Diskrete Mathematik II
Tibor Szabó

WS 2012 / 2013

Solutions to Exercise Sheet 7

Exercise 1$^+$ (Constructive proof of Baranyai's Theorem):

Suppose $n \geq 1$. Baranayai's Theorem guarantees that $\binom{[3n]}{3}$ has a decomposition into perfect matchings, without explicitly describing the matchings. The purpose of this exercise is to find a construction of the decomposition in the case $p := 3n - 1 \geq 3$ is a prime number.

(i). Consider the field $\mathbb{F}_p$ and denote by $\mathbb{F}_p^*$ the invertible elements, i.e. the set $\{1, 2, \ldots, p-1\}$. Define $\pi : \mathbb{F}_p^* \to \mathbb{F}_p$ by $\pi(x) = -\frac{1+x}{x}$. Show that π is injective and $\pi^3(x) = x$, for any $x \neq p-1$.

(ii). Add an element u to $\mathbb{F}_p$ and extend π to $\{u, 0\}$ injectively in such a way that $\pi^3(x) = x$, for any $x \in \mathbb{F}_p \cup \{u\}$. Explain how this gives a perfect matching M_0 in $\binom{[3n]}{3}$. Using algebraic operations on M_0 find the remainining $\binom{3n-1}{2} - 1$ perfect matchings from Baranyai's theorem and prove that this is indeed a decomposition into disjoint perfect matchings.

Solution:

The construction presented in this exercise is due to Thomas Beth. There are no known constructions for $k \geq 4$ and to the best of my knowledge this is the only construction known for $k = 3$.

(i). Clearly π is well defined. Now if $\pi(x) = \pi(y)$ then $y + xy = x + xy$ and hence $x = y$. So π is injective. Furtermore, for $x \neq p-1$ we have

$$\begin{aligned}
\pi(x) &= -\frac{1+x}{x}, \\
\pi^2(x) &= -\frac{1+\pi(x)}{\pi(x)} = -\frac{1}{x+1}, \\
\pi^3(x) &= -\frac{1+\pi^2(x)}{\pi^2(x)} = x,
\end{aligned}$$

and the two values $\pi(x), \pi^2(x)$ are well-defined. We further have $\pi(p-1) = 0$.

(ii). We define $\pi(0) = u$ and $\pi(u) = p-1$.

For $x \neq 0$, the identity $\pi(x) = x$ implies $x^2 + x + 1 = 0$, from which we obtain $x^3 = 1$. But $p \geq 5$ so $x \neq 1$. Then the order of x in $\mathbb{F}_p^*$ is 3 and hence by Lagrange's theorem, $3 | p - 1 = 3n - 2$, which is not possible. Also $\pi^2(x) = x$ implies $x^2 + x + 1 = 0$, so we get $\pi(x), \pi^2(x) \neq x$.

Hence π has all orbits of size 3, and thus defines a perfect matching M_0 on vertex set $\mathbb{F}_p \cup \{u\} \simeq [3n]$, with edges represented by the orbits.

We will now define two actions on the 3-element subsets of $\mathbb{F}_p \cup \{u\}$.

If $a \in \mathbb{F}_p^*$ and $e \subseteq \mathbb{F}_p \cup \{u\}$ is any 3-set containing points x_1, x_2, x_3, we define $a \cdot e$ as the set $\{ax_1, ax_2, ax_3\}$. This is well-defined, provided we assume $au = u$. We furthermore define $a \cdot M_0$ as the collection $\{a \cdot e : e \in M_0\}$. Then $a \cdot M_0$ is also a perfect matching.

If $a \in \mathbb{F}_p$ and $e \subseteq \mathbb{F}_p \cup \{u\}$ is any 3-set containing points x_1, x_2, x_3, we define $a + e$ as the set $\{a + x_1, a + x_2, a + x_3\}$. This is well-defined, provided we assume $a + u = u$. Then if M is any perfect matching, $a + M$ is also a perfect matching.

Now the group $\mathbb{F}_p^*$ is cyclic. Fix a generator v and consider the sets $M_{i,j} := \{v^i \cdot M_0 + j : 0 \leq i < \frac{p-1}{2}, 0 \leq j \leq p-1\}$. Then by the above $M_{i,j}$ are all perfect matchings in $\mathbb{F}_p \cup \{u\}$ and there are $\frac{p(p-1)}{2} = \binom{3n-1}{2}$ of them. To prove Baranyai's theorem it is therefore enough to show that any 3-set appears in at most one matching.

So suppose for a contradiction that some 3-set e belongs to two distinct matchings $M_{i,j}$ and $M_{k,l}, k \geq i$. Then $e = v^i \cdot e_1 + j = v^k \cdot e_2 + l$, for some $e_1, e_2 \in M_0$. Hence $e_1 = v^{k-i} \cdot e_2 + v^{-i}(l - j)$. W.l.o.g. we may take $i = 0$ and $j = 0$. Consequently $e_1 = v^k \cdot e_2 + l$ with $0 \leq k < \frac{p-1}{2}$.

To simplify notation we set $a := v^k, b := l$ and assume $e_1 = \{x_1, x_2, x_3\}, e_2 = \{y_1, y_2, y_3\}$, with $x_i = a \cdot y_i + b, 1 \leq i \leq 3$. W.l.o.g. we assume $y_2 = \pi(y_1), y_3 = \pi^2(y_1)$.

Note that we can not have $a = 1$ and $b = 0$, for then $k = 0$ and the two matchings are the same, a contradiction. We also can not have $a = -1$, for then $a^2 = 1$ and hence $k = \frac{p-1}{2}$, again a contradiction.

Now consider the case when $u \in e_2$. We assume $y_1 = u$ (as all other cases follow by permuting indices). Then $x_1 = u$. We also get $y_2 = p-1, y_3 = 0$ and $x_2 = a(p-1)+b, x_3 = b$.

If $x_3 = \pi^2(x_1) = 0$ then $b = 0$ and so $x_2 = p - 1 = a(p-1)$. Then $a = 1$, a contradiction.

So $x_2 = \pi^2(x_1) = 0$ and $b = x_3 = \pi(x_1) = p - 1$. Then $(a + 1)(p - 1) = 0$, hence $a = -1$. But as we have seen this is not possible.

Consequently we may assume that $u \notin e_2$ and hence $p - 1, 0, u \notin e_1 \cup e_2$.

By the computation done at (i) we know that $y_2 = -\frac{1+y_1}{y_1}$ and $y_3 = -\frac{1}{y_1+1}$. We see that

$$y_1 - y_2 = \frac{y_1^2 + y_1 + 1}{y_1}, \tag{1}$$

$$y_1 - y_3 = \frac{y_1^2 + y_1 + 1}{y_1 + 1}. \tag{2}$$

Consequently,

$$a(y_1 - y_2) = a\frac{y_1^2 + y_1 + 1}{y_1} = x_1 - x_2,$$

$$a(y_1 - y_3) = a\frac{y_1^2 + y_1 + 1}{y_1 + 1} = x_1 - x_3,$$

and therefore

$$a(y_1^2 + y_1 + 1) = y_1(x_1 - x_2) = (y_1 + 1)(x_1 - x_3). \tag{3}$$

First assume $x_2 = \pi(x_1), x_3 = \pi^2(x_1)$. Then from (3) and using (1), (2) with y_i replaced by x_i, we get

$$\frac{y_1}{x_1} = \frac{y_1 + 1}{x_1 + 1},$$

from which we deduce that $x_1 = y_1$. But then $x_i = y_i, 1 \leq i \leq 3$, and furthermore $b = 0, a = 1$, a contradiction.

Therefore the only possibility is that $x_2 = \pi^2(x_1), x_3 = \pi(x_1)$. Again from (3) and (1), (2), we obtain

$$\frac{y_1}{x_1 + 1} = \frac{y_1 + 1}{x_1},$$

from which we deduce that $y_1 = -(x_1 + 1)$. But then $y_1 = \frac{1}{x_2}, y_2 = \frac{1}{x_3}$ and $y_3 = \frac{1}{x_1}$. We thus obtain the system of equations

$$\begin{cases} x_1 &= \frac{a}{x_2} + b, \\ x_2 &= \frac{a}{x_3} + b, \\ x_3 &= \frac{a}{x_1} + b. \end{cases}$$

Subtracting cyclically we get

$$\begin{aligned} x_1 - x_2 &= a\frac{x_3 - x_2}{x_2 x_3}, \\ x_2 - x_3 &= a\frac{x_1 - x_3}{x_1 x_3}, \\ x_3 - x_1 &= a\frac{x_2 - x_1}{x_1 x_2}. \end{aligned}$$

Consequently,

$$a^3 = (-1)x_1^2 x_2^2 x_3^2.$$

We now use the identity $x\pi(x)\pi^2(x) = 1$, which is true for any $x \in \mathbb{F}_p^* \setminus \{p-1\}$. Then $a^3 = -1$, and hence $a^6 = 1$. As $a \notin \{1, -1\}$, the order of a in $\mathbb{F}_p^*$ is 3 or 6. Therefore by Lagrange's theorem again, $3 | p - 1 = 3n - 2$, a contradiction.

This completes the proof.