Contributions to Discrete Mathematics

Volume 4, Number 1, Pages 107–111
ISSN 1715-0868

RESULTS ON PERMUTATIONS WITH A DISTINCT DIFFERENCE PROPERTY

JORDAN BELL AND QIANG WANG

Abstract. We prove that for all odd primes p and positive integers $\alpha \geq 2$, a construction of Batten and Sane yields at least $(p-1)^3/4$ permutations with a distinct difference property (DDP) of $\{1, 2, \ldots, p^\alpha - 1\}$. This proves a conjecture of Batten and Sane, that at least $(p-1)^2/2$ such permutations exist. We also pose several research questions for DDP permutations.

1. Introduction

A permutation $a_1, a_2, \ldots, a_n$ of $\{1, 2, \ldots, n\}$ is said to have the *distinct difference property* (DDP) if $a_{i+1} - a_i = a_{j+1} - a_j$ implies that $i = j$. That is, all the differences between consecutive elements are distinct. For example, $1, 3, 2$ is a DDP permutation (since the differences $3 - 1 = 2$ and $2 - 3 = -1$ are distinct) whereas $1, 2, 3$ is not (since the differences $2-1 = 1$ and $3-2 = 1$ are equal). DDP permutations are weaker variants of Costas arrays, which have applications in signal processing for radar and sonar systems [4], [5, §5.2].

Batten and Sane [1, Corollary 2.1] show that for all $n \geq 1$ there exist at least 2^{n-1} DDP permutations of $\{1, \ldots, n\}$. They then consider a particular class of DDP permutations, which they construct using "modular" DDP sequences, which we explain now. They make a conjecture about the number of DDP permutations of this class, which we prove in this paper.

For p an odd prime and α a positive integer, Batten and Sane [1, Theorem 2.3] give the following construction for DDP permutations of $\{1, 2, \ldots, p^\alpha - 1\}$. It is well known that if an integer g is a primitive root of an odd prime p, then either g or $g+p$ is a primitive root of all powers of p [6, §4.1]. Therefore, we can choose g as a primitive root of p such that g is also a primitive root of $p^2, \ldots, p^\alpha$. Then, for any $1 \leq k \leq \alpha$, we define

$$\pi_k = g \bmod p^k, g^2 \bmod p^k, \ldots, g^{p^k - p^{k-1} - 1} \bmod p^k, 1 \tag{1.1}$$

Received by the editors February 14, 2008, and in revised form March 31, 2009.

2000 *Mathematics Subject Classification.* Primary: 05A05, 05B15, Secondary: 94A12.

Key words and phrases. Distinct difference property, DDP, permutations, Costas arrays.

Research of both authors is partially supported by NSERC.

and

$$\Pi_k = p^{\alpha-k}(g \bmod p^k), p^{\alpha-k}(g^2 \bmod p^k), \dots, p^{\alpha-k}(g^{p^k-p^{k-1}-1} \bmod p^k), p^{\alpha-k}; \tag{1.2}$$

here $a \bmod b$ is the remainder when a is divided by b. Batten and Sane [1, Theorem 2.3] prove that for each element i of Π_1, we can cyclically shift Π_1 so i is at the left, and then attach this to some cyclic shift of Π_2 such that $\Pi_2\Pi_1$ is a DDP permutation, and that there is then a cyclic shift of Π_3 to which we can attach $\Pi_2\Pi_1$ such that $\Pi_3\Pi_2\Pi_1$ is a DDP permutation, etc. Therefore their construction yields at least $(p-1)$ DDP permutations for all odd primes p and positive integers α.

Batten and Sane [1, Conjecture 4.2] conjecture that for p an odd prime and α a positive integer, this construction yields at least $(p-1)^2/2$ DDP permutations of $\{1, 2, \dots, p^\alpha - 1\}$. In this paper we prove that their construction [1, Theorem 2.3] yields at least $(p-1)^3/4$ DDP permutations of $\{1, 2, \dots, p^\alpha - 1\}$ for any odd prime p and positive integer $\alpha \geq 2$, thus proving their conjecture, since $(p-1)^3/4 \geq (p-1)^2/2$ for all primes $p \geq 3$.

2. Results

We shall prove a lower bound on the number of DDP permutations given by Batten and Sane's construction that implies their conjecture. First of all, we describe explicitly sequences π_1, π_2, Π_1 and Π_2. Since p is a prime and g is a primitive root of p, the sequence π_1 contains all integers $1, 2, \dots, p-1$; therefore, Π_1 contains these same integers multiplied by a factor $p^{\alpha-1}$. Similarly, since p is a prime and g is also a primitive root of p^2, the sequence π_2 contains all integers of $\{1, 2, \dots, p^2-1\}$, except those that are multiples of p; therefore, Π_2 contains all integers of $\{p^{\alpha-2}, 2p^{\alpha-2}, 3p^{\alpha-2}, \dots, (p^2-1)p^{\alpha-2}\}$, except those that are multiples of $p^{\alpha-1}$, that is, except those integers in Π_1.

Theorem 2.1. *For all odd primes p and positive integers $\alpha \geq 2$, there are at least $(p-1)^3/4$ DDP permutations given by Batten and Sane's construction.*

Proof. It is clear that half the elements in π_1 are less than $p/2$, and half are greater than $p/2$. Let δ be the number of positive differences between consecutive elements (the last element and the first element are also considered as consecutive elements) in Π_2; thus $p(p-1) - \delta$ is the number of negative differences between consecutive elements in Π_2.

For $i \in \pi_1$, if $i > p/2$ then most of the differences of $p^{\alpha-1}i \in \Pi_1$ with elements in Π_2 will be positive; indeed, $\frac{i}{p}p(p-1) = i(p-1)$ of the differences between $p^{\alpha-1}i$ and elements in Π_2 will be positive. Since there are δ positive differences between consecutive elements in Π_2 and all differences between consecutive elements in Π_1 are multiples of $p^{\alpha-1}$, there will be at least $i(p-1) - \delta$ positions in Π_2 at which we can attach i.

Similarly, if $i < p/2$ then most of the differences with i and elements in Π_2 will be negative; indeed, $(1 - \frac{i}{p})p(p-1)$ of the differences between i

and elements in Π_2 will be negative. Since there are $p(p-1)-\delta$ negative differences between consecutive elements in Π_2, there will be at least

$$\left(1-\frac{i}{p}\right)p(p-1)-p(p-1)+\delta=\delta-i(p-1)$$

positions in Π_2 at which we can attach i.

Thus there are at least N ways to attach Π_1 to Π_2, where N is given by

$$\begin{aligned}
N &= \sum_{i=(p+1)/2}^{p-1}\left(i(p-1)-\delta\right)+\sum_{i=1}^{(p-1)/2}\left(\delta-i(p-1)\right)\\
&= (p-1)\sum_{i=(p+1)/2}^{p-1} i-(p-1)\sum_{i=1}^{(p-1)/2} i\\
&= \frac{(p-1)(p-1)p}{2}-\frac{(p-1)(p-1)(p+1)}{8}-\frac{(p-1)(p-1)(p+1)}{8}\\
&= \frac{2(p^2-2p+1)p}{4}-\frac{(p-1)(p^2-1)}{4}\\
&= \frac{p^3-3p^2+3p-1}{4}\\
&= \frac{(p-1)^3}{4},
\end{aligned}$$

proving the claim. □

Since for all $p\geq 3$, one has $(p-1)^3/4\geq(p-1)^2/2$, Theorem 2.1 implies the conjecture of Batten and Sane. Moreover, since each of the $\phi(p-1)$ distinct primitive roots of p can be used in the Batten and Sane construction, we can multiply any lower bound we get by $\phi(p-1)$, where ϕ is the Euler phi function. Thus there are at least $\frac{(p-1)^3}{4}\cdot\phi(p-1)$ DDP permutations of the form of the Batten and Sane construction.

For example, take $p=5$ and $\alpha=2$. We find that $g=3$ is a primitive root of 5 that is also a primitive root of 25. Then for this choice of primitive root g, $\Pi_1=15, 20, 10, 5$ and $\Pi_2=3, 9, 2, 6, 18, 4, 12, 11, 8, 24, 22, 16, 23, 19, 7, 21, 13, 14, 17, 1$.

We observe that $\delta=10$. Now, $3\in\pi_1$ and $3>p/5=5/2$. By Theorem 2.1, there are at least $3\cdot 4-10=2$ elements in Π_2 at which we can attach Π_1. In fact, there are precisely 4 elements in Π_2 at which we can attach Π_1, namely $2, 6, 4, 24$; see Table 1. Similarly, there are precisely 6 elements in Π_2 at which we can attach the cyclic shift $20, 10, 5, 15$ of Π_1. For the cyclic shifts $10, 5, 15, 20$ and $5, 15, 20, 10$ of Π_1, we have precisely 4 and 6 ways each to attach them to Π_2. By the previous theorem there are at least $(p-1)^3/4=16$ such DDP permutations of $\{1, 2, \ldots, 24\}$, and in fact there are precisely 20, which we give in Table 1.

3. Conclusions

In this paper we have proved that for all odd primes p and positive integers $\alpha \geq 2$, Batten and Sane's construction yields at least $(p-1)^3/4$ DDP permutations of $\{1, 2, \ldots, p^\alpha - 1\}$, which proves the conjecture [1, Conjecture 4.2]. As we remarked in Section 1, DDP permutations are a weaker version of Costas arrays; Costas arrays are difficult to study, and studying weaker structures like DDP permutations may help us understand Costas arrays better and to find new results about them. We now pose several open problems for DDP permutations.

It would be desirable to find more constructions of DDP permutations. Let $\mathbb{Z}/n$ be the ring of residue classes modulo n. A polynomial $f(x)$ over $\mathbb{Z}/n$ is said to be a permutation polynomial if the evaluation mapping $t \mapsto f(t)$ is a bijection. It would be extremely interesting to find classes of permutation polynomials of $\mathbb{Z}/n$ that yield DDP permutations of $\{1, 2, \ldots, n\}$ when lifted to the integers $\mathbb{Z}$.

It is interesting to ask when a DDP permutation has other properties. An n-queens solution is a permutation $a_1, a_2, \ldots, a_n$ of $\{1, 2, \ldots, n\}$ such that $a_i + i = a_j + j$ implies $i = j$ and $a_i - i = a_j - j$ implies $i = j$ [2]. We ask if there exist DDP permutations which are also n-queens solutions. This is a

Table 1: 20 DDP permutations made by modular construction, $p = 5, \alpha = 2, g = 3$

6,18,4,12,11,8,24,22,16,23,19,7,21,13,14,17,1,3,9,2,15,20,10,5
18,4,12,11,8,24,22,16,23,19,7,21,13,14,17,1,3,9,2,6,15,20,10,5
12,11,8,24,22,16,23,19,7,21,13,14,17,1,3,9,2,6,18,4,15,20,10,5
22,16,23,19,7,21,13,14,17,1,3,9,2,6,18,4,12,11,8,24,15,20,10,5
9,2,6,18,4,12,11,8,24,22,16,23,19,7,21,13,14,17,1,3,20,10,5,15
2,6,18,4,12,11,8,24,22,16,23,19,7,21,13,14,17,1,3,9,20,10,5,15
6,18,4,12,11,8,24,22,16,23,19,7,21,13,14,17,1,3,9,2,20,10,5,15
8,24,22,16,23,19,7,21,13,14,17,1,3,9,2,6,18,4,12,11,20,10,1,15
21,13,14,17,1,3,9,2,6,18,4,12,11,8,24,22,16,23,19,7,20,10,5,15
3,9,2,6,18,4,12,11,8,24,22,16,23,19,7,21,13,14,17,1,20,10,5,15
19,7,21,13,14,17,1,3,9,2,6,18,4,12,11,8,24,22,16,23,10,5,15,20
7,21,13,14,17,1,3,9,2,6,18,4,12,11,8,24,22,16,23,19,10,5,15,20
13,14,17,1,3,9,2,6,18,4,12,11,8,24,22,16,23,19,7,21,10,5,15,20
3,9,2,6,18,4,12,11,8,24,22,16,23,19,7,21,13,14,17,1,10,5,15,20
4,12,11,8,24,22,16,23,19,7,21,13,14,17,1,3,9,2,6,18,5,15,20,10
22,16,23,19,7,21,13,14,17,1,3,9,2,6,18,4,12,11,8,24,5,15,20,10
16,23,19,7,21,13,14,17,1,3,9,2,6,18,4,12,11,8,24,22,5,15,20,10
23,19,7,21,13,14,17,1,3,9,2,6,18,4,12,11,8,24,22,16,5,15,20,10
19,7,21,13,14,17,1,3,9,2,6,18,4,12,11,8,24,22,16,23,5,15,20,10
17,1,3,9,2,6,18,4,12,11,8,24,22,16,23,19,7,21,13,14,5,15,20,10

weaker version of the question of Golomb and Taylor [4, §V, Question 10], whether there are Costas arrays which are also n-queens solutions. Golomb and Taylor's question is unsolved; however, an important construction for (modular) n-queens solutions is by cyclotomic permutations (permutations defined by membership in cyclotomic cosets), and the authors show [3] that circular Costas arrays of size $(p-1)\times(p-1)$ must be generated by cyclotomic permutations of $\mathbb{Z}/p$ with index greater than a certain lower bound, and with a certain parity.

References

1. Lynn M. Batten and Sharad Sane, *Permutations with a distinct difference property*, Discrete Math. **261** (2003), no. 1-3, 59–67.
2. Jordan Bell and Brett Stevens, *A survey of known results and research areas for n-queens*, Discrete Math. **309** (2009), no. 1, 1–31.
3. Jordan Bell and Qiang Wang, *A note on Costas arrays and cyclotomic permutations*, Ars Combin. (to appear).
4. Solomon W. Golomb and Herbert Taylor, *Constructions and properties of Costas arrays*, Proc. IEEE **72** (1984), no. 9, 1143–1163.
5. Nadav Levanon and Eli Mozeson, *Radar signals*, John Wiley & Sons, 2004.
6. William J. LeVeque, *Fundamentals of number theory*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1977.
7. Oscar Moreno, *Survey on Costas arrays and their generalizations*, Mathematical properties of sequences and other combinatorial structures (Los Angeles, CA, 2002), Kluwer Acad. Publ., Boston, MA, 2003, pp. 55–64.

Department of Mathematics, University of Toronto,
Toronto ON, M5S 2E4, Canada
E-mail address: jordan.bell@utoronto.ca

School of Mathematics and Statistics, Carleton University,
Ottawa ON, K1S 5B6, Canada
E-mail address: wang@math.carleton.ca