Golomb Rulers

Adapted from notes by Yingkun Li

High School I - 12/2/2018

1 Introduction

A foot-long ruler has 13 "inch marks," labelled '0' to '12'. Suppose, however, that on your favorite ruler (which you carry at all times), some of the marks have worn off, leaving:

$$0, 1, 2, 3, 5, 7, 9, 11, 12.$$

Even though the mark '4' is gone, you can still measure a length of 4 inches using the marks '1' and '5', or the marks '3' and '7'. In the example above, it is not hard to see that each of the distances 1 inch, 2 inches, $\ldots$, 12 inches, can be measured by some pair of marks. In this case, we say that the ruler is **spanning**.

If more marks are missing however, then the ruler would no longer be spanning. For example, the following ruler is not spanning

$$0, 1, 3, 7, 12,$$

since it is not possible to measure a distance of 8 inches using a pair of marks. On the other hand, those distances that can be measured can only be done in one way. For example, it is only possible to measure a distance of 6 inches, by using only the marks '1' and '7'. We call it a **Golomb** ruler.

The ruler described above has many applications. For example, suppose we want to locate the source of a wave (light, sound, water, etc.) using a series of detectors. We can line up the detectors, set them to receive the same frequency, and measure the phase difference between the pairs of detectors. To maximize the accuracy, the distances between pairs of detectors need to be distinct. This idea can be applied in radio astronomy to locate a faraway radio source in space. In this case, the detectors are large and expensive telescopes. It makes sense to use as few of them as possible to maximize accuracy. In addition, one can use Golomb rulers to reduce intermodulation distortions in radio communication [**?**], and to reduce ambiguity in X-ray analysis of crystal structures [**?**].

Exercise 1. Please give 3 examples of spanning foot-long rulers with at most 7 marks remaining.

Exercise 2. Please give an example of a spanning foot-long ruler, which is no longer spanning if any of the remaining marks is erased.

Exercise 3. Find the smallest number n such that any foot-long ruler with n marks, including '0' and '12', is spanning.

Exercise 4. Please give another example of a foot-long Golomb ruler with 5 marks. What about with 6 marks? What is the most number of marks a foot-long Golomb ruler can have?

Exercise 5. Can you give an example of a foot-long Golomb ruler which is spanning? If not, can you prove that such ruler does not exist?

2 Golomb Ruler

After looking at the warm-up problems, it is natural to ask similar questions for a ruler with an arbitrary integral length L. For example, how many marks can a spanning ruler of length L have? What about a Golomb ruler of length L? For which length L is there a spanning Golomb ruler of length L?

To answer these questions, we need to setup the mathematical notations. We represent marks on a ruler using a set of nonnegative natural numbers $\{a_1, a_2, \ldots, a_n\}$, where

$$a_1 < a_2 < \cdots < a_n.$$

The number of marks, n, is called the **size** of the ruler, and its **length** L is

$$L = a_n - a_1.$$

Remark 1. We will consider two such sets to represent the same ruler if one can be translated or reflected to become the other. For example, $\{0, 1, 3, 7\}$ and $\{4, 5, 7, 11\}$ represent the same ruler, because the second set can be obtained by adding four to each element of the first. Similarly, $\{0, 1, 3, 7\}$ and $\{0, 4, 6, 7\}$ represent the same ruler, since the second one is obtained by reflecting the elements of the first about the midpoint 3.5.

Definition 1. A set $\{a_1, \ldots, a_n\}$ with $a_i < a_{i+1}$ is called a **Golomb ruler** if for any two distinct pairs of integers, say $a_i < a_j$ and $a_m < a_n$, satisfy $a_j - a_i \neq a_n - a_m$. It is called a **spanning** ruler if for every positive integer $M \leq a_n - a_1$, there exists indices $1 \leq i < j \leq n$ such that $M = a_j - a_i$. A spanning Golomb ruler is called **perfect**.

Exercise 6. Find another set of integers that represent the ruler $\{0, 2, 3, 5, 11\}$. What about a general ruler $\{a_1, a_2, \ldots, a_n\}$?

Exercise 7. Give three examples of Golomb rulers of length 20 and size 6 such that they are not physically the same.

Exercise 8. How many of the Golomb rulers you gave in the previous exercise are perfect?

It seems that coming up with perfect rulers is not so easy. As we will see, there are very few perfect rulers.

Theorem 1. *The only physically distinct perfect rulers are* $\{0\}, \{0, 1\}, \{0, 1, 3\}$ *and* $\{0, 1, 4, 6\}$.

The proof of this theorem can be deduced from the following series of exercises.

Exercise 9. Verify that the rulers in the theorem are all the physically distinct perfect rulers with at most 4 marks.

Exercise 10. Show that a Golomb ruler of size n must have length at least $\frac{n(n-1)}{2}$. It has this size exactly when it is perfect.

Exercise 11. Suppose that $\{0, a_2, a_3, a_4 \ldots, a_{n-2}, a_{n-1}, L\}$ is a perfect ruler of length $L \geq 10$. Prove that $n \geq 5$ and either $a_2 = 1$ or $a_{n-1} = L - 1$, but not both.

Exercise 12. Suppose that $\{0, 1, a_3, a_4 \ldots, a_{n-2}, a_{n-1}, L\}$ is a perfect ruler of length $L \geq 10$. Prove that $a_3 = 4$ and $a_{n-1} = L - 2$.

Exercise 13. Suppose that $\{0, 1, 4, a_4 \ldots, a_{n-2}, L - 2, L\}$ is a Golomb ruler of length $L \geq 10$. Prove that it cannot be perfect.

Exercise 14. Use the previous exercises to conclude the proof of Theorem **??**.

3 Constructions of Golomb Rulers

Since perfect Golomb rulers are rare, it is natural to consider "less perfect" Golomb rulers. Instead of trying to measure every distance, we will try to measure as many distances as possible.

Definition 2. Among all Golomb rulers of a fixed size r, let $G(r)$ be the shortest possible length. A Golomb ruler of size r is call **optimal** if it has length $G(r)$.

It is not too difficult to see that perfect Golomb rulers are also optimal (why?). For an arbitrary r, it is an interesting algorithmic problem to determine $G(r)$. The current record for the largest $G(r)$ for any r is $G(26) = 492$. It is given by:

$$0, 1, 33, 83, 104, 110, 124, 163, 185, 200, 203, 249, 251, 258,$$
$$314, 318, 343, 356, 386, 430, 440, 456, 464, 475, 487, 492.$$

Although there is no explicit formula for $G(r)$, we could try to bound it from below and above. The naïve lower bound is

$$G(r) \geq \frac{r(r-1)}{2} \quad \text{(see Exercise ??)}.$$

For the upper bound, we need to find a way to construct Golomb rulers of size r. Here is a simple construction:

Construction 1. Let $r \geq 5$ be any positive integer. The following sequence forms a Golomb ruler:

$$a_n = (rn - r - 1)(n - 1), 1 \leq n \leq r.$$

Exercise 15. Prove that the sequence above indeed gives a Golomb ruler.

Exercise 16. Use the first construction to make a Golomb ruler of size 5.

Exercise 17. The Golomb ruler constructed above has size r. Calculate its length and conclude that we have the upper bound $G(r) < r^3$.

Note that this construction tells us $G(r) < r^3$, but we only know $G(r) \geq r(r-1)/2$. When r is large, these two numbers are very far apart, so we still don't have much information about the "true" size of $G(r)$.

Construction 2 (CHALLENGE)

Here is another more clever construction, which uses modular arithmetic. However, it has the drawback that it only works for r being one less than a prime number.

Let $\mathbb{Z}/p\mathbb{Z}$ represent the integers modulo a prime p. Recall, Fermat's Little Theorem states that $a^{p-1} \equiv 1$ for all $a \in \mathbb{Z}/p\mathbb{Z}$. Additionally, a primitive element g in $\mathbb{Z}/p\mathbb{Z}$ is such that $g^{p-1} \equiv 1 \pmod{p}$ and $g^k \not\equiv 1 \pmod{p}$ for all $1 \leq k \leq p-1$.

Construction 2. Let p be a prime number and g a primitive element of $\mathbb{Z}/p\mathbb{Z}$. The following sequence is a Golomb ruler of size $p - 1$.

$$R(p, g) = p \cdot n + (p-1)g^n \bmod p(p-1), 1 \leq n \leq p-1$$

Proof. To show that distances measured by distinct pairs of marks are different, it suffices to prove that sums of distinct pairs of marks are all different.

Let $1 \leq m \leq n \leq p-1$ and $0 \leq a \leq p(p-1)$ such that

$$p \cdot m + (p-1)g^m + p \cdot n + (p-1)g^n \equiv a \pmod{p(p-1)}. \tag{1}$$

By considering the left hand side modulo p and $p-1$ separately, we conclude that

$$\begin{aligned} (m+n) &\equiv a \pmod{p-1} \\ (g^m + g^n) &\equiv -a \pmod{p}. \end{aligned}$$

By Fermat's Little Theorem, the equations above are equivalent to

$$g^{m+n} \equiv g^a \pmod{p} \tag{2}$$
$$(g^m + g^n) \equiv -a \pmod{p}. \tag{3}$$

Now consider the following quadratic equation over the finite field $\mathbb{Z}/p\mathbb{Z}$

$$X^2 + aX + g^a = 0. \tag{4}$$

By equations (**??**), we know that $X = g^m, g^n$ are roots of this polynomial. Furthermore, suppose there is another pair of (m', n') satisfying equation (**??**) and $1 \leq m' \leq n' \leq p-1$. Then by the reasoning above $X = g^{m'}, g^{n'}$ are also solutions of the polynomial (**??**). It is a fact that a quadratic polynomial over $\mathbb{Z}/p\mathbb{Z}$ has only two solutions. Thus we have $m = m', n = n'$ so the sum of two marks is unique. □

Remark 2. The construction above tells us that $G(r) \leq (r+1)r$ when $r = p-1$ for p a prime number. So the naïve lower bound above is not too bad when r is large and one less than a prime number.

Exercise 18. Use the second construction to make a Golomb ruler of size 6.

Exercise 19. Given $G(5) = 11, G(6) = 17$, could you improve the constructions above to produce the optimal Golomb rulers of size 5 and 6?

Exercise 20. For any positive integer r, let $p(r)$ be the smallest prime greater than r. Prove that $G(r) \leq p(r) \cdot (p(r) - 1)$.

References

[1] R.C. Alperin, V. Drobot, *Golomb Rulers*, Math. Mag. 84 (2011) 48–55.

[2] W.C. Babcock, *Intermodulation Interference in Radio Systems.*, Bell Systems Technical Journal, 63–73, January (1953).

[3] G.S. Bloom, S.W. Golomb, *Applications of numbered undirected graphs*, Proc. IEEE 65 April (1977) 562–570.

[4] A. Dimitromanolakis, *Analysis of the Golomb ruler and the Sidon set problem, and determination of large near-optimal Golomb rulers*, Diploma thesis, Technical University of Crete (Greece) 2002. (See http://www.cs.toronto.edu/~apostol/golomb for the English version)

[5] N. Jacobson, *Basic Algebra I*, W.H. Freeman and Company, New York (2009)

[6] I.Z. Ruzsa, *Solving a linear equation in a set of integers I*, Acta Arithmetica LXV.3 (1993), 259–282.