S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 10, стр. 562–565 (2013) УДК 519.147, 512.541
MSC 05B45

TILINGS OF P-ARY CYCLIC GROUPS

D.K. ZHUKOV

Abstract. A tiling of a finite abelian group G is a pair (T, A) of subsets of G such that every element $g \in G$ can be uniquely represented as $t + a$ with $t \in T$, $a \in A$. In this paper we consider tilings of groups $\mathbb{Z}_{p^n}$ (p is prime) and give a description of a recurrent scheme embracing all tilings of such groups. Furthermore we count their number.

Keywords: tiling, finite abelian group, set's kernel, factor group.

1. Introduction

Definition 1. *Let G be a finite abelian group, $A, T \subseteq G$. A pair (T, A) forms a* tiling *of G if every $g \in G$ can be uniquely written as $g = t + a$ with $t \in T$, $a \in A$.*

The most trivial examples of tilings are provided by a group's covering with one of its subgroup's cosets. This concept also includes several well-known combinatorial structures such as the perfect codes and the MDS-codes. For instance, any q-ary perfect code can be considered as $\mathbb{Z}_q^n$ tiling with balls (in Hamming metric).

Initial studies of tilings using coding theory's approach took place in groups $\mathbb{Z}_2^n$ [1, 2]. As was shown in [1] every tiling of $\mathbb{Z}_2^n$ could be reduced to a so-called *full rank tiling* . This decomposition method was then generalized to the case of arbitrary finite abelian groups [3]. Full rank tilings in their turn admit reduction to *non-periodic full rank tilings* , which play a similar role in the problem of tilings desciption as simple groups in the finite group description problem. In this paper we consider tilings of $\mathbb{Z}_{p^n}$ (p is prime) and show that in this case every tiling can be reduced to another one in a group of smaller order.

Definition 2. *The* kernel *of a subset $A \subseteq G$ is the set* $\ker A = \{g \in G \mid g + A = A\}$.

Zhukov, D.K., Tilings of p-ary cyclic groups.

The work was supported by the Russian Foundation for Basic Research (grant 13-01-00463).
Received July, 2, 2013, published September, 14, 2013.

It is not hard to see that $\ker A \leq G$. Furthermore if $0 \in A$ then $\ker A \subseteq A$ and $A = A' + \ker A = \{a + g \mid a \in A', g \in \ker A\}$ for some A' $(0 \in A')$.

We will need few simple propositions (proofs are given in [3]).

Proposition 1. *(T, A) is a tiling of a finite abelian group G if and only if $|T| \cdot |A| = |G|$ and $(T - T) \cap (A - A) = \{0\}$.*

Proposition 2. *Let (T, A) be a tiling of a finite abelian group G and let $\varphi : G \to G/\ker A$ be a canonical homomorphism . Then $(\varphi(T), \varphi(A))$ is a tiling of $G/\ker A$ and $\ker \varphi(A) = \{0\}$.*

2. Reduction of tilings

The following proposition is a special case of Theorem 4.4 from [4]. We give a new simple proof of this fact which doesn't require any knowledge of the general theory of tilings.

Theorem 1. *If (T, A) is a tiling of $\mathbb{Z}_{p^n}$ then either $\ker T \neq \{0\}$ or $\ker A \neq \{0\}$.*

Proof. Let $T = \{t_1, t_2, ..., t_s\}, A = \{a_1, a_2, ..., a_l\}$. Denote

$$\psi_T(z) = z^{t_1} + z^{t_2} + ... + z^{t_s}$$

$$\psi_A(z) = z^{a_1} + z^{a_2} + ... + z^{a_l}$$

Let $\xi = e^{\frac{2\pi i}{p^n}}$. Since (T, A) is a tiling, we have

$$\psi_T(\xi) \cdot \psi_A(\xi) = \sum_{j,k} \xi^{t_j + a_k} = \sum_{m=0}^{p^n - 1} \xi^m = 0 \tag{1}$$

It follows that either $\psi_T(\xi) = 0$ or $\psi_A(\xi) = 0$.

Assume that $\psi_T(\xi) = 0$. Then the minimal polynomial for ξ over the field of rational numbers divides $\psi_T(z)$. It is known (see e.g. [5] , chapter 13) that if ξ is a root of $z^{p^n} - 1$ then $1 + z^{p^{n-1}} + z^{2p^{n-1}} + \ldots + z^{(p-1)p^{n-1}}$ is the minimal polynomial for ξ and hence

$$\psi_T(z) = (1 + z^{p^{n-1}} + z^{2p^{n-1}} + \ldots + z^{(p-1)p^{n-1}}) \cdot (\alpha_1 z^{t'_1} + \alpha_2 z^{t'_2} + \ldots + \alpha_r z^{t'_r}) =$$
$$= \sum_{j,l} \alpha_j z^{t'_j + l \cdot p^{n-1}} = \sum_k z^{t_k}$$

Now, for all j we have $t'_j + (p - 1)p^{n-1} < p^n$, so $t'_j < p^{n-1}$ and all powers in $\sum_{j,l} \alpha_j z^{t'_j + l \cdot p^{n-1}}$ are different. Consequently, for every j we have $\alpha_j = 1$ and for every k there exist j and l such that $t_k = t'_j + l \cdot p^{n-1}$. Hence, $\ker T \geq \langle p^{n-1} \rangle$. This completes the proof of Theorem 1.

Since every factor group of $\mathbb{Z}_{p^n}$ is isomorphic to some group $\mathbb{Z}_{p^m}$ of similar form, it follows from Proposition 2 and Theorem 1 that every tiling (T_n, A_n) of group $\mathbb{Z}_{p^n}$ can be reduced to a certain tiling (T_m, A_m) of group $\mathbb{Z}_{p^m}$ for some $m < n$. Moreover, either one of T_m, A_m has a nontrivial kernel or $T_m = A_m = \{0\}$. A factorization by a kernel itself is unnecessary: since every proper subgroup of $\mathbb{Z}_{p^n}$ contains the minimal proper subgroup $\langle p^{n-1} \rangle$, we may factorize by $\langle p^{n-1} \rangle$ at every step obtaining a tiling (T_{n-1}, A_{n-1}) of $\mathbb{Z}_{p^{n-1}}$. Note that only one of components can have the nonzero kernel. Indeed, by the definition of tiling 0 can be represented as $x - x$ where $x \in T \cap A$. If both $\ker T$ and $\ker A$ are nonzero (it means that $p^{n-1} \in \ker T \cap \ker A$) then we have $x + p^{n-1} \in T \cap A$ and there is another representation $0 = (x + p^{n-1}) - (x + p^{n-1})$ which contradicts to the definition of tiling.

Proposition 3. *Let* (T_n, A_n) *be a tiling of* $\mathbb{Z}_{p^n}$*, and let* $\ker T_n \neq \{0\}$*. If* (T_{n-1}, A_{n-1}) *is obtained from* (T_n, A_n) *using factorization by* $\langle p^{n-1}\rangle$ *then*

$$(2) \qquad T_n = T_{n-1} + \langle p^{n-1}\rangle, \qquad A_n = \{a + f(a)\cdot p^{n-1} \mid a \in A_{n-1}\}$$

for some function $f_n\colon A_{n-1} \to \{0, 1, ..., p-1\}$

Any choise of the tiling (T_{n-1}, A_{n-1}) *of* $\mathbb{Z}_{p^{n-1}}$ *and the function* $f_n\colon A_{n-1} \to \{0, 1, \ldots, p-1\}$ *provides a tiling* (T_n, A_n) *of* $\mathbb{Z}_{p^n}$ *defined by (2).*

Proof. The canonical homomorphism $\varphi\colon \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^{n-1}}$ relates a value $x \bmod p^{n-1}$ to every $x \in \mathbb{Z}_{p^n}$. Consider $x \in T_n$. If $x < p^{n-1}$ then $\varphi(x) = x \in T_{n-1}$. In case of $x \geq p^{n-1}$, using the condition $\ker T_n \geq \langle p^{n-1}\rangle$, we get $y = x - k\cdot p^{n-1} \in T_n$ for every integer k. We may choose such k that $y < p^{n-1}$. Then, as it was shown above, $\varphi(y) = y \in T_{n-1}$. So, for every $x \in T_n$ $x = y + k\cdot p^{n-1}$ for some $y \in T_{n-1}$. This leads to the first equation in (2). Now we are going to show that φ acts injectively on A_n. Consider $a_1, a_2 \in A_{n-1}$ such that $\varphi(a_1) = \varphi(a_2) = a \in A_{n-1}$. By the definition of φ, we have $a_1 - a_2 \in \langle p^{n-1}\rangle$. And using the fact that $\langle p^{n-1}\rangle \leq \ker T_n \subseteq T_n - T_n$, we obtain $a_1 - a_2 \in (A_n - A_n) \cap (T_n - T_n)$. By Proposition 1 we conclude that $a_1 = a_2$. This means that for every element $a \in A_{n-1}$ there exists a unique $a' \in A_n$ such that $a' = a + k\cdot p^{n-1}$ for some integer $k = f(a)$. The first statement of the proposition is proved.

Now consider a tiling (T_{n-1}, A_{n-1}) of $\mathbb{Z}_{p^n}$ and a function $f_n\colon A_{n-1} \to \{0, 1, \ldots, p-1\}$. We will show that a pair (T_n, A_n) of $\mathbb{Z}_{p^n}$ subsets defined by (2) forms a tiling of $\mathbb{Z}_{p^n}$. It's easy to see that $|T_n| = p\cdot|T_{n-1}|$ and $|A_n| = |A_{n-1}|$. Since (T_{n-1}, A_{n-1}) is a tiling of Z_{p^n}, by Proposition 1 we have $|T_{n-1}|\cdot|A_{n-1}| = p^{n-1}$ and so $|T_n|\cdot|A_n| = p^n$. Consider $x \in (A_n - A_n) \cap (T_n - T_n)$. By the definition of T_n and A_n (2), there exist $a_1, a_2 \in A_{n-1}$ $(a_1 \leq a_2)$, $t_1, t_2 \in T_{n-1}$ $(t_1 \leq t_2)$ and integers $k, l < p$ such that $x = a_2 - a_1 + k\cdot p^{n-1} = t_2 - t_1 + l\cdot p^{n-1}$. Note that $a_2 - a_1 < p^{n-1}, t_2 - t_1 < p^{n-1}$; so, the last equality means that $a_2 - a_1 = t_2 - t_1$ and $k = l$. Since $(A_{n-1} - A_{n-1}) \cap (T_{n-1} - T_{n-1}) = \{0\}$, we have $x = 0$. Finally, using Proposition 1 again, we conclude that (T_n, A_n) is a tiling of $\mathbb{Z}_p^n$.

3. Construction of tilings

Considerations given in the previous paragraph lead to the following scheme.

1. Fix a boolean vector $\delta \in \{0,1\}^n$. Denote

$$\Delta_k = |\{j \in \{1, ..., k\} \mid \delta_j \neq \delta_k\}|$$

2. Fix a set of functions $f_k\colon \{1, 2, ..., p^{\Delta_k}\} \to \{0, 1, ..., p-1\}$, $k = 1, \ldots, n$.

3. Let $A_0 = T_0 = \{0\}$. If $\delta_k = 0$ then

$$T_k = T_{k-1} + \{0, p^{k-1}, 2\cdot p^{k-1}, \ldots, (p-1)\cdot p^{k-1}\}$$

$$A_k = \{a_j + f_k(j)\cdot p^{k-1} \mid a_j \in A_{k-1}\}$$

Otherwise

$$A_k = A_{k-1} + \{0, p^{k-1}, 2\cdot p^{k-1}, \ldots, (p-1)\cdot p^{k-1}\}$$

$$T_k = \{t_j + f_k(j)\cdot p^{k-1} \mid t_j \in T_{k-1}\}$$

Proposition 4. *Every tiling of* $\mathbb{Z}_{p^n}$ *can be obtained according to this scheme with the unique choice of* δ *and* $f_1, \ldots, f_n$*.*

Proof. By Theorem 1, every tiling of $\mathbb{Z}_{p^n}$ has a component with nonzero kernel and therefore is reducible. Using the reduction described above we may decrease group order until we get the trivial tiling. As mentioned above, only one of tiling's components has nontrivial kernel; so (T_{k-1}, A_{k-1}) is uniquely determined by (T_k, A_k). It is clear that on every step (T_k, A_k) can be obtained from (T_{k-1}, A_{k-1}) with only one choice of δ_k and f_k . These arguments provide the uniqueness of (T_n, A_n) constuction.

4. Number of different tilings of $\mathbb{Z}_{p^n}$

Theorem 2. *The number of different tilings of $\mathbb{Z}_{p^n}$ is*

$$\sum_{\delta \in B^n} p^{\sum_{k=1}^n p^{\Delta_k}} \tag{3}$$

Proof. Fix $\delta \in B^n$. If $\delta_k = 0$ then $|T_k| = p \cdot |T_{k-1}|$, $|A_k| = |A_{k-1}|$. If $\delta_k = 1$ $|A_k| = p \cdot |A_{k-1}|$, $|T_k| = |T_{k-1}|$. It follows $|T_k| = p^{\sum_{j \le k} \overline{\delta_j}}$, $|A_k| = p^{\sum_{j \le k} \delta_j}$. Let $\delta_k = 0$. Then there are $p^{|A_{k-1}|} = p^{p^{\sum_{j \le k} \delta_j}}$ ways to chose f_k i.e. to build some (T_k, A_k) from (T_{k-1}, A_{k-1}). If $\delta_k = 1$, we have $p^{|T_{k-1}|} = p^{p^{\sum_{j \le k} \overline{\delta_j}}}$ ways. In general there are $p^{p^{\sum_{j \le k} (\overline{\delta_k} \delta_j + \delta_k \overline{\delta_j})}} = p^{p^{\Delta_k}}$ of ways to construct (T_k, A_k) from (T_{k-1}, A_{k-1}). This implies that for a fixed δ there is

$$\prod_{k=1}^{n} p^{p^{\Delta_k}} = p^{\sum_{k=1}^n p^{\Delta_k}}$$

tilings of $\mathbb{Z}_{p^n}$. Summing these values over all δ, we obtain the number of tilings of $\mathbb{Z}_{p^n}$.

5. Acknowledgments

The author would like to thank his scientific adviser V.N. Potapov and the Department of Theoretical Cybernetics of Sobolev Institute of Mathematics for valuable comments and support.

References

[1] G. Cohen, S. Litsyn, A. Vardy, and G. Zemor, *Tilings of binary spaces*, SIAM J. Discrete Math., 9 (1996), 393–412. MR1402187

[2] T. Etzion, A. Vardy, *On perfect codes and tilings: problems and solutions*, SIAM J. Discrete Math., 11 (1998), 205–223. MR1617153

[3] M. Dinitz, *Full rank tilings of finite abelian groups*, SIAM J. Discrete Math., 20 (2006), 160–170. MR2257253

[4] Sandor Szabo, Arthur D. Sands, *Factoring groups into subsets*, Taylor & Francis Group, 2009. MR2484422

[5] Kenneth Ireland, Michael Rosen, *A classical Introduction To Modern Number Theory*, Springer-Verlag New York Inc., 1982. MR0661047

Dmitry Konstantinovich Zhukov
Sobolev Institute of Mathematics,
prosp. Koptyuga 4,
630090, Novosibirsk, Russia
E-mail address: zhukov-dmconst@mail.ru