GOLOMB RULER AND RELATED QUESTIONS

YINGKUN LI

1. Warm-up Questions

A foot-long ruler has 13 inch marks, from 0 to 12. After using for a while though, some of the marks in the middle are missing. For example, we can have the following marks left

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

Even though the mark '4' is gone, we 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 the distances 1 inch, 2 inches, etc., up to 12 inches can be measured by some pairs of marks. In that case, we say that this 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.

(1) Please give 3 examples of spanning foot-long rulers with at most 7 marks remaining.
(2) Please give an example of a spanning foot-long ruler, which is no longer spanning if any of the remaining marks is erased.
(3) Find the smallest number n such that any foot-long ruler with n marks, including '0' and '12', is spanning.
(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?
(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?

Date: May 12, 2016.

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 N. For example, how many marks can a spanning ruler of length N have? What about a Golomb ruler of length N? For which length N is there a spanning Golomb ruler of length N?

To answer these questions, we need to setup the mathematical notations. We represent marks on a ruler with length N using a set of natural numbers $\{a_1, a_2, \dots, a_n\}$ such that

$$0 \le a_1 < a_2 < \cdots < a_n = N + a_1.$$

The **size** of a ruler is the number of marks, including the endpoints, which is n in this case.

Remark 1. Two sets above can represent the same physical ruler. For example, consider $\{0, 1, 3, 7\}$ and $\{0, 4, 6, 7\}$, where the first one is obtained from the second one by subtracting each entry from the largest number 7. In terms of physical rulers, they are reflections of each other about the midpoint. In both cases, we treat them as representing one ruler. Similarly, $\{0, 1, 3, 7\}$ and $\{4, 5, 7, 11\}$ represents the same physical ruler, as one is the translate of the other.

Definition 1. A set $\{a_1, \dots, a_n\}$ 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 call a **spanning** ruler if for every positive integer $M \le a_n - a_1$, there exists indices $1 \le i < j \le n$ such that $M = a_j - a_i$. A spanning Golomb ruler is called **perfect**.

The ruler described in the first question 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 [2], and to reduce ambiguity in X-ray analysis of crystal structures [3].

Exercise 1. Find another set of integers that represent the ruler $\{0, 2, 3, 5, 11\}$. What about a general ruler $\{a_1, a_2, \dots, a_n\}$?

Exercise 2. Give three examples of Golomb rulers of length 20 and size 6 such that they are not physically the same.

Exercise 3. How many Golomb rulers you gave in the previous exercise are perfect?

It seems that coming up with perfect rulers are 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 4. Verify that the rulers in the theorem are all the physically distinct perfect rulers with at most 4 marks.

Exercise 5. 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 6. Suppose that $\{0, a_2, a_3, a_4 \ldots, a_{n-2}, a_{n-1}, N\}$ is a perfect ruler of length $N \geq 10$. Prove that $n \geq 5$ and either $a_2 = 1$ or $a_{n-1} = N - 1$, but not both.

Exercise 7. Suppose that $\{0, 1, a_3, a_4 \ldots, a_{n-2}, a_{n-1}, N\}$ is a perfect ruler of length $N \geq 10$. Prove that $a_3 = 4$ and $a_{n-1} = N - 2$.

Exercise 8. Suppose that $\{0, 1, 4, a_4 \ldots, a_{n-2}, N-2, N\}$ is a Golomb ruler of length $N \geq 10$. Prove that it cannot be perfect.

Exercise 9. Use the previous exercises to conclude the proof of Theorem 1.

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 close formula for $G(r)$, we could try to bound it from below and above. The naïve lower bound is

$$G(r) \geq \frac{r(r-1)}{2}.$$

With some counting argument, one can show that $G(r) > r^2 - 2r\sqrt{r} + \sqrt{r} - 2$ for any r (see [4, Theorem 4.9]).

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 form a Golomb ruler:

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

Exercise 10. Prove that the sequence above indeed gives a Golomb ruler.

The simple construction above does not give very good upper bound for $G(r)$. When r is large, it only says $G(r) < r^3$, which is not on the same order of magnitude as the lower bound. Here is another more clever construction, which uses the finite field (see appendix). However, it has the drawback that it only works for r being one less than a prime number.

Construction 2 ([6])**.** Let p be a prime number and g a primitive element of the finite field $\mathbb{F}_p$. 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 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 $\mathbb{F}_p$

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

By equations (3), we know that $X = g^m, g^n$ are roots of this polynomial. Furthermore, suppose there is another pair of (m', n') satisfying equation (1) 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 (4). Since a quadratic polynomial over a finite field has only two solutions, we must 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 11. Use the first construction to make a Golomb ruler of size 5.

Exercise 12. Use the second construction to make a Golomb ruler of size 6.

Exercise 13. 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 14. For any positive integer r, let $p(r)$ be the smallest prime greater than r. Prove that $G(r) \leq p(r) \cdot (p(r) - 1)$.

Exercise 15. Use the bounds above to show that $\lim_{r \to \infty} \frac{G(r)}{r^2}$ exists and equals to 1. (Hint: you will need the fact that $\lim_{n \to \infty} \frac{p_{n+1}}{p_n} = 1$ where p_n is the n^{th} prime.)

Appendix A. Finite Field

In the appendix, we will include a short description of finite field, which was used in Ruzsa's construction of Golomb rulers. For a more rigorous introduction, you can check out [5].

A *field* is a set $\mathbb{F}$ such that

(1) It is equipped with an addition and a multiplication operation, both of which are associative and commutative. Also distributivity holds.
(2) $\mathbb{F}$ is closed under the above operations, i.e. sum (or product) of two elements in $\mathbb{F}$ is also in $\mathbb{F}$.
(3) It contains an an additive and a multiplicative identity, denoted by 0 and 1.
(4) Every element has a unique additive inverse.
(5) Every nonzero element has a unique multiplicative inverse.

Some common fields include the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. (However, the integers $\mathbb{Z}$ do not form a field.) In addition to these examples, there are also finite fields, i.e. the set $\mathbb{F}$ is finite. For example, let p be a prime number, $\mathbb{F}_p$ be the set of integers $\{0, 1, \ldots, p-1\}$. Operations are standard addition and multiplication modulo p. Additive (resp. multiplicative) identity is 0 (resp 1). Also, every nonzero element $a \in \mathbb{F}_p$ has a unique inverse. We will use $\mathbb{F}_p^\times$ to denote the nonzero elements of $\mathbb{F}_p$.

Remark 3. All finite fields of size p, where p is a fixed prime number, are isomorphic, i.e. they have the same structure. So it is enough to consider the example $\mathbb{F}_p$ above.

Remark 4. It is a fact from field theory that the size of any finite field must be the power of a prime number. Also, any finite field of size p^n, with p a prime number and n a natural number, is an extension of the finite field $\mathbb{F}_p$, i.e. can be "derived" from $\mathbb{F}_p$ by adding an element.

Given a finite field $\mathbb{F}_p$, the **multiplicative order** of a nonzero element $a \in \mathbb{F}_p^\times$, denoted by $\text{ord}(a)$, is the least positive integer n such that $a^n = 1$. Here a^n denotes $a \cdot a \cdots a$ a total of n times. Fermat's (small) theorem states that $a^{p-1} = 1$ for any $a \in \mathbb{F}_p^\times$. In particular, multiplicative orders have to divide $p - 1$. If $\text{ord}(a) = p - 1$, then a is call a **primitive element** of $\mathbb{F}_p$. In that case, the set $\{a, a^2, a^3, \ldots, a^{p-1}\}$ is exactly $\mathbb{F}_p^\times$.

Since one can solve polynomial equations over fields like $\mathbb{R}$ and $\mathbb{C}$, it is natural to try to solve such equations over finite field $\mathbb{F}_p$. In fact, from the definitions of fields above, one can deduce that a polynomial equation of degree m defined over $\mathbb{F}_p$ can have at most m solutions in $\mathbb{F}_p$. One way to solve such an equation $f(X) = 0$ is to substitute all the elements of $\mathbb{F}_p$ into $f(X)$.

Remark 5. A polynomial equation with coefficient in $\mathbb{F}_p$ need not to have all its zeros in $\mathbb{F}_p$. See exercise below.

Exercise 16. Write out the multiplication table of $\mathbb{F}_5$ and check that every nonzero element has a unique multiplicative inverse.

Exercise 17. Find the order of each element in $\mathbb{F}_7^\times$ and all the primitive elements. How many are there? In general, how many primitive element does $\mathbb{F}_p^\times$ have?

Exercise 18. Solve the polynomial equations below:

(1) $X^2 + 1 = 0$ over $\mathbb{F}_2$.
(2) $X^2 + 9X + 7 = 0$ over $\mathbb{F}_5$.
(3) $X^2 + 9X + 7 = 0$ over $\mathbb{F}_{11}$.
(4) $X^2 + 9X + 7 = 0$ over $\mathbb{F}_{13}$.
(5) *Challenge:* Solve all the problems above using the quadratic formula.
(6) $X^{16} - 1 = 0$ over $\mathbb{F}_{17}$.

Appendix B. Answers

Warm-up questions.

(1) For example $\{0, 1, 3, 7, 8, 10, 12\}, \{0, 2, 4, 6, 8, 11, 12\}, \{0, 1, 4, 5, 7, 10, 12\}$.
(2) For example $\{0, 1, 7, 8, 10, 12\}$.
(3) Since $\{0, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ is not spanning, we need at least 12 marks. This is also sufficient. Since only one mark is missing in this case, we can suppose it is mark m with $1 \leq m \leq 11$. Then $m + 1$ and 1 are both present and can be used to measure a distance of m.
(4) For example $\{0, 1, 7, 10, 12\}$ is a foot-long Golomb ruler with 5 marks. Any ruler with 6 marks can measure $\binom{6}{2} = 15$ distances. If the ruler is one foot long, then there must be a distance which is not measured uniquely by the pigeonhole principle. Thus, there are no foot-long Golomb ruler with 6 marks.
(5) From the previous question, we see that a foot-long Golomb ruler can have at most 5 marks, in which case $\binom{5}{2} = 10$ distances can be measured. But a foot-long spanning ruler can measure 12 different distances. So it is not possible to have a foot-long spanning Golomb ruler.

Exercise 1. The sets $\{0, 2, 3, 5, 11\}, \{0, 6, 8, 9, 11\}$ and $\{4, 6, 7, 9, 15\}$ represent the same ruler.

Exercise 2. For example: $\{0, 1, 3, 7, 12, 20\}, \{0, 1, 3, 7, 15, 20\}, \{0, 2, 6, 7, 10, 19\}$.

Exercise 3. None. The only perfect rulers have lengths less than or equal to 6. They are listed in the later exercises.

Exercise 4. For $\{0, 1, 4, 6\}$, we have $1 = 1-0, 2 = 6-4, 3 = 4-1, 4 = 4-0, 5 = 6-1, 6 = 6-0$. The others can be checked similarly and are indeed all the physically distinct perfect rulers with at most 4 marks.

Exercise 5. A ruler with size n can measure $\binom{n}{2} = \frac{n(n-1)}{2}$ distances. Since a Golomb ruler measures each distance uniquely, its length must be at least $\frac{n(n-1)}{2}$. If it is perfect and has length N, then all the distances $1, 2, \ldots, N$ can be measured distinctly. Thus, $N = \frac{n(n-1)}{2}$.

Exercise 6. Since the ruler is perfect, we have $\frac{n(n-1)}{2} = N$ from the previous exercise. When $N \geq 10$, we must have $n \geq 5$. To measure $N - 1$, we can use exactly one of $a_{n-1} - 0$ and $N - a_2$. Thus, either $a_{n-1} = N - 1$ or $a_2 = 1$, but not both.

Exercise 7. Since $a_2 = 1$, we must have $a_{n-1} \leq N - 2, a_{n-2} \leq N - 3$ and $a_3 \geq 3$. In order to measure $N - 2$, we could only use a_{n-1} and 0, which implies that $a_{n-1} = N - 2$. That also means $a_3 \geq 4$ and $a_{n-2} \leq N - 5$, otherwise $2 = N - a_{n-1} = a_3 - 1$ or $2 = N - a_{n-1} = a_{n-1} - a_{n-2}$. Thus, to measure $N - 4$, we could only use N and a_3, meaning $a_3 = 4$.

Exercise 8. If $N = 10$, then $n = 5$ by exercise 5 and the ruler $\{0, 1, 4, 8, 10\}$ is not spanning since it cannot measure 5. Suppose $N \geq 11$, then $n \geq 6$ and $N \geq 15$. Since this is a Golomb ruler, we need $a_{n-2} \leq N - 6$. However, the distance $N - 5$ cannot be measured. Thus, this ruler cannot be perfect.

Exercise 9. Given a perfect ruler $\{a_1, \ldots, a_n\}$, let N be its length. As seen in exercise 5, the length N is also $\frac{n(n-1)}{2}$. Suppose $n \geq 5$, i.e. $N \geq 10$. By exercise 5, either $a_2 = 1$ or $a_{n-1} = N - 1$, but not both. By replacing the ruler with the physically equivalent ruler $\{N - a_n, N - a_{n-1}, \ldots, N - a_1\}$, we can suppose that $a_1 = 1$. Then exercises 6 and 7 implies that $a_3 = 4, a_{n-1} = N - 2$. Finally, exercise 8 shows that the ruler cannot be perfect, which means $n \geq 4$. This finishes the proof, as we have listed all physically distinct perfect rulers in exercise 4 for $n \leq 4$.

Exercise 10. Suppose there exists $1 \leq m < n \leq r$ and $1 \leq m' < n' \leq r$ such that $a_n - a_m = a_{n'} - a_{m'}$. This is equivalent to

$$(n - m)(rn + rm - 2r - 1) = (n' - m')(rn' + rm' - 2r - 1).$$

When modulo both sides by r, we obtain $n - m \equiv n' - m' \bmod r$. Since m, n, m', n' are all between 1 and r, so is the difference and we must have $n - m = n' - m'$, which implies that

$$rn + rm - 2r - 1 = rn' + rm' - 2r - 1.$$

This is equivalent to $n + m = n' + m'$. Together with $n - m = n' - m'$, we must then have $n = n', m - m'$.

Exercise 11. For $r = 5$, the ruler is $\{0, 4, 18, 42, 76\}$.

Exercise 12. For $p = 7, g = 2$, we have $\{6, 17, 19, 27, 38, 40\}$.

Exercise 13. There are 2 optimal Golomb rulers of size 5: $\{0, 1, 4, 9, 11\}, \{0, 2, 7, 8, 11\}$, and 4 optimal Golomb rulers of size 6:

$$\{0, 1, 4, 10, 12, 17\}, \{0, 1, 4, 10, 15, 17\}, \{0, 1, 8, 11, 13, 17\}, \{0, 1, 8, 12, 14, 17\}.$$

They are all physically distinct.

Exercise 14. If $r \leq r'$, then $G(r) \leq G(r')$ since any subset of a Golomb ruler is still a Golomb ruler. Then for any positive integer r, we have $G(r) \leq G(p(r) - 1) \leq p(r)(p(r) - 1)$.

Exercise 15. For the lower bound, we use have $1 - 2/\sqrt{r} < G(r)/r^2$ for $r \geq 4$. For the upper bound, we have $G(r) \leq p(r)^2/r^2$. As $r \to \infty$, the lower bound goes to 1. Let $q(r)$ be the greatest prime less than or equal to r. Then

$$\frac{q(r)}{p(r)} \leq \frac{r}{p(r)} \leq 1.$$

Since $q(r)$ and $p(r)$ are consecutive primes, this ratio goes to 1 as r goes to infinity. Thus, the upper bound also goes to 1 and $\lim_{r\to\infty} \frac{G(r)}{r^2} = 1$.

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), 259282.

E-mail address: `li@mathematik.tu-darmstadt.de`