) > d^{1/3}$
- Asymptotic bound:
  $F_2(d) > d^{1/2} - O(d^{5/16})$ (Erdős 1944)

Equivalence of the two problems

- Sidon sets and Golomb rulers are equivalent problems! See that

$$a_i + a_j = a_k + a_l \iff a_i - a_k = a_l - a_j$$

- Fragmentation of the research community. Sometimes results were proven again.
- In 1967 Atkinson et al proved that asymptotically Golomb rulers have length n^2, already proven in 1944 by Erdős

Differences between the two problems

- Golomb rulers:
  - have 0 as a element
  - $G(n)$ is the **mininum length** of ruler with n marks
- Sidon sets:
  - minimum element is 1
  - $F_2(n)$ is the **maximum number of elements** that can be selected from $1, \ldots, n$

Easy things to prove

- If a value is know for F_2:

$$F_2(d) = n \quad \Longleftrightarrow \quad \begin{array}{l} G(n) \leqslant d - 1 \\ G(n+1) > d - 1 \end{array}$$

- If a value is known for $G(n)$:

$$G(n) = d \quad \Longleftrightarrow \quad \begin{array}{l} F_2(d) = n - 1 \\ F_2(d+1) = n \end{array}$$

Inverse relations between G and F_2

- The next theorem allows easy restatement of bounds between the two problems.
- **Theorem 1:** For any two functions l and u,

$$l(d) < F_2(d) < u(d) \;\Rightarrow\; u^{-1}(n) < G(n) + 1 < l^{-1}(n)$$

- and also for the other direction: For any functions l and u,

$$l(n) < G(n) < u(n) \;\Rightarrow\; u^{-1}(d) \leqslant F_2(d) \leqslant l^{-1}(d)$$

- F_2 and G are essentially inverse functions.

An improved limit for $G(n)$

- Lindstom (1969) proved that $F_2(d) < d^{1/2} + d^{1/4} + 1$
- Using theorem 1 it follows that:

$$G(n) > n^2 - 2n\sqrt{n} + \sqrt{n} - 2$$

(not known to the Golomb ruler community)

A conjecture

- A conjecture for Golomb rulers:

$$G(n) < n^2 \text{ for all } n > 0$$

- First mentioned by Erdős in the 40's in an equivalent form: $F_2(n) > \sqrt{n}$
- Known to be true for $n \leqslant 150$ (but the rulers obtained are not proven optimal).

Our goal:

- extend this computational verification of the conjecture, and
- exhibit the near-optimal Golomb rulers for use in applications.

Constructions for Golomb rulers

- For finding near-optimal rulers with $\geqslant 24$ marks exhaustive search is not a possibility.
- Our approach: use constructive theorems for Golomb rulers/Sidon sets.
- A simple construction: For any n the set

$$na^2 + a \quad , \quad a = \{0, 1, \ldots, n-1\}$$

is a Golomb ruler with n marks. Maximum element: $n^3 - 2n^2 + 2n - 1$

- A construction by Erdős: When p is prime

$$2pa + (a^2)_p \;, \quad 0 \leqslant a < p$$

forms a Golomb ruler with p marks. Maximum element: $\approx 2p^2$

Modular constructions

The next 3 constructions are modular:

- Every pair a_i,a_j has a different difference modulo some integer m: $a_i - a_j \neq a_k - a_l \ (mod\ m)$
- Each pair generates two differences: $a_i - a_j \ (mod\ m)$ and $a_j - a_i \ (mod\ m)$
- $n(n-1)$ instead of $\frac{1}{2}n(n-1)$ different distances: so $m \geqslant n(n-1)$

Ruzsa construction (1993)

$$R(p,g) = pi + (p-1)g^i \mod p(p-1) \quad \text{for } 1 \leqslant i \leqslant p-1$$

p : prime number

g : primitive element $Z_p^* = \mathrm{GF}(p)$

- $n = p - 1$ elements modulo $p(p-1)$
- Maximum element: $\approx n^2 + n$ for a ruler with n elements (but $n+1$ must be prime!).
- Possible to extract subquadratic Golomb rulers
- for example ($g = 3, p = 7$) generates the modular Golomb ruler $\{6, 10, 15, 23, 25, 26\} \mod 42$

Bose-Chowla construction (1962)

$$B(q,\theta) = \{a : 1 \leqslant a < q^2 \ \text{ and } \ \theta^a - \theta \in GF(q)\}$$

q : prime or prime power p^n

θ : primitive element of Galois field $GF(q^2)$

- $n = q$ elements modulo $q^2 - 1$
- relatively slow construction (operations on 2nd degree polynomials required)
- length of ruler generated $< n^2 - 1$ (already subquadratic but works only for prime powers)

Singer construction (1938)

There exist $q+1$ integers that form a modular Golomb ruler

$$d_0, d_1, \ldots, d_q \mod q^2+q+1$$

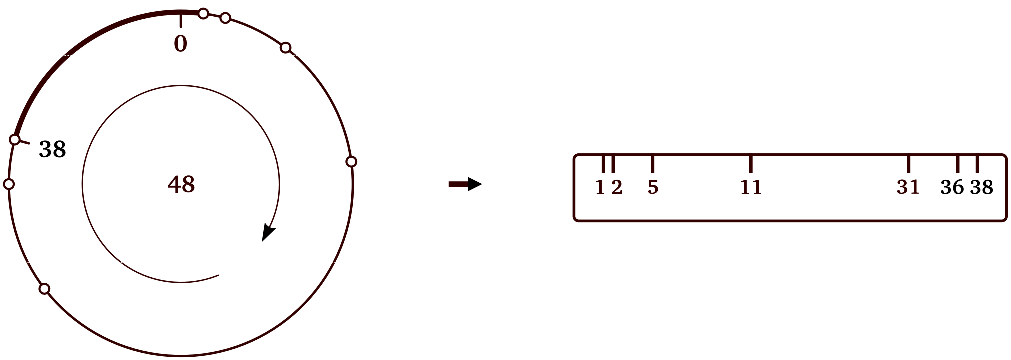
whenever q is a prime or prime power p^n

- $n = q+1$ elements modulo q^2+q+1
- very unpractical to apply (3rd degree polynomial calculations)
- maximum element $< n^2-n+1$

Generating a Golomb ruler from a modular set

From a modular construction with n marks Golomb rulers with n, $n-1, \ldots$ marks can be extracted:

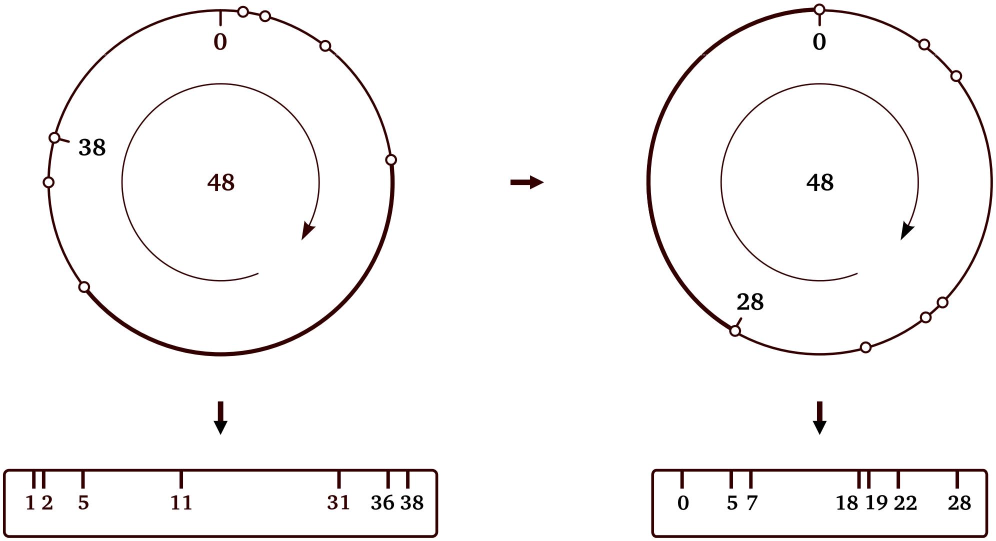
$$\{1,2,5,11,31,36,38\} \quad \text{mod } 48 \quad \text{(Bose-Chowla)}$$



- a ruler with 7 marks: $\{1,2,5,11,31,36,38\}$
- a ruler with 6 marks: $\{1,2,5,11,31,36\}$

Rotations

$$\{1, 2, 5, 11, 31, 36, 38\} \mod 48$$



- If $a_i \mod q$ is a modular Golomb ruler then so is $a_i + k \mod q$.
- Rotating a modular construction may result in a shorter Golomb ruler being extracted.

Multiplication

If $a_i \mod q$ is a modular Golomb ruler and $(g, q) = 1$ then $g \cdot a_i \mod q$ is also a modular ruler.

- The number of possibly multipliers is the number of integers $< q$ such that $(g, q) = 1$: Euler ϕ function
- A multiplication of a modular construction may also result in extracting a shorter Golomb ruler.

The computational search

The conjecture: $G(n) < n^2$ for all $n > 0$

- Up to now verified for $n \leqslant 150$: Lam and Sarwate (1988)
- Goal of our work: extend this result for $n \leqslant 65000$.

Approach

- For the this search we used two of the constructions (Ruzsa & Bose-Chowla)
- These constructions only apply when n is a prime or prime power.
- Not possible to directly generate a ruler for number of marks between two primes directly!
- For the cases where n is not prime we used the construction for the next larger prime and removed the extra elements.
- Search through all possible multipliers and rotations to find the shortest ruler.

Algorithms

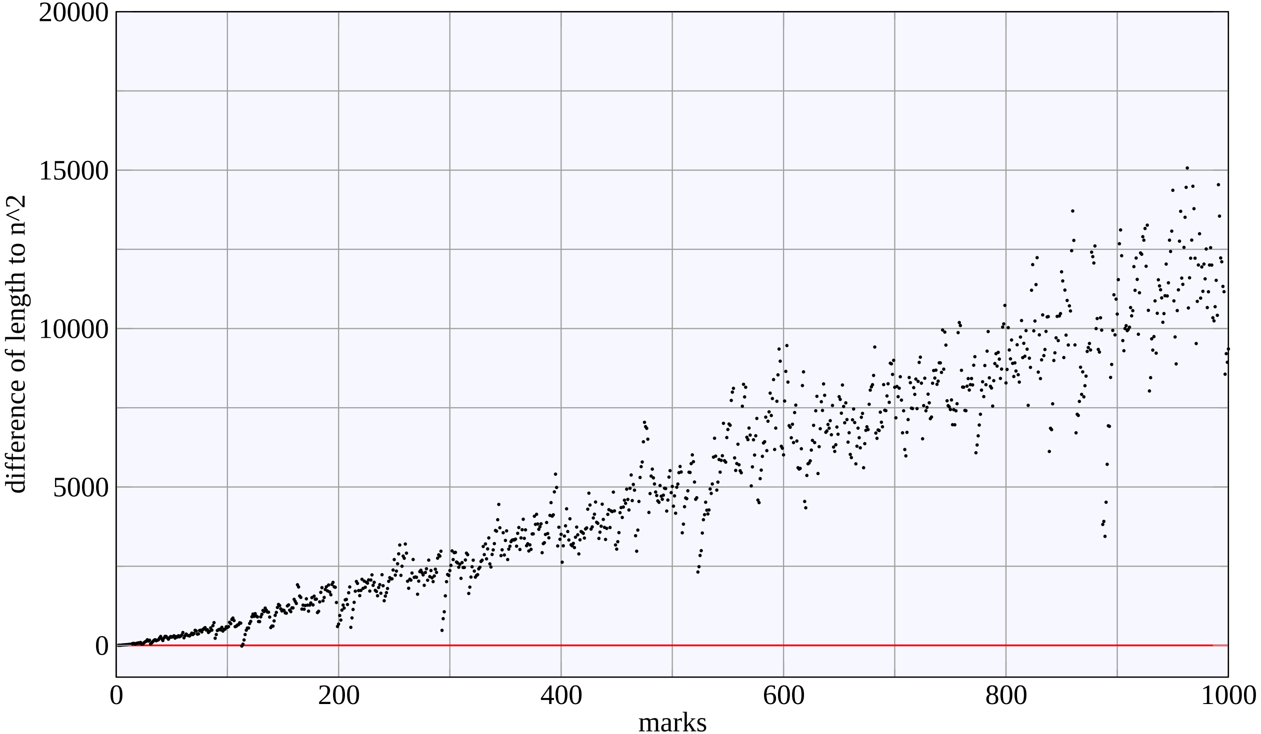
Two algorithms were implemented for an efficient search:

- RUZSA-EXTRACT$\{l, p\}$: Uses Ruzsa construction for prime p and returns the best rulers found with l,$l+1$,...,$p-1$ marks. Running time $T_1(l, p) = O(\ p^2(p-l)\ )$
- BOSE-EXTRACT$\{l, p\}$: Uses Bose-Chowla construction for p prime and produces rulers with l,$l+1$,...,p marks. Running time $T_2(l, p) = O(\ p^3 \log p + p^2(p-l)\ )$
- RUZSA-EXTRACT was the main workhorse and BOSE-CHOWLA was used to settle the remaining cases.
- The algorithms check for each number of marks which is the shortest ruler we can extract from the next larger possible construction.

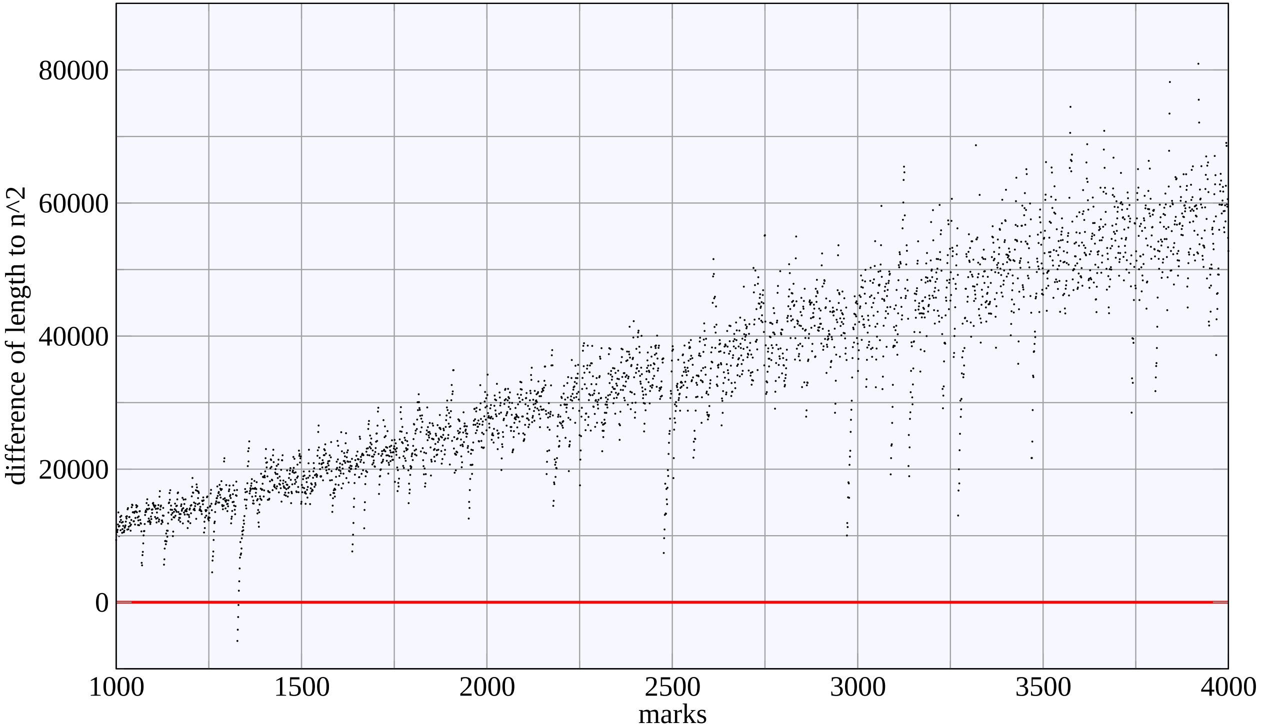
The technical details

- Both algorithms were implemented in C using the LiDIA library for computations in Galois fields.
- C was chosen for speed, Mathematica would take years to finish.
- A distributed network of 10 1.5GHz personal computers running Linux was used for 5 days for the computation of RUZSA-EXTRACT up to 65000 marks.

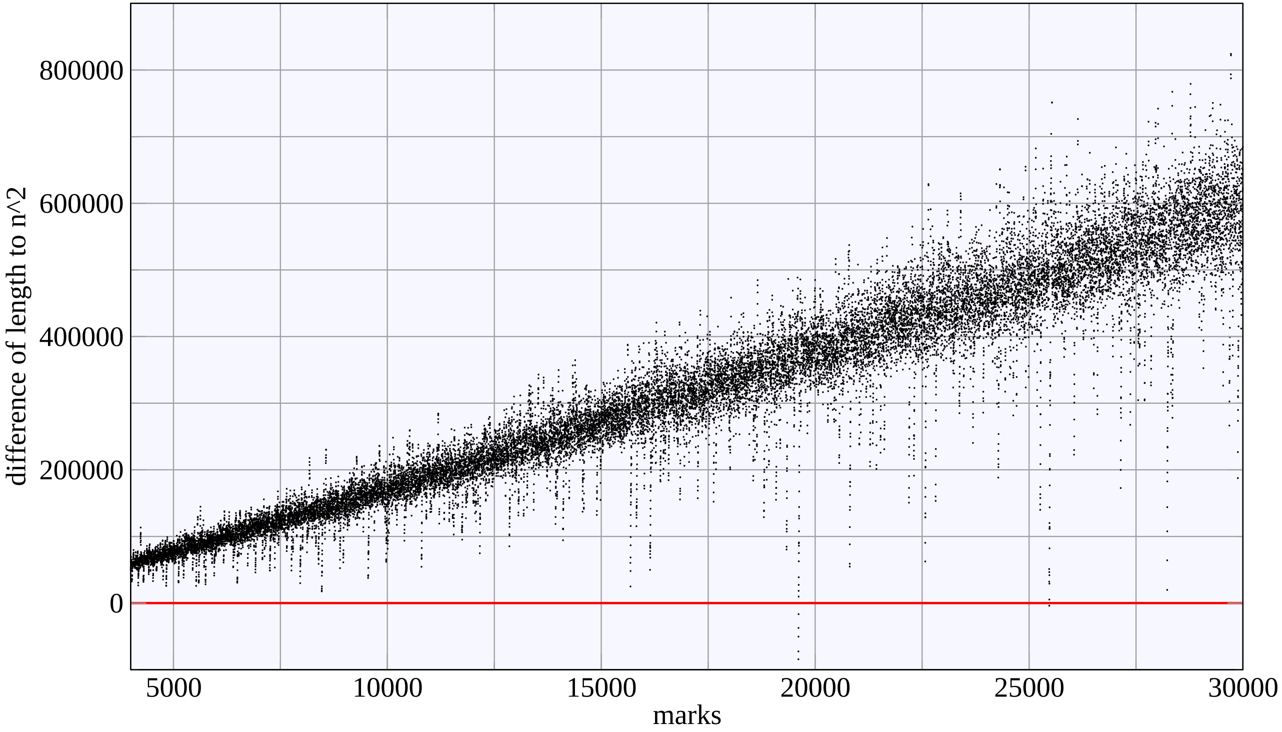
Results (0-1000 marks)



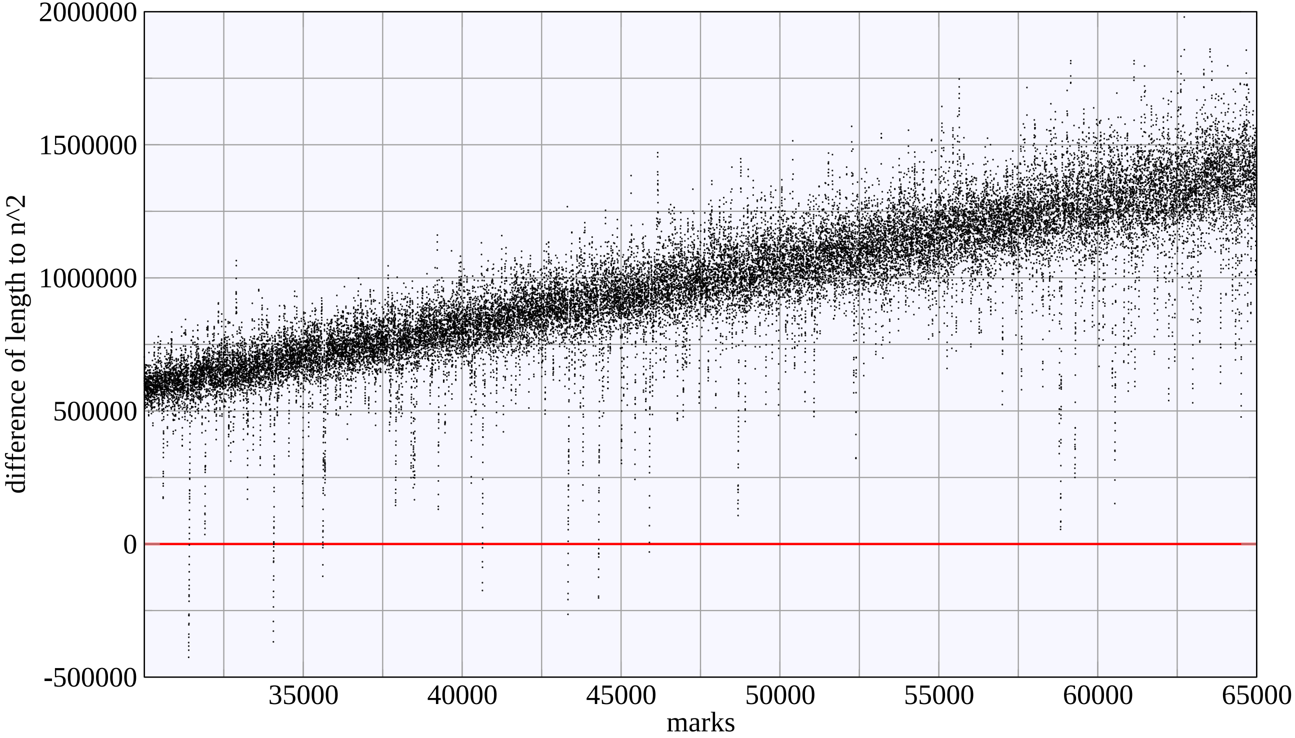
Results (1000-4000 marks)



Results (4000-30000 marks)



Results (30000-65000 marks)



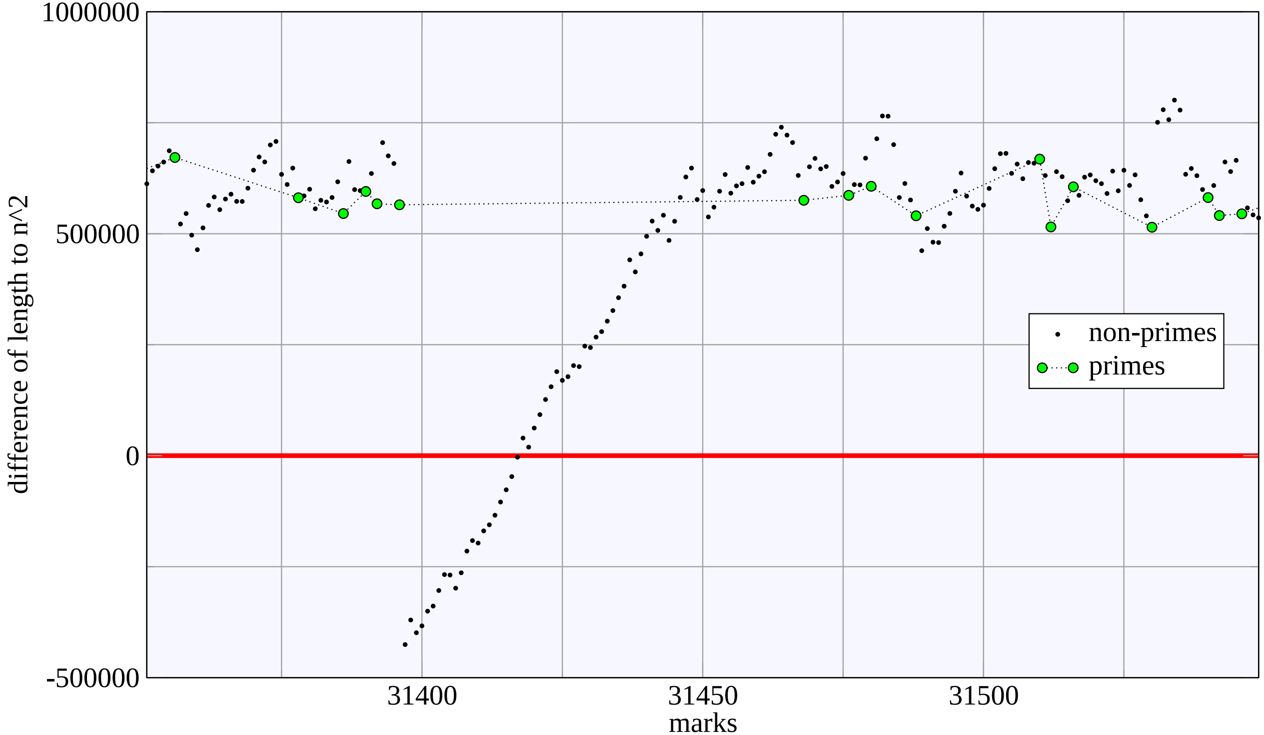
Negative results

- The algorithm was unable to find sub-quadratic length rulers precisely in the cases where there is a large prime gap. In total 72 out of 65000 rulers turned out to be of length $\geqslant n^2$:

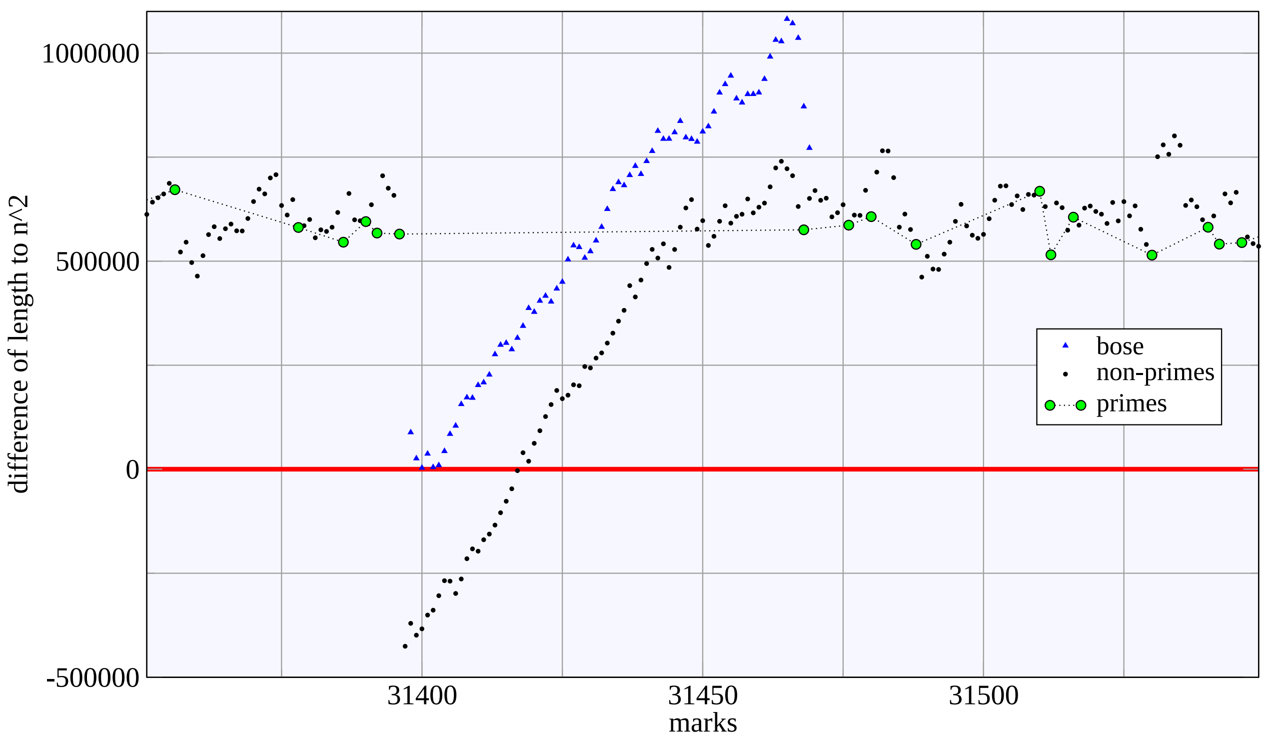
number of marks	prime gap	length of gap
113	113 – 127	14
1327 – 1330	1327 – 1361	34
19609 – 19613	19609 – 19661	52
25474	25471 – 25523	52
31397 – 31417	31397 – 31469	72
34061 – 34074	34061 – 34123	62
35617 – 35623	35617 – 35671	54
40639 – 40643	40639 – 40693	54
43331 – 43336	43331 – 43391	60
44293 – 44301	44293 – 44351	58
45893	45893 – 45943	50

- For these cases the much slower Bose construction was used to find sub-quadratic rulers.

A bad case with a large prime gap



A bad case settled



Conclusion - Summary

- We proved a theorem that allows the easy restatement of bounds between $G(n)$ and $F_2(n)$. An improved bound for $G(n)$ followed: $G(n) > n^2 - 2n\sqrt{n} + \sqrt{n} - 2$
- We extended the verification of Erdős conjecture and computationally proved that
$$G(n) < n^2 \text{ for } n \leqslant 65000$$
(previously it has been verified for up to 150 marks).
- In Sidon set terms: $F_2(n) < \sqrt{n}$ for all $n \leqslant 4.225.000.000$.
- The results and the code can be found at the thesis web page (relocated in Toronto): http://www.cs.utoronto.ca/~apostol/golomb
- In the future: extend the search for even larger Golomb rulers (will be much slower though)