Recurrence relations for Steiner systems with $t = 2$

James Nechvatal
Computer Security Division
National Institute of Standards and Technology, Gaithersburg, MD 20899, USA
james.nechvatal@nist.gov

Abstract A Steiner system $S(2, k, v)$ is a collection of k-subsets (blocks) of a v-set V such that each 2-subset of V is contained in exactly one block. We find recurrence relations for $S(2, k, v)$.

1. Introduction.

Suppose t, k, v are integers with $2 \leq t < k < v$. A Steiner system $S(t, k, v)$ is a v - set V and a collection of k-subsets (blocks) of V such that each t-subset of V is contained in exactly one block. An $S(t, k, v)$ is also a $t-(v, k, 1)$ design. Here we treat the case $t = 2$. An element of V occurs in exactly $(v-1)/(k-1)$ blocks of an $S(2, k, v)$. It follows that every $S(2, k, v)$ has the form $S(2, k, (k-1)z+1)$ for an integer z, and it is easily seen that $z \geq k$. Here we find two recurrence relations for $S(2, k, v)$:

Theorem 1.1. *Suppose k, z, z' are integers, $k \geq 3$, $z \geq k$, $z' \geq k$, an $S(2, k, (k-1)z+1)$ exists, an $S(2, k, (k-1)z'+1)$ exists, and there exist z' - 2 orthogonal Latin squares of order z. Then an $S(2, k, (k-1)z'z+1)$ exists.*

Theorem 1.2. *Suppose k, z, z' are integers, $z > z' \geq k \geq 3$, an $S(2, z', z)$ exists, and an $S(2, k, (k-1)z'+1)$ exists. Then an $S(2, k, (k-1)z+1)$ exists.*

The above are established in Section 2 below. To obtain a more usable form of Theorem 1.1, suppose p is a prime, p^n divides $m > 1$, and p^{n+1} does not divide m. Then call p^n a prime power factor of m. It is well-known that there exist r - 1 orthogonal Latin squares of order m, where r is the smallest prime power factor of m. This yields

Corollary 1.1. *Suppose k, z, z' are integers, $k \geq 3$, $z \geq k$, $z' \geq k$, an $S(2, k, (k-1)z+1)$ exists, an $S(2, k, (k-1)z'+1)$ exists, and z has no prime power factor less than z' - 1. Then an $S(2, k, (k-1)z'z+1)$ exists.*

For example, taking $z' = 4$, $z = 10$, $k = 3$ in Theorem 1.2, existence (e.g., [2]) of an $S(2, 3, 9)$ and an $S(2, 4, 10)$ implies the existence of an $S(2, 3, 21)$. As another example, taking $z' = 6$, $z = 13$, $k = 6$ in Corollary 1.1, existence (e.g.,

[1]) of an $S(2,6,31)$ and an $S(2,6,66)$ implies the existence of an $S(2,6,391)$. In addition to use with sporadic $S(2,k,v)$, Theorem 1.2 and Corollary 1.1 can be instantiated by fixing z' via existing infinite families of $S(2,k,v)$, which include (e.g., [1], p. 103):

A. $S(2,q,q^n)$, q a prime power, $n \geq 2$.

B. $S(2,q+1,q^n+\ldots+q+1)$, q a prime power, $n \geq 2$.

C. $S(2,q+1,q^3+1)$, q a prime power.

For example, suppose q is a prime power. Then in Corollary 1.1 we can take $z' = k = q+1$. Family (B) shows that an $S(2,q+1,q^2+q+1)$ exists. Thus we find

Corollary 1.2. *Suppose q is a prime power, $z \geq q+1$, an $S(2,q+1,qz+1)$ exists, and z has no prime power factor less than q. Then an $S(2,q+1,q(q+1)z+1)$ exists.*

Alternatively, in Corollary 1.1 we can take $k = q$, $z' = q+1$. Family (A) shows that an $S(2,q,q^2)$ exists. Thus we find

Corollary 1.3. *Suppose q is a prime power, $z \geq q \geq 3$, an $S(2,q,(q-1)z+1)$ exists, and z has no prime power factor less than q. Then an $S(2,q,(q^2-1)z+1)$ exists.*

In turn, Corollaries 1.2 and 1.3 can be used to extend existing infinite familes of $S(2,k,v)$. For example, applying Corollary 1.3 to family (A) yields

Corollary 1.4. *Suppose q is a prime power, $z \geq q \geq 3$, $n \geq 2$, and $q^{n-1}+\ldots+q+1$ has no prime power factor less than q. Then an $S(2,q,q^{n+1}+q^n-q)$ exists.*

Applying Corollary 1.2 to family (B) yields

Corollary 1.5. *Suppose q is a prime power, $n \geq 1$, and $q^n+\ldots+q+1$ has no prime power factor less than q. Then an $S(2,q+1,q(q+1)(q^n+\ldots+q+1)+1)$ exists.*

Another application of Corollary 1.1 is

Corollary 1.6. *Suppose $k \geq 3$, q is a prime power, $m \geq 1$, $n \geq 1$, $q^m \geq k$, and an $S(2, k, (k-1)q^m + 1)$ exists. Then an $S(2, k, (k-1)q^{nm} + 1)$ exists.*

The above follows from Corollary 1.1 by first taking $z' = z = q^m$, yielding the case $n = 2$, and then taking $z' = q^m$, $z = q^{(n-1)m}$ to accomplish induction on n. In particular, taking $k = q + 1$, $m = 2$ in the above extends family (C):

Corollary 1.7. *Suppose q is a prime power and $n \geq 1$. Then an $S(2, q+1, q^{2n+1} + 1)$ exists.*

The above and Corollary 1.2 yield

Corollary 1.8. *Suppose q is a prime power and $n \geq 1$. Then an $S(2, q+1, q^{2n+2} + q^{2n+1} + 1)$ exists.*

In Theorem 1.2 we can take $z' = k = q + 1$ and replace z by $qz + 1$. This yields

Corollary 1.9. *Suppose q is a prime power, $z \geq 2$, and an $S(2, q+1, qz+1)$ exists. Then an $S(2, q+1, q^2 z + q + 1)$ exists.*

For example, taking $z = q^{2n}$ in the above and invoking Corollary 1.7 gives

Corollary 1.10. *Suppose q is a prime power and $n \geq 1$. Then an $S(2, q+1, q^{2n+2} + q + 1)$ exists.*

Alternatively, in Theorem 1.2 we can take $k = q$, $z' = q + 1$ and replace z by $qz + 1$. This yields

Corollary 1.11. *Suppose q is a prime power, $q \geq 3$, $z \geq 2$, and an $S(2, q+1, qz+1)$ exists. Then an $S(2, q, q^2 z - qz + q)$ exists.*

For example, taking $z = q^{2n}$ in the above and invoking Corollary 1.7 gives

Corollary 1.12. *Suppose q is a prime power, $q \geq 3$, and $n \geq 1$. Then an $S(2, q, q^{2n+2} - q^{2n+1} + q)$ exists.*

The previous results derive from the study of what we call product systems. These are generalizations of ordinary block designs. In an ordinary t-design, a block consists of k entries from one v-set of varieties V, and each t-set of V must occur in exactly λ blocks. In a product system, V is replaced by a collec-

tion of sets $\{V_i\}$; a block consists of k entries from k different $\{V_i\}$. Each t-set, with entries from t different $\{V_i\}$, must occur in exactly λ blocks. If $|V_i| = 1$ for all i then the product system is isomorphic to an ordinary design. At the opposite extreme, we could choose all the $\{V_i\}$ arbitrarily. In Section 2 we generalize $S(2, k, v)$ via product systems with $|V_i| = m$ for all i, where m is fixed but arbitrary. We find recurrences for the product systems which, when specialized, yield Theorems 1.1 and 1.2. It is not immediately clear whether the results we obtain can be extended to other classes of designs. The prospects for such extensions are difficult to assess. For one thing, we have wide latitude in the choice of $\{V_i\}$, and the choice used in Section 2 might not be optimal for generalizing designs with $t > 2$ or $\lambda > 1$. Also, a given class of product designs may satisfy recurrences not analogous to any noted here. Finally, it is possible that direct construction techniques might exist for product systems; when specialized, these might yield new construction techniques for ordinary designs. An exploration of any of these topics would be beyond the scope of this article.

2. Product systems.

Suppose k, m, n are integers with $n \geq k \geq 2$ and $m \geq 1$. Suppose $V_0, \ldots, V_{n-1}$ are pairwise disjoint m-sets. Let $V = \{V_0, \ldots, V_{n-1}\}$. Suppose $x \in V_i$ and $y \in V_{i'}$ for some i, i' with $i \neq i'$. Then call $\{x, y\}$ a V-pair. Suppose A is a k-set (block) such that if $\{x, y\} \subseteq A$ then $\{x, y\}$ is a V-pair. Then call A a k-block of V. Suppose B is a collection of k-blocks of V such that every V-pair is contained in a unique block of B. Then call B a $PS(k, m, n)$ over V. The exact nature of the $\{V_i\}$ does not affect existence of a $PS(k, m, n)$, as long as the $\{V_i\}$ are pairwise disjoint m-sets. Thus, if a $PS(k, m, n)$ exists over any V we can simply say that a $PS(k, m, n)$ exists. The reason we are interested in product systems is the following:

Lemma 2.1. *Suppose k, z are integers with $z \geq k \geq 3$. Then there exists a $PS(k, k-1, z)$ if and only if an $S(2, k, (k-1)z + 1)$ exists.*

Proof: Suppose B is an $S(2, k, (k-1)z + 1)$ over $V' = \{0, \ldots, (k-1)z\}$. Let

$$V_j = \{ j(k-1), \ldots, j(k-1) + k - 2 \} \qquad (0 \leq j \leq z - 1).$$

Let $V = \{V_0, \ldots, V_{z-1}\}$. We can assume without loss of generality that the blocks of B containing $(k-1)z$ are $\{B_0, \ldots, B_{z-1}\}$ where $B_j = \{(k-1)z\} \cup V_j$. The $\{B_j\}$ contain all pairs of V' of the form $\{i, (k-1)z\}$, $0 \leq i \leq (k-1)z - 1$, and all pairs $\{i, i'\} \subseteq V_j$ for some j. Thus the blocks of B not containing $(k-1)z$ are k-blocks of V containing all V-pairs. Hence the latter blocks consti-

tute a $PS(k, k-1, z)$ over V. Conversely, given a $PS(k, k-1, z)$ over V, adjoining $B_0, \ldots, B_{z-1}$ yields an $S(2, k, (k-1)z+1)$ over V'. □

Now we note

Lemma 2.2. *Suppose k, m, n are integers, $n \geq k \geq 2$, $m \geq 1$, $\{V_0, \ldots, V_{n-1}\}$ are pairwise disjoint m-sets, $V = \{V_0, \ldots, V_{n-1}\}$, and*

$$(2.1) \qquad b = \frac{m^2 n(n-1)}{k(k-1)}.$$

Then if B is a $PS(k, m, n)$ over V then b is an integer and $|B| = b$. Conversely, suppose b is an integer and $B = \{B_0, \ldots, B_{b-1}\}$ is collection of k-blocks of V such that if $0 \leq i < i' \leq b-1$ then $|B_i \cap B_{i'}| \leq 1$. Then B is a $PS(k, m, n)$ over V.

Proof: Suppose B is a $PS(k, m, n)$ over V and $|B| = b'$. Then

$$\binom{k}{2} b' = \binom{n}{2} m^2.$$

The left side of the above is the number of V-pairs contained in the blocks of B. The right side is the total number of V-pairs. Thus $b' = b$ and $|B| = b$. Conversely, suppose b is an integer and $B = \{B_0, \ldots, B_{b-1}\}$ is a collection of k-blocks of V such that if $0 \leq i < i' \leq b-1$ then $|B_i \cap B_{i'}| \leq 1$. Then a V-pair is contained in at most one B_i, and hence, since the above holds with $b' = b$, in a unique B_i. Thus B is a $PS(k, m, n)$ over V. □

Lemma 2.3. *Suppose m, k are integers with $k \geq 3$ and $m \geq 1$. Then there exists a $PS(k, m, k)$ if and only if there exist $k-2$ orthogonal Latin squares of order m.*

Proof: For $0 \leq r \leq k-1$, let $V_r = \{rm, \ldots, rm + m - 1\}$. Let $V = \{V_0, \ldots, V_{k-1}\}$ and $J = \{0, \ldots, m-1\}$. Suppose $M_2, \ldots, M_{k-1}$ are orthogonal Latin squares over J, each with rows and columns indexed by J. For $i, j \in J$ let

$$(2.2) \qquad B_{i,j} = \{i, j+m\} \cup \{M_r[i, j] + rm : 2 \leq r \leq k-1\}.$$

In the above we note $0 \leq M_r[i, j] \leq m-1$, and hence $M_r[i, j] + rm \in V_r$. Thus $B = \{B_{i,j}\}$ is a collection of k-blocks of V. We claim that B is a $PS(k, m, k)$ over V. To prove this claim, suppose $\{x, y\}$ is a V-pair and $\{x, y\} \subseteq B_{i,j} \cap B_{i',j'}$ for some i, j, i', j'. Suppose $x \in V_r$, $y \in V_{r'}$ for some r, r', $0 \leq r < r' \leq k-1$. For some $x', y' \in J$ we have $x = x' + rm$, $y = y' + r'm$. There are four

cases:

Case 1. $r, r' \geq 2$: Then we find $M_r[i, j] = x' = M_r[i', j']$ and $M_{r'}[i, j] = y' = M_{r'}[i', j']$, whence

$$(M_r[i, j], M_{r'}[i, j]) = (M_r[i', j'], M_{r'}[i', j']).$$

Since $r \neq r'$ and M_r and $M_{r'}$ are orthogonal, the above yields $(i, j) = (i', j')$.

Case 2. $r = 0$, $r' \geq 2$: Then we find $i = x' = i'$ and $M_{r'}[x', j] = y' = M_{r'}[x', j']$. Since $M_{r'}$ is a Latin square, $j = j'$.

Case 3. $r = 1$, $r' \geq 2$: Then we find $j = x' = j'$ and $M_{r'}[i, x'] = y' = M_{r'}[i', x']$. Since $M_{r'}$ is a Latin square, $i = i'$.

Case 4. $r = 0$, $r' = 1$: Then we find $i = x' = i'$ and $j = y' = j'$.

In all cases we find $(i, j) = (i', j')$. Thus $|B_{i,j} \cap B_{i',j'}| \leq 1$ for $(i, j) \neq (i', j')$. Also, $|B| = m^2$. The claim follows from Lemma 2.2. Conversely, suppose B is a $PS(k, m, k)$ over V. Then from (2.1) we find $|B| = m^2$. Now $\{i, j + m\}$ is a V-pair, where $i, j \in J$. For $i, j \in J$, let $B_{i,j}$ be the block of B containing $\{i, j + m\}$. Then $B = \{B_{i,j}\}$. For $2 \leq r \leq k - 1$ define M_r over J, with rows and columns indexed by J, via (2.2). We claim that $\{M_2, \ldots, M_{k-1}\}$ are orthogonal Latin squares. To prove the claim, first of all we note that if $x \in V_r$, $y \in V_{r'}$, $r \neq r'$, and $\{x, y\} \subseteq B_{i,j} \cap B_{i',j'}$ then $(i, j) = (i', j')$. The proof of the claim splits into three cases:

Case 1. Suppose $i, i', j \in J$, $i \neq i'$, $2 \leq r \leq k - 1$, and $M_r[i, j] = M_r[i', j]$. Let $x = j + m$, $y = M_r[i, j] + rm$. Then $\{x, y\} \subseteq B_{i,j} \cap B_{i',j}$, but $x \in V_1$ and $y \in V_r$, contradiction.

Case 2. Suppose $i, j, j' \in J$, $j \neq j'$, $2 \leq r \leq k - 1$, and $M_r[i, j] = M_r[i, j']$. Let $x = i$, $y = M_r[i, j] + rm$. Then $\{x, y\} \subseteq B_{i,j} \cap B_{i,j'}$, but $x \in V_0$ and $y \in V_r$, contradiction.

Case 3. Suppose $i, i', j, j' \in J$, $(i, j) \neq (i', j')$, $2 \leq r < r' \leq k - 1$, $M_r[i, j] = M_r[i', j']$, and $M_{r'}[i, j] = M_{r'}[i', j']$. Let $x = M_r[i, j] + rm$, $y = M_{r'}[i, j] + r'm$. Then $\{x, y\} \subseteq B_{i,j} \cap B_{i',j'}$, but $x \in V_r$ and $y \in V_{r'}$, contradiction.

Cases 1 and 2 show that each M_r is a Latin square over J. Case 3 shows that the $\{M_r\}$ are orthogonal. □

Remark: In Lemma 2.3, taking $m = k - 1$ and invoking Lemma 2.1 shows that an $S(2, k, k(k-1)+1)$ exists if and only if there exist $k - 2$ orthogonal Latin squares of order $k - 1$. This is a well-known result: an $S(2, k, k(k-1)+1)$ is a projective plane of order $k - 1$.

Lemma 2.4. *Suppose k, m, z, z' are integers, $k \geq 2$, $z \geq k$, $z' \geq k$, $m \geq 1$, a $PS(k, m, z)$ exists, a $PS(k, m, z')$ exists, and a $PS(z', z, z')$ exists. Then a $PS(k, m, z'z)$ exists.*

Proof: For $0 \leq i \leq z' - 1$, $0 \leq j \leq z - 1$ suppose $V_i(j)$ is an m-set. Suppose $V_i(j) \cap V_{i'}(j') = \emptyset$ if $(i, j) \neq (i', j')$. For $0 \leq i \leq z' - 1$ let $V_i = \{V_i(0), \ldots, V_i(z-1)\}$. Let $V = V_0 \cup \ldots \cup V_{z'-1}$. For $0 \leq i \leq z' - 1$, V_i is a set of z pairwise disjoint m-sets; hence, suppose A_i is a $PS(k, m, z)$ over V_i. For $0 \leq r \leq z' - 1$ let $W_r = \{rz, \ldots, rz + z - 1\}$. Let $W = \{W_0, \ldots, W_{z'-1}\}$. Then W is a set of z' pairwise disjoint z-sets; hence, suppose B is a $PS(z', z, z')$ over W. Suppose $B = \{B_0, \ldots, B_{b-1}\}$. Then per (2.1), $b = z^2$. Also, each B_s is a z'-block of W. Thus, B_s contains exactly one element from each W_r. Suppose for $0 \leq s \leq b - 1$ that $B_s = \{a_{s,r} + rz : 0 \leq r \leq z' - 1\}$, where $0 \leq a_{s,r} \leq z - 1$. For $0 \leq s \leq b - 1$, $0 \leq r \leq z' - 1$ let $Y_{s,r} = V_r(a_{s,r})$. For $0 \leq s \leq b - 1$ let $Y_s = \{Y_{s,0}, \ldots, Y_{s,z'-1}\}$. Since the $\{V_i(j)\}$ are pairwise disjoint they are distinct. Hence $Y_{s,r} = Y_{s,r'}$ implies $r = r'$. Thus each Y_s is a set of $z' - 1$ pairwise disjoint m-sets. For $0 \leq s \leq b - 1$ suppose E_s is a $PS(k, m, z')$ over Y_s. Let

$$G = E_0 \cup \ldots \cup E_{b-1} \cup A_0 \cup \ldots \cup A_{z'-1}.$$

We claim that G is a $PS(k, m, z'z)$ over V. To prove the claim, first of all, per (2.1) we have

$$|E_s| = \frac{m^2 z'(z'-1)}{k(k-1)} \quad (0 \leq s \leq b-1),$$

$$|A_i| = \frac{m^2 z(z-1)}{k(k-1)} \quad (0 \leq i \leq z'-1).$$

Thus, assuming that the blocks defining G are all distinct,

$$|G| = \frac{m^2 z'z(z'z-1)}{k(k-1)}.$$

Per (2.1), the right side above is the correct number of blocks for a $PS(k, m, z'z)$. Also, each V_i and Y_s is a subset of V. Thus, each block of each A_i

and E_s is a k-block of V, as is each block of G. Per Lemma 2.2, to prove the claim we need only show that if H, H' are two of the blocks defining G then $|H \cap H'| \leq 1$. There are four cases:

Case 1. H, H' are blocks of A_i , or blocks of E_s , for some i or s: Then by definition $|H \cap H'| \leq 1$.

Case 2. H is a block of A_i and H' is a block of $A_{i'}$, for some $i \neq i'$: Then each element of H is from some V_i (j), and each element of H' is from some $V_{i'}$ (j'). Since V_i (j) and $V_{i'}$ (j') are disjoint, $|H \cap H'| = 0$.

Case 3. H is a block of E_s and H' is a block of $E_{s'}$, for some $s \neq s'$: Suppose $x \neq y$ and $\{x, y\} \subseteq H \cap H'$. Then $x \in Y_{s,r} \cap Y_{s',r'}$ for some r, r', and $y \in Y_{s,r''} \cap Y_{s',r'''}$ for some r'', r''' with $r'' \neq r$ and $r''' \neq r'$. Thus $x \in V_r\ (a_{s,r}) \cap V_{r'}\ (a_{s',r'})$ and $y \in V_{r''}\ (a_{s,r''}) \cap V_{r'''}\ (a_{s',r'''})$. Hence $r' = r$, $r''' = r''$, $a_{s,r} = a_{s',r}$, and $a_{s,r''} = a_{s',r''}$. Now if $w \in W_r$ and $w'' \in W_{r''}$, then $\{w, w''\}$ is contained in a unique B_s . Let

$$w = a_{s,r} + rz = a_{s',r} + rz\,,$$

$$w'' = a_{s,r''} + r''z = a_{s',r''} + r''z\,.$$

Then $w \in W_r$ and $w'' \in W_{r''}$, but $\{w, w''\} \subseteq B_s \cap B_{s'}$. Thus $s' = s$, contradiction. Hence $|H \cap H'| \leq 1$.

Case 4. H is a block of E_s and H' is a block of A_i , for some s, i: Suppose $x \neq y$ and $\{x, y\} \subseteq H \cap H'$. Then $x \in Y_{s,r} \cap V_i\ (j)$ and $y \in Y_{s,r'} \cap V_i\ (j')$ for some r, r', j, j' with $r \neq r'$ and $j \neq j'$. Now $x \in V_r\ (a_{s,r}) \cap V_i\ (j)$ and $y \in V_{r'}\ (a_{s,r'}) \cap V_i\ (j')$. Hence $r = i = r'$, contradiction. Thus $|H \cap H'| \leq 1$. □

Corollary 2.4. *Suppose k, z, z' are integers, $k \geq 3$, $z \geq k$, $z' \geq k$, a $PS(k, k-1, z)$ exists, a $PS(k, k-1, z')$ exists, and there exist z' - 2 orthogonal Latin squares of order z. Then a $PS(k, k-1, z'z)$ exists.*

Proof: In Lemma 2.4 take $m = k$ - 1 and invoke Lemma 2.3. □

Combining Corollary 2.4 and Lemma 2.1 yields Theorem 1.1. Finally we note

Lemma 2.5. *Suppose k, m, z, z' are integers, $z > z' \geq k \geq 3$, $m \geq 1$, a $PS(k, m, z')$ exists, and an $S(2, z', z)$ exists. Then a $PS(k, m, z)$ exists.*

Proof: Suppose $V(0), \ldots, V(z-1)$ are pairwise disjoint m-sets. Let $V = \{V(0), \ldots, V(z-1)\}$ and $V' = \{0,\ldots,z\text{-}1\}$. Suppose B is an $S(2, z', z)$ over V' and $B = \{B_0, \ldots, B_{b-1}\}$. For $0 \le s \le b$ - 1 suppose $B_s = \{a_{s,0}, \ldots, a_{s,z'-1}\}$. Then each $a_{s,r} \in V'$. For $0 \le s \le b$ - 1 let $Y_s = \{V(a_{s,0}), \ldots, V(a_{s,z'-1})\}$. Then each Y_s is a set of z' pairwise disjoint m-sets. Hence, suppose A_s is a $PS(k, m, z')$ over Y_s. Let $A = A_0 \cup \ldots \cup A_{b-1}$. We claim that A is a $PS(k, m, z)$ over V. To prove the claim, we note that

$$b = \frac{z(z-1)}{z'(z'-1)}.$$

Per (2.1), for $0 \le s \le b$ - 1,

$$|A_s| = \frac{m^2\, z'(z'-1)}{k(k-1)}.$$

Thus, assuming that the blocks defining A are all distinct,

$$|A| = \frac{m^2\, z(z-1)}{k(k-1)}.$$

Per (2.1), the right side above is the correct number of blocks for a $PS(k, m, z)$. Also, each Y_s is a subset of V. Thus, each block of each A_s is a k-block of V, as is each block of A. Per Lemma 2.2, to prove the claim we need only show that if H, H' are two of the blocks defining A then $|H \cap H'| \le 1$. There are two cases:

Case 1. H, H' are blocks of A_s for some s: Then by definition $|H \cap H'| \le 1$.

Case 2. H is a block of A_s and H' is a block of $A_{s'}$, for some $s \ne s'$: Suppose $x \ne y$ and $\{x, y\} \subseteq H \cap H'$. Then $x \in V(a_{s,r}) \cap V(a_{s',r'})$ for some r, r', and $y \in V(a_{s,r''}) \cap V(a_{s',r'''})$ for some r'', r''' with $r'' \ne r$ and $r''' \ne r'$. Since the $\{V_i\}$ are pairwise disjoint, $a_{s,r} = a_{s',r'}$ and $a_{s,r''} = a_{s',r'''}$. Now $|B_s \cap B_{s'}| \le 1$. Hence $a_{s,r} = a_{s,r''}$ and thus $r = r''$, contradiction. Hence $|H \cap H'| \le 1$. □

Taking $m = k$ - 1 in Lemma 2.5 and invoking Lemma 2.1 yields Theorem 1.2.

References:

[1] C. J. Colbourn and R. Mathon, Steiner systems, in: C. J. Colbourn and J. H.